Information Security & Cyber Threats to the Private Critical Infrastructure and Financial Services

Trends & Implications for the Public and Private Sectors

Session: Securing Cyberspace & America’s Cyber Assets: Threats, Strategies & Opportunities

September 10, 2009

Presenter:
Brian McGinley
Principal
BGM Risk Management Group
“it” happens every day.....

Phishers point scam at Apple's iTunes
Music store users targeted for the first time by sophisticated ID theft, says Proofpoint
By Gregg Keizer
May 20, 2008 (Computerworld) Phishers have targeted users of Apple’s iTunes music store with sophisticated identity theft attacks for the first time, a security company said today.

Credit Card Breach Raises Broad Concerns
PORTLAND, Maine (AP) — When up to 4.2 million account numbers were stolen over three months by thieves who cracked computers at Hannaford.

Boeing laptop theft puts U.S. data breach tally over 100M
A privacy group has kept tabs on incidents since February 2005
By Rachel Konrad, AP Technology Writer

DSW Data Theft Much Larger Than Estimated
COLUMBUS, Ohio - Thieves who accessed a DSW Shoe Warehouse database obtained 1.4 million credit card numbers and the names on those accounts — 10 times more than investigators estimated last month.

Sears sued over privacy breach
Class-action lawsuit seeks damages and wants Sears to determine whether its Managementhome Web site was misused by criminals
By Robert McMillan, IDG News Service
January 08, 2008

Burned By ChoicePoint Breach, Potential ID Theft Victims Face a Lifetime of Vigilance
Feb. 24, 2005
More than 9.9 million Americans were victims of identity theft last year. Many victims are dumbfounded by the dearth of federal and state laws aimed at protecting their credit histories and other information about them.
By Rachel Konrad, AP Technology Writer
His Was Stolen...
How Safe Is Your Identity?
What you must do to protect yourself

By Lynn Brenner
Fraud Trends / Privacy at Risk – Information Under Attack

• Consumer and Business Information has become a “Criminal Commodity” wherein its value and market for open exchange has increased to unprecedented scale. Information has become the currency and enabler of FRAUD

The reason?

• **Information = Transactional Access** in the financial services’ world – and it is all about the **MONEY**!

• Internal data compromise
• External data compromise

Consumer information and privacy is under siege by individuals who are able to gain access to personal biographic, demographics and financial information via theft of trash, internet, public record sources, compromise of non-public sources via hacking and/or “social engineering” & corruption of individuals with access to the information.
Critical Infrastructure - Private Sector

• Where we sit today:

Banking & Finance; Telecommunications; Energy & Water; Transportation, Healthcare as U.S. Critical Infrastructure are often similarly positioned:

• Don’t go to Fort Knox or the Federal Reserve looking for our Nation’s wealth – we have truly become a “Digital Economy”

• We have all moved from “Computer Assisted to Computer Dependent” internally and externally

• Large complex, distributed networks and applications – many “cobbled” together from merger & acquisitions from disparate, antiquated legacy systems – many serviced remotely and many by third party service providers

• Collect, Store, and Transmit sensitive and confidential data including:
  - Customers/Clients/Employees/Vendors
  - Business Data containing our key strategies as well as operating practices, policies, procedures, and systems information
  - Intellectual Property
Critical Infrastructure - Private Sector

• Where we sit today (continued):

• We all have significant assets at risk. In Financial Services, we Initiate and manage Trillions of Dollars in Electronic Financial Transactions in the United States Daily.

• We all have “exploitable data” exposed on our internal systems as well as on the Internet

• We have all experienced significant cyber incidents, many of which have cost us millions of dollars, loss of client trust, and landed us in the media......in some cases in front of Congress

• The Barbarians are not only at the gate – they are in our dining room, eating off our best china!”

• Cyber Protection Posture? Nobody has it right, yet! – Not the Government – Not the Private Sector

• We are all, in some form, government regulated
Critical Infrastructure - Private Sector

• Our Common Challenges:

  • Key Threats to our Viability include Disruption of Service and Damage, Theft or Exploitation of our assets, information or resources

  • We have all made very large investments in our IT infrastructure, systems and security but are yet, still significantly “underinvested” based on current and emerging threats

  • We are still often times in a state of denial in the Executive Suite

  • We are resourced constrained in the IT and Information Security areas by both funding & SME. There is exceptional competition for resources within our businesses aggravated by aggressive expense reduction initiatives to survive the economic downturn.
Critical Infrastructure - Private Sector

• Our Common Challenges (Continued):
  • We are chasing cybercrime based on our “investment model” of “too little, too late!
  
  • Remediation and Upgrading are most often very slow, staged and cumbersome processes
  
  • Long solution identification, vetting, selection, approval, funding and procurement process
  
  • The System Development Lifecycle is a two edged sword – it is vital to successful system implementation and change management but is hurting us in terms of rapid deployment of system countermeasures against the threat
  
  • The “life-time” of successful countermeasures is limited – often by deployment, the bad guys have already defeated it
  
  • Often “drowning in information but starved for knowledge”
Should The Threat & Reality of Compromised Consumer and Business Information housed by the Financial Services Sector as an “Intelligence Commodity” be of concern? Consider the information:

- Economic Impact – US = Loss, Opportunity Cost, Imposed Limitations
  THEM (The Bad Guys) = source of funding & information
- Financial – source, distribution, & destination of funds
- Detailed Spending Activities & Patterns (Personal & commercial behaviors)
- Geographic Movement of Principals
- Time & Place of Transactions
- Photographic Retrieval of transactions
- Predictive Analysis of Individual and Company Patterns
- Exploitation of individuals & companies based on internal knowledge
- Classic recruitment utilization
- Compromise of operations
- Utilization of informational access for new methods & tradecraft
Trends – Financial Services

• Bank & Financial Fraud will continue to increase driven by:
  • Expansion of Access Opportunities, New Technology, and Speed - New Products and Product Functionalities
  • Expansion of criminal elements
    ▪ Organized Crime
    ▪ Street Gangs
    ▪ Local, Regional, National & International Fraud Rings
    ▪ Underground International Hacker Community & Marketplace
    ▪ Terrorist Financing Opportunity
    ▪ Intelligence Exploitation Opportunity
    ▪ Active Placement and/or Recruitment of insiders with access to customer information
  • Limited risk of immediate detection, apprehension, & prosecution
Trends – Financial Services

• **Bank & Financial Fraud will continue to increase driven by:**
  
  • Expansion of Access Opportunities, New Technology, and Speed - New Products and Product Functionalities
  
  • Expansion of criminal elements
    • Organized Crime
    • Street Gangs
    • Local, Regional, National & International Fraud Rings
    • Underground International Hacker Community & Marketplace
    • Terrorist Financing Opportunity
    • Intelligence Exploitation Opportunity
    • Active Placement and/or Recruitment of insiders with access to customer information
  
  • Limited risk of immediate detection, apprehension, & prosecution
Trends – Financial Services

• Traditional Bank Customer Verification Tools Are Being Compromised:

• Technology is in the hands of the criminals:

  ▪ Counterfeiting of checks, personal identification, account access devices, signature verification, business documentation and reference letters is a major exposure area. This has carried over to the electronic environment

  ▪ PC document scanning/laser printing, color copiers
  ▪ PC Check Printing Packages with MICR Ink
  ▪ Plastic Card Embosser / Mag Stripe duplicator
  ▪ User IDs, Passwords, & Tokens vs. Malicious software & Hacker Tools
Examples of Fraudulent Ids

One person...multiple identities
It is now possible to begin the order, kent4 (enough cheap) Language: 

Choice the dokes what you want.

New Offer!

-35€ 25€
Counterfeit Checks
Counterfeit USPS Money Orders
Bogus US Treasury Check
Misery Enjoys Company
Trends – Financial Services

• Traditional Bank Fraud Not Going Away – Issues are complicated and compounded by additive cyber-risks

  • High Volume Compromises
  • 24X7 Automated Scripted Attacks
  • “Over-run the Compound” Resources
  • Cross Channel Infiltration
  • Identification of Point of Compromise (POC) is complex and adds to investigative overhead
Trends – Financial Services

• New Technology – New Opportunities
  • PC Banking & Expanded Functionality – “Bank in a Box”
    • High Risk Functionality – Inter-bank Money Movement, Wire Transfers and Bill Pay
    ▪ Customer self-service – Product Sign-up & account maintenance like change of address and telephone number, check & card orders, change credentials
  • The Internet – “Reach out and touch someone” - get touched right back!
  • Peer to Peer File Sharing (PTP & BTB) Exploits
  • Electronification – ACH conversation & presentation of checks and return deposits.
    • Check R&T + Account Number = electronified check, ACH or Draft
    • Opportunity for Merchant and Merchant employee collusion
  • Remote Deposit Collection (RDC)
  • eCommerce – a world of new payment mechanisms
  • 3rd Party Aggregators – “Partying With Third Parties” – InfoSec Risk
  • Wireless – PCs, Palms, Text, and Cells
Fraud Containment Challenges

• **More Access Channels – Many No Longer Under Direct Bank Control**
  - ATMs – Proprietary, Networked, Privately Owned
  - POS Expansion
  - Telephone Banking & Bank By Mail
  - Internet / PC Banking, Blackberry, Palm et al Access
  - ACH – now allows direct access to customer accounts by merchants – both bank customer merchants and non-customer merchants via their respective bank (ala ODFI and RDFI)
  - 3rd Party Aggregation & Merchant Processors

• **Remote Identification of Customers – A Continuing Challenge**
  - Bank By Mail
  - Telephone Banking
  - PC / Home Banking
  - Availability of correct bio/demo information
  - Availability and customer acceptance of unique remote identification information and options
CardTool™ Magnetic Card Reader for Visor™ Handheld Computer

Features
- Versatile 3-Track Card Reader
- 2 Megabytes of Flash Memory
- Springboard Compatible
- Low Power Design
- Low Profile Case
- No external batteries required
- No Serial or IR port required
- Compatible with Palm OS® development tools
- Durable and reliable
- Optional custom magnetic Decoding Algorithms and Security Management features

The Perfect Tool for Magnetic Cards

The CardTool reader is a Springboard expansion module that contains a 3 track magnetic card reader and 2 Megabytes of internal flash memory. The 3 track reader can read all standard encoded magnetic cards and can be field updated to read proprietary encoded cards. The 2 Megabytes of flash memory provides a convenient way to distribute card applications and back-up important data such as card transaction databases.

The plug-and-play architecture of the Visor handheld facilitates the automatic installation of applications. Applications can automatically install when the CardTool reader module is inserted. Eliminates the need to download software distribution a snap! Simply insert the CardTool reader module and start reading cards!

The Springboard expansion slot provides the data communication paths and power. No external batteries are required plus the USB and IR ports remain available. No need to remove the CardTool reader to download transaction data.

The CardTool reader module ships with a sample card application (CardDemo) installed. It provides a convenient demonstration application and the C source code is included in the System Development Kit. If you've been looking for a low cost, handheld magnetic card transaction processing platform, look no further. Start developing your application today!

CardTool Reader Pays for Itself

The CardTool will actually pay for itself by saving the time and hassle of loading card applications. Unlike 'clip-on' serial port readers, the CardTool reader module takes advantage of the Springboard expansion slot's plug and play architecture. The built in flash memory allows CardTool applications to be archived in non-volatile memory and activated when inserted into the handheld computer. The flash memory can also back-up critical transaction data. In the event the handheld computer is disabled, just insert the CardTool reader into another handheld and resume where you left off. Not only do you save installation time, but all the time and effort that went into creating critical card transaction data. What is the cost of losing a day's worth of transactions?

CardTool Reader Module Specifications

- Weight: 2.5 ounces / 72 grams
- 3.3V 0.1 x 17 84mA CMOS (75mA@7VDC (LWV))
- 2 Megabytes of flash memory—Field upgradable for software applications and card transaction database files
- Field Upgradable magnetic card decode algorithms and proprietary VSDK
- Applications can run entirely in flash memory without taking away Visor computer memory
- Bi-directional card swiping
- Cards thickness from 0.75 mm to 0.09 mm thick.
- Read data densities of 60 to 288 BPI.

Duraibity
- MTBF: The reader chassis electronics have a minimum mean time before failure in excess of 500,000 hours.
- The reader head chasses are designed for at least 500,000 swipes.

Environmental
- Operational Temperature: -20°C to +50°C
- Storage Temperature: -20°C to +70°C
- Humidity (non-condensing): 90% to 40°C

Electrical
- Shut Down current: < 0.25mA
- Card Processing standby: < 40mA
- Card Processing active: < 15mA
- Flash Write/erase current: < 20mA
- Flash Read current: < 5mA

The following specifications apply for bit densities of 75 or 216 BPI or ISO 7811 compliant media:
- Media Speed: The reader reads at speeds from 10 to 180 seconds (4 to 71 IPS).
- Media Specifications: 200 - 4000 density (53 - 1100 IPS).

System Development Kit

The CardTool System Development Kit has been designed by TokenWorks to get developers developing quickly. The less time spent searching for needed information and support, the quicker your product gets to your customer. The SDK contains: One CardTool reader Module, Sample encoded magnetic striped cards, shared library, sample application with source code, user and quick start documentation, programmers reference documentation, and email technical support. The SDK supports the GNU and CodeWarrior compilers. Check the TokenWorks web site for pending support for other development environments.

Visor Handheld Specifications

Presently there are six Visor handheld models, the Visor Deluxe, Visor Neo, Visor Platinum, Visor Pico, Visor Edge, and the Visor Pro. Visit www.handspring.com for complete product information.
- RAM: 2 MB 5 MB or 16 MB depending on the model.
- Springboard expansion slot for CardTool reader module or other springboard modules
- Infrared transceiver to beam records and software to other HandSpring or Palm devices
- Palm OS version 3.1 or 3.5.2 depending on model
- Easy to use large touch screen display (192 x 160 pixels) with backlight. Palm has 65,000 colors display.
- Power 2 AAA alkaline batteries or internal rechargeable lithium ion battery. Rechargeable Ni-MH can replace alkaline AAA batteries.

Preiliminary Product Information, Subject to Change Without Notice.

Date: November 2001
FIN: 001-132109-C6GG-R1

CardTool and TokenWorks are trademarks of TokenWorks Inc. Visor, Handspring and Springboard are trademarks of Handspring. Inc. All other brands, product names, and logos are trademarks of their respective owners.
Skimming Device

• Restaurant employee caught using skimming device to capture ATM and Credit Card numbers in Drive-Thru window.
• Employee was paid $1000 for 50 numbers and $2000 for 100 numbers provided to recruiter.
• Recruiter was paid $4000 for every restaurant employee he recruited by ring leader.
Embedded Parasites discovered inside POS Terminals

Fair Isaac’s CardAlert Fraud Manager Team has received permission from the US Secret Service to distribute information pertaining to a recent investigation that revealed embedded card skimming equipment inside gas station POS terminals in Southern California. It is suspected that individuals are approaching gas station attendants in the Los Angeles area with offers of cash in exchange for their cooperation. Sources close to the investigation indicate that once cooperation is gained the criminals then replace the normal POS terminals with specially engineered ones that have skimming units embedded inside them.

The US Secret Service has confiscated several terminals that have uniquely engineered interior components designed to capture card and PIN information. It is believed that the criminals involved in this operation modify the interior workings of the POS terminals with simple handheld PDA devices that are perfect for continuous recording of card and PIN data. Once in place, the POS terminals do not require attention until the criminals return to reclaim their POS equipment. Fresh terminals then replace terminals already full of stolen data which will later be downloaded and used to produce counterfeit debit cards. The US Secret Service has stated that additional POS parasites may exist.

Please contact the Los Angeles field office fraud squad of the US Secret Service at (213) 533-4525 if you have any information that may lead to the detection of additional terminals.

The following is an actual photograph of the interior of one of the confiscated POS devices:

![Image of a POS terminal]

A higher resolution of this image is located within the “What’s Happening with CardAlert Fraud Manager” section of our website at: [http://fraudforum.fairisaac.com/cgi-bin/yabb/YaBB.pl](http://fraudforum.fairisaac.com/cgi-bin/yabb/YaBB.pl)
Recent example of card skimmer attached to the front of an ATM with the added twist of a camera!
Fraud Containment Challenges

As the skimmer is removed, you notice that part of an existing label on the ATM was partially obscured (see the previous slide).
Fraud Containment Challenges

When the brochure pocket is removed, the hole cut for the camera is clearly visible.
Example of Skimmer Recently Discovered an ATM in FL.

No skimmer.

Skimmer!
Skimmer and Keyboard Overlay Components

- The keypad fits neatly over the existing keypad and would also be very hard to detect. When the customers enter the PIN on the fake keypad, the keypad is wired to record the PIN.
Fraud Containment Challenges

• **New Frontiers Convergence – Some Volatile Combinations**
  - New Technology
  - Global Reach – without benefit of parity of law or law enforcement
  - Lack of Experience – Lack of Experts
  - New Legal Issues, new laws, no laws, lack of litigation findings
  - A Handful of Electrons – Investigate and Prosecute this!!!
  - Image – No Originals – Manipulation – Beyond a Reasonable Doubt

• **Outsourcing, Off-shoring, and Utilization of Temporary Employees**
  - “Who is Minding Our Stores?”
  - Administrative, Security & Janitorial, Production Shops, Mail Rooms, Copy Centers, Archival & Destruction
  - PC, Server, and LAN Support; Business Continuity Hot & Warm sites
  - Off-shore of Application Development & Maintenance (ADM); Business Process Offshoring (BPO); and Knowledge Process Off-shoring (KPO)
CyberThreat Landscape

Technologies Facilitate Criminal Activity
Internet Fraud Considerations

• Prevalent Internet Schemes:
  • Phishing, Pharming, Smishing, Vishing
  • SPAM - Fraudulent Notification or Requests for Information
  • BOTS & BOTNETS
• Malicious Software – Spyware, Virus Infection, Key Stroke Capture, Turn off protections, create cache, backdoors & high value transaction alerting. Zero Day Attacks
• Web Site Impersonations (Spoofing) & Redirection – Collection of Account & Authentication Information
• Man in the Middle & Session Hijacking
• Breach of Credit Card Processors & Merchant Sites for theft of customer and account information – followed by fraudulent transactions & card counterfeiting
• Exploitation of Peer File Share Functions – PTP; BTB; BTP
• Identity Theft/Customer Impersonation – Establishment of New Account & Remote Authentication Challenges
• Packet Sniffing – customer, employment, transmission site or bank
• Use of Remote Access PC Programs – (PC Anywhere – Timbuktu)
• Denial of Service Attacks
• Web Vandalism
Internet users work at computers at the Philadelphia Public Library. Using public terminals carries some risk.

Kinko's spy case illustrates risks of public Internet use

Man used software to steal computer users' names, passwords

BY ANICK JESDANUN
Associated Press

NEW YORK – For more than a year, unbeknownst to people who used Internet terminals at Kinko's stores in New York, Juju Jiang was recording what they typed, paying particular attention to their passwords.

Jiang had secretly installed, in at least 14 Kinko's stores, software that logs individual keystrokes. He captured more than 450 user names and passwords, using them to access and even open bank accounts.

The case, which led to a guilty plea earlier this month after Jiang was caught, highlights the risks and dangers of using public Internet terminals at cybercafes, libraries, airports and other establishments.

"Use common sense when using any public terminal," warned Neel Mehta, research engineer at Internet Security Systems Inc. "For most day-to-day stuff like surfing the Web, you're probably all right, but for anything sensitive you should think twice."

Jiang was caught when, according to court records, he used one of the stolen passwords to access a computer with GoToMyPC software, which lets individuals remotely access their own computers from elsewhere.

The GoToMyPC subscriber was home at the time and suddenly saw the cursor on his computer move around the screen and files open as if by themselves. He then saw an account being opened in his name at an online payment transfer service.

Jiang, who is awaiting sentencing, admitted installing Invisible KeyLogger Stealth software at Kinko's as early as Feb. 14, 2001. The software is one of several keystroke loggers available for businesses and parents to monitor their employees and children.

SEE KINKO'S 1 50
Russian Business Network

• Network traces taken outside of Banks show encrypted data being “posted” to RBN collection points.

• Network traces show malware being downloaded onto Bank data equipment.

• Undetected malware from Bank machines that was traced to RBN collection servers.

• Many compromised internal and remote access machines were participating in the Storm Worm botnet, which is tied to the RBN.

• Some computers of home users and customers appear on malicious activity blacklists. These users may be unaware that they are housing – or involved with – the malicious activity.
To whom it may concern;

In cooperation with the Department Of Homeland Security, Federal, State and Local Governments your account has been denied insurance from the Federal Deposit Insurance Corporation due to suspected violations of the Patriot Act. While we have only a limited amount of evidence gathered on your account at this time it is enough to suspect that currency violations may have occurred in your account and due to this activity we have withdrawn Federal Deposit Insurance on your account until we verify that your account has not been used in a violation of the Patriot Act.

As a result Department Of Homeland Security Director Tom Ridge has advised the Federal Deposit Insurance Corporation to suspend all deposit insurance on your account until such time as we can verify your identity and your account information.

Please verify through our IDVerify below. This information will be checked against a federal government database for identity verification. This only takes up to a minute and when we have verified your identity you will be notified of said verification and all suspensions of insurance on your account will be lifted.

http://www.fdic.gov=01@211.191.98.216:3180/index.htm
http://www.fdic.gov/idverify/cgi-bin/index.htm

Failure to use IDVerify below will cause all insurance for your account to be terminated and all records of your account history will be sent to the Federal Bureau of Investigation in Washington D.C. for analysis and verification. Failure to provide proper identity may also result in a visit from Local, State or Federal Government or Homeland Security Officials.

Thank you for your time and consideration in this matter.

Donald E. Powell
Chairman Emeritus FDIC
John D. Hawke, Jr.
Comptroller of the Currency
Michael E. Bartell
Chief Information Officer

Email used in recent “phish” that sent responders to a fake FDIC website.

Address appears to be legitimate but after the http://www.fdic.gov the address that follows routes users to a server located at 211.191.98.216
RED FLAG: Note the claim that “your information is being submitted via a secure server.” A quick look at the address does NOT show the prefix https which indicates a secure server. Also, the lock and keys icon is missing from the lower right hand part of the screen.
Identity Verification. Step 2 of 3.

Please, enter the details of your ATM card you are using to access your checking account with.

Card Number: 551213664561231
Expiration date: 01 / 2033
CVV2 Code: 584  This is a non-embossed 3-digit number printed on the signature panel on the back, immediately following the account number.
ATM Pin-Code: 1234

Continue
Screenshot of spoofed FDIC site-page 3

Thank you.
Your information is now verified and all holds on your account have now been released.
Impact of a Phish

Customer receives unsolicited email

Customer responds to Phish with one or more of the following: UserID, Password, Checkcard, PIN, CVV2, Expiration Date, DDA

Crook tests validity

Sell on Black Market

Use for Fraud

Access Online Banking to create Billpay, perform balance transfers or Online Money Movement **

In controlled tests - within 3 minutes

@

Create counterfeit checks from image viewed online (use in-range check numbers and/or lift signature)

Upon Password reset or Blue List block, crook uses Checkcard and account number to reset credentials

Use Checkcard CNP Purchase i.e.; WebHost

Reset Data (email adds)
Phish Progression – The Bait

---------- Forwarded message ----------
From: Wachovia <service@wachovia.com>
Date: Jan 6, 2007 9:16 PM
Subject: Wachovia Online Banking Notice
To:

Dear Wachovia Bank Customer,

It has come to our attention that your account needs to be updated due to the recent changes we have made to our Online Banking system. This update will allow us to activate new features for your account on our new system. We have made these changes to serve you better.

With our 24 hour online financial center, you can manage your Wachovia accounts, see images of the front and back of cleared checks and deposit tickets, transfer funds between eligible Wachovia Bank accounts, order checks and much more.

Wachovia Online Banking is quick, easy and convenient allowing you to bank whenever and wherever you want. Please click the link below, this will take you to Wachovia Online Banking to complete your update.

It's important that you activate your card, otherwise you will not be able to access our new Online Banking system and features.

https://www.wachovia.com/auth/AuthService

Sincerely,
Wachovia Bank
Security Department.
Phish Progression – The Hook

Notice where you landed when you clicked on the link - NOT Wachovia.com!

When you enter your UserID and Password - you have just provided that information to the Phisher!
Phish Progression – The Line

Notice there is no "s" after "http" which indicates that this is not a secure site. If you were really in Wachovia's authenticated space, this would appear as "https:"

Notice the absence of a 'padlock' symbol, indicating this is not a secure site. Wachovia's real site displays a padlock symbol.
Phish Progression – The Sinker

This phishing site is a good example of the level of sophistication the phishers have achieved. When you click "submit", the phishing site tries to redirect you to the real Wachovia.com site. (If you had not been paying attention - you may think that you are really in Wachovia.com and not realize what has just happened!)
Internet threat: Hackers swarm bank accounts
By Byron Acohido, USA TODAY

New and nasty banking trojans are on the rise on the Internet and attacking online bank accounts.
The new trojan programs — which wait on your hard drive for an opportunity to crack your online banking account — are different from traditional "phishing" e-mail scams that try to trick you into typing your login information at fake bank websites.
They're invisible, can steal data multiple ways and require no action by the victim to be launched.
"Phishing doesn't work as well as it used to," says Patrik Runald, security specialist at F-Secure, the Internet security firm. "Banking trojans provide a very effective and direct means for the bad guys to get their hands on the money."
Heartland Breach: Bigger than TJX?
Experts Debate How it Happened and What Damage Could be Done
Linda McGlasson, Managing Editor
January 26, 2009

Exactly how big was the Heartland data breach? This is the great unanswered question since last week, when Heartland Payment Systems (HPY), a Princeton, NJ-based credit card processor, revealed that its computer systems had been breached, and an unknown number of credit card account numbers were exposed to hackers. Since then, at least eight financial institutions have stepped forward to say their customers had cards affected by the breach, and one security expert says, in theory, that Heartland could be bigger than the TJX breach that dominated the news and set the data breach benchmark in 2007.
Example – Malware Delivery

http://charlestonharbourresort.com – Legitimate javascript applet used to detect flash player and has been injected with obfuscated malicious code

A program installs malicious service then deletes itself.
This behavior hides the malware
Even if the initial download is detected, the local service will not be seen via the network.
Wachovia accounts for sale with a minimum balance of $14,000.
...where credentials can be purchased

2800 customers identified from one source in the last few months, sourced from Russian business network

Actual records of malware compromises of the Bank’s customers

Bank’s credit and debit card numbers
Being checked for status and available balances
in preparation for fraud

Source “just buy it” CChecker - Haxtor network
Wireless Vulnerabilities

• **New Trojan Endangers Windows Mobile Devices** – This malware affects Windows Mobile PocketPC devices. The Trojan sends the infected device’s serial number, operating system and other sensitive information to the Trojans’ creators.

• **Security Hole Found in Apple's iPhone** - Hackers could take control of an iPhone if its owner visits a doctored web site or Internet hotspot.

• **Car Whisper** - A Bluetooth mobile phone exploit called “car whisperer” allows hackers to take advantage of default Bluetooth passwords. The hackers sit at a stoplight and snoop information off of your phone.
Collaboration Strategies

• **Identity Theft Assistance Center**
  - Financial Services Roundtable – ITAC – 41+ Members
  - Operational Success – 50,000+ Consumers helped
  - Strategic Success – Credibility and relationships with law makers, regulators, and law enforcement

• **Shared Industry Information**
  - Loss & Operational Metrics
  - VISA IRKI and Mastercard Loss Information
  - Early Warning Services
  - Hot files
  - Internal Fraud Prevention Program (EW/BITS)
  - Shared Social Networks of Fraud
  - BITS, ABA, Financial Services Technology Consortium

• **Cooperative Industry, Law Enforcement & Intelligence**
  - FS - ISAC
  - US Postal Inspection Service; US Secret Service; FBI
  - IRS and various Federal Law Enforcement work groups
Private & Public Cooperation

• *** Joint USSS/FBI Advisory ***

• PREVENTIVE MEASURES
• Over the past year, there has been a considerable spike in cyber attacks against the financial services and the online retail industry. There are a number of actions a firm can take in order to prevent or thwart the specific attacks and techniques used by these intruders. The following steps can be taken to reduce the likelihood of a similar compromise while improving an organization's ability to detect and respond to similar incidents quickly and thoroughly.

• Attacker Methodology:
• In general, the attackers perform the following activities on the networks they compromise:
  • They identify Web sites that are vulnerable to SQL injection. They appear to target MSSQL only.
  • They use "xp_cmdshell", an extended procedure installed by default on MSSQL, to download their hacker tools to the compromised MSSQL server.
  • They obtain valid Windows credentials by using fgdump or a similar tool.
  • They install network "sniffers" to identify card data and systems involved in processing credit card transactions.
  • They install backdoors that "beacon" periodically to their command and control servers, allowing surreptitious access to the compromised networks.
  • They target databases, Hardware Security Modules (HSMs), and processing applications in an effort to obtain credit card data or brute-force ATM PINs.
  • They use WinRAR to compress the information they pilfer from the compromised networks.

• Recommendation 1: Disable potentially harmful SQL stored procedure calls.
Collaboration & Containment Strategies

• Cooperative Industry Ventures & Intelligence Sharing
  Can be powerful BUT
  - Many individual initiatives – often too little connectivity
  - Long start-up times – usually from the beginning with limited trust, credibility, and confidence
  - Sharing of information of value is limited – often one way
  - True value and impact is too often marginal in terms of tangible benefit
  - Lifetime is limited – “often dies on the vine”

• Mutual Authentication
  - Customer to Institution
  - Institution to Customer
  - Institution to Institution
  - Citizen to Government –
  - Government to Citizen/Commerce
Collaboration & Containment Strategies

• Enlisting the Academics – Computer Science
  ▪ CERT - (Carnegie-Mellon University)
  ▪ University of Alabama
  ▪ MIT
  ▪ Many Others

• Other Opportunities – Use The Data To Our Advantage
  ▪ FINCEN – Suspicious Activity Reports (SARS)
    — “Mine the Data” for Identification & Prevention vs. just compliance & law enforcement – “There’s Gold in dem, der hills!”
  ▪ SSA – Blind Verification of SSN to Name
  ▪ IRS – Blind Verification of Personal & Financial Info
  ▪ TBD
Collaboration & Containment Strategies

- **Multi-Factor Authentication**
  - Digital Certificates
  - Tokens - One Time Passwords
  - Challenge Questions – “in Wallet” and “Out of Wallet.”
  - Biometric
  - Device Fingerprinting
  - Adaptive Authentication

- **Hot Listing**
  - IP Black Lists
  - White Lists
  - Shared Industry Hot files

- **Device Signature & Fingerprint**
  - 41st Parameter, RSA, Iovation
  - Hardware & Software plug-ins
What is needed to be successful

• Recognize You Are Dealing With a Protection of Information Issue & likely the need to successfully operate in a “Dirty Environment” - likely at the root is the limitations & shortcomings of Customer Authentication

• Break the Silos — intra-bank; inter-bank; inter-industry; inter-commerce; commerce to government — embrace perspective, learnings, tools, and resources afforded by interdisciplinary approaches

• Time is of the Essence – It’s the 11th Hour — you likely don’t have the time to build it all by yourself from scratch

• Holistic End to End View of the Issues, Problems, & Solutions

• Proactive Investment & Discipline to get your transactional, non-financial, and external data accessible and usable
What is needed to be successful

• Envision & Build “Gauntlets of Protection”
  ▪ Multiple Layers of Protection for product, process, &
    distribution channels and systems
  ▪ Integration of Multiple Point Solutions
  ▪ Integration of Case Management & Prevention Platforms

• Be Aggressive in identifying and attacking criminal
  behavior – know your enemy – know your friends!
  ▪ Detection & Prevention Systems
  ▪ Investigation and Recovery
  ▪ What is the Point of Compromise (POC)? Internal or External –
    who, what, how, when, and why?
  ▪ What are the financial & information recovery
    options?
  ▪ Who are the “other kids on the block”– Allies who are
    adversely affected.? Financial Services, Telecom, Energy, Payments, Merchants.
What is needed to be successful

• Cycle of Continuous Improvement
  ▪ Closed Loop – ID & Measure what is presented for review vs. what is caught and actioned

• Translate into the “language of business” – Return on Investment; True Operational Cost Impacts; etc.