Email Spoofing and Malware; New Variants and Strategies to Avoid Becoming a Victim

October 2014
Agenda

- Fraud Overview
- Phishing and Malware
- Emerging Fraud Landscape
- Employee Awareness & Best Practices
Reuters
Target breach worse than thought, states launch joint probe
By Dhanya Skariachan and Jim Finkle

The New York Times
Neiman Marcus Data Breach Worse Than First Said
By ELIZABETH A. HARRIS, NICOLE PERLROTH and NATHANIEL POPPER

Information Week
Hotel Company Investigates Data Breach, Card Fraud
By Mathew Schwartz

The theft of consumer data from Neiman Marcus appears far deeper than had been disclosed originally, with the luxury retailer now saying that hackers invaded its systems for several months in a breach that involved 1.1 million credit and debit cards.

The malware installed on terminals in Neiman Marcus stores seems to be the same malware that infiltrated Target's systems and exposed information from as many as 110 million customers, according to a person briefed on the investigations who spoke on the condition of anonymity and is not authorized to speak publicly about the attacks.

White Lodging, which manages 168 hotels under Hilton, Marriott, and Sheraton brand names, is investigating a suspected credit and debit card breach.

Update: 2/5/14
White Lodge has named 14 hotels -- as well as some hotel restaurants and lounges -- where "the suspected breach of point of sales systems" occurred, from March 20 to Dec. 16, 2013:
Marriott Midway, Chicago, Ill
Sheraton Erie Bayfront, Erie, Pa
Westin Austin at the Domain, Austin, Texas
Contributors to Online Fraud and Survey Results

- More sophisticated and targeted threats
- Increasing variants of malware and viruses
- Segregation of duties not being implemented
- Not utilizing all the available company, user, account controls
- Opt out of administrative and application controls

AFP Payments Fraud & Control Survey

- On average, 61% of organizations experience attempted or actual payments fraud
  - 73% of organizations that were fraud victims of actual and/or attempted payments fraud experienced no financial loss from payments fraud
  - $20,300 was typical financial loss
- 14% of the organizations were subject to payment fraud attack involving compromised user IDs passwords and other access credentials
Malware Threats – How Fraud Occurs

Anatomy of an attack
User targeted & Malware installed:

- **Phishing & SMiShing**: Infected files/malicious links sent through email or SMS message
- **Drive by Downloads**: Clicking on a document, ad, or video, posted on legitimate website initiates malware download
- Using infected flash drive

Attack is launched and fraud committed:

- Credential theft and/or HTML injection
- Transaction manipulation
Example of Phishing Email

- Look like a legitimate correspondence from the company.
- Wording does not have the level of refinement expected from an authentic company message.
- Has an attention getter – High dollar amount of a cell bill in this case.
- Embedded links activate Malware download on your device.
- Often works whether or not you have a relationship with the company.
Targeted Phishing Example

Federal Government to pay your utility bills

- Staged introductions into different markets.
- Social Media (primary) and Email (secondary) distributed.
- Instructed customers to call a number to receive their government grant.
- Customers provided Utility information, SSN, Bank Account information.
- Fraudster provided Account Number, RT/ABA, and grant confirmation number to be used for government grant.
- Provided customer with bill pay VRU at Utility Company.
- Customer called bill pay phone number and entered information.
- Received notice from Utility Company that payment was returned and account was overdue.

Utility Bill Payment Scam

Scam: Fraudsters claim a government grant will pay your utility bill in full for one month.

Examples: [Collected via e-mail, May 2012]

- My friend just informed me that President Obama is paying her electric bill this month. That supposedly you call and use your $6 as the bank account, then give them the routing number of 061000146 and that's it, it pays for your electric bill but only once a year.

- My daughter called me a couple of days ago asking me if I had already paid my Florida Power & Light (FPL) bill, I told her that I hadn't and she proceeded to tell me that the accounts were being funded by some entity for this month only for Florida residents. I gave her my account information, including SS #. I received a confirmation # from FPL today she calls me to tell me that she had found out this was a scam. She has no idea of how this was distribute, a friend of hers is the one who provided all the information.

Snopes.com
Email Spoofing

Once fraudsters have Malware or Spyware on your computer system:

- Harvest your access credentials; internal systems, financial systems, etc.
- Read your business contacts and collects their information
- Program initiates email to businesses or customers pretending to be you
- Asks the recipient to make a change; receivables account in this case.
- Passively awaits receipt of payment

If you receive a Phishing email such as this:

- Contact the sender by an alternate method
- Follow authentication procedures
- Employ dual controls prior to making payment changes
Online Security Best Practices

Securing Online Transactions

- Be attentive: Are login prompts occurring where they should? Do your online screens look correct?
- Recognize Phishing scams. Do not open file attachments or click links in suspicious emails. Always be on lookout for:
  - Requests for personal information
  - Urgent appeals claiming your account will be closed if you fail to respond
  - Messages about system/security updates
- Avoiding social networking & unknown sites from business computer
- Update your Anti-Virus software, system patches and anti-malware software to protect Internet Browsers
- Prohibit sharing user names/passwords. Avoid using automatic login features that save usernames/passwords
- Never access critical systems from Internet cafes, public libraries or open Wi-Fi hotspots
Emerging Fraud Threats
Mobile is the Next Target

Mobile Fraud
- A growing risk, albeit less than online
- 1,800 mobile strains vs. 75M online
- Online techniques crossing over to mobile
- All of threat vectors not yet known

Physical device security
- Secure mobile device with pin/strong password
- Lock device after use
- Install software to track mobile device in case of theft

Manage system settings, downloads and device software
- Don’t leave Wi-Fi in ad hoc mode
- Disable discoverable mode after enabling Bluetooth devices, if your Smartphone does not automatically default to off after adding a device
- Setup a personal firewall
- Don’t modify the device to:
  - Give yourself more control
  - Enable features that void warranties
  - Change root file systems
  - Allow modifications to install third party software/hardware components
Data Breaches Continue to Make Headlines

**Targeted Information:**
- Customer identifiable information (SSN, Drivers License)
- Account and Payment data

Information stolen from you or a service provider working on your behalf can be used by criminals to commit fraud

**Financial impact:**
- You may be subject to significant fines and losses arising from such fraud and from not properly protecting card account information
- Potential for monetary losses related to a card data compromise
  - Card organization fines and assessments passed through to the merchant
  - Other reimbursements to card issuers for fraud losses passed through to the merchant
- Significant cost to remediate source of Compromise

**Reputation impact:**
Potentially more damaging than the financial impacts, public trust and confidence in your organization can be negatively impacted by this type of data security breach
Payment Card Fraud

In a revenue or receivables environment, watch for Card fraud schemes:

- Often starts with registration of a new account or new service
  - Parking, taxes, registration, utilities
- Card payment is used for deposit or initial payment
  - Newly issued or stolen cards are used
  - Often via online or phone payment processes
- Overpayment is made. i.e. $800.00 for a bill of $80.00
- The perpetrator requests a refund for the “mistaken” over payment. Usually requests a check.

Ensure you have the appropriate controls in your refund processes

- Monitor for new card added to customer profile.
- If payment is made on a card, issue the refund on a card.
- Similar processes should exist for check payments, wait to confirm the check has cleared before issuing a refund for overpayment.
Mitigating Fraud through Appropriate Controls
Layered Security Model

The purpose of layered security is to create controls at multiple points in a transaction process; compromise of one control is compensated for by another.

- Front-end controls; Controls used to authenticate and establish a session into critical infrastructure.
  - User Authentication
  - Device Authentication
  - Two Factor Authentication
- Transaction based controls; Features incorporated into an application to prevent fraud during application processing.
- Entitlements and Administrative Controls
- Two Factor Authentication
- Fraud detection and monitoring
- Customer Education and Awareness; Written, visual and spoken communications to ensure clients recognize cyber/fraud attacks are aware of how to use security tools and features to protect themselves.
Best Practices and Employee Education
Best Practices – Electronic Payments

- Separate duties & audit responsibilities across users to provide additional security
- Set individual user limits appropriate for payment /user
  - Maximum dollar amount at transaction level for initiating/approving payments
  - Maximum daily cumulative dollar amount of all wires initiated and/or approve
- Review Payment Transfer Procedures on regular basis
  - Confirm user credentials updated and maintained to appropriate levels
- Use Repetitive Wire Templates to eliminate manual intervention/manipulation
- Implement ACH Blocks, Filters, ACH Positive Pay, and ACH Authorizations

Best Practices – Paper Payments

- Reconcile accounts daily
- Safeguard check stock/use check stock security features
- Consider outsourcing check processing
- Leverage Positive Pay - Automate review of items before decision to Pay or Return
- Set Maximum Dollar Control - Flag any check over a given dollar amount to decision
There is a direct correlation between employee fraud education and decreased number of successful fraud attacks

**Fraud Awareness Training:**

- Be **proactive** in conducting periodic fraud and security training
- Don’t assume employees understand email and internet risks
- Set rules for **personal internet usage** – tell them why
- Articulate employee policies for the monitoring of their computer activity
- **Formal training:** don’t rely only on your company’s email or intranet to inform employees of email and internet policies and procedures
- Consider restricting the ability to load/download data on your company computers

- Show employees how to recognize threats and convey the consequences of those threats
- Be explicit about what to look for to identify a malicious email
- Explain that users will keep passwords in a secure place and not to share them with coworkers
- Provide frequent reports of new threats and statistics of how many viruses have been caught within your organization
- Never turn off security protection on your computer and stay current with updates
- Do not use your personal computer for company business
- Do not connect to the internet through suspect wireless networks (e.g., Wi-Fi from a café)
- Forward suspicious emails to the company’s designated email security team (include the email address)
- Open only identifiable attachments from known sources. Financial institutions and government agencies never ask you to enter personal data, such as passwords, SSN, account numbers, etc

**Bank of America**

**Merrill Lynch**
Appendix
Glossary of terms

- **Malware** – malicious software; software used or created by attackers to disrupt computer operation, gather sensitive information, or gain access to private computer systems.

- **DDOS** – Distributed Denial of Service – is an attack where multiple compromised systems – which are usually infected with a **Trojan** – are used to target a single system causing incoming traffic to flood the victim.

- **Man In The Browser (MITB)** – a threat related to Man in the Middle where a web browser is infected by a proxy Trojan that allows web pages and transactions to be modified covertly, invisible to both the user and the application.

- **Phishing** – the act of attempting to acquire information such as usernames, passwords, and credit card details (and sometimes, indirectly, money) by masquerading as a trustworthy entity in an **electronic communication**. Phishing emails may contain links to websites that are infected with **malware**.

- **SMishing** – is a form of criminal activity using **social engineering** techniques. SMS phishing uses cell phone text messages to deliver the bait to induce people to divulge their personal information. The hook (the method used to actually capture people’s information) in the text message may be a website URL, but it has become more common to see a telephone number that connects to an automated voice response system.
• **Trojan** – malware Trojan that uses fake pop up ads to force the infected victim to buy malicious software to repair it or any type of drive-by downloads to load bad software.

• **Keystroke Logging** – is the action of recording or logging the keys struck on the a keyboard (to capture user IDs, passwords, etc.)

• **Spyware** – is software that aids in gathering information about a person or organization without their knowledge and that may send such information to another entity without the consumer’s consent, or that asserts control over a computer without the consumer’s knowledge.
These materials have been prepared by one or more subsidiaries of Bank of America Corporation for the client or potential client to whom such materials are directly addressed and delivered (the “Company”) in connection with an actual or potential mandate or engagement and may not be used or relied upon for any purpose other than as specifically contemplated by a written agreement with us. These materials are based on information provided by or on behalf of the Company and/or other potential transaction participants, from public sources or otherwise reviewed by us. We assume no responsibility for independent investigation or verification of such information (including, without limitation, data from third party suppliers) and have relied on such information being complete and accurate in all material respects. To the extent such information includes estimates and forecasts of future financial performance prepared by or reviewed with the managements of the Company and/or other potential transaction participants or obtained from public sources, we have assumed that such estimates and forecasts have been reasonably prepared on bases reflecting the best currently available estimates and judgments of such managements (or, with respect to estimates and forecasts obtained from public sources, represent reasonable estimates). No representation or warranty, express or implied, is made as to the accuracy or completeness of such information and nothing contained herein is, or shall be relied upon as, a representation, whether as to the past, the present or the future. These materials were designed for use by specific persons familiar with the business and affairs of the Company and are being furnished and should be considered only in connection with other information, oral or written, being provided by us in connection herewith. These materials are not intended to provide the sole basis for evaluating, and should not be considered a recommendation with respect to, any transaction or other matter. These materials do not constitute an offer or solicitation to sell or purchase any securities and are not a commitment by Bank of America Corporation or any of its affiliates to provide or arrange any financing for any transaction or to purchase any security in connection therewith. These materials are for discussion purposes only and are subject to our review and assessment from a legal, compliance, tax or accounting perspective, as appropriate, following our discussion with the Company. We assume no obligation to update or otherwise revise these materials. These materials have not been prepared with a view toward public disclosure under applicable securities laws or otherwise, are intended for the benefit and use of the Company, and may not be reproduced, disseminated, quoted or referred to, in whole or in part, without our prior written consent. These materials may not reflect information known to other professionals in other business areas of Bank of America Corporation and its affiliates.

Bank of America Corporation and its affiliates (collectively, the “BAC Group”) comprise a full service securities firm and commercial bank engaged in securities, commodities and derivatives trading, foreign exchange and other brokerage activities, and principal investing as well as providing investment, corporate and private banking, asset and investment management, financing and strategic advisory services and other commercial services and products to a wide range of corporations, governments and individuals, domestically and offshore, from which conflicting interests or duties, or a perception thereof, may arise. In the ordinary course of these activities, parts of the BAC Group at any time may invest on a principal basis or manage funds or an inducement to obtain business or other compensation. We are required to obtain, verify and record certain information that identifies the Company, which information includes the name and address of the Company and other information that will allow us to identify the Company (in accordance, as applicable, with the USA Patriot Act (Title III of Pub. L. 107-56 (signed into law October 26, 2001)) and such other laws, rules and regulations as applicable within and outside the United States.

We do not provide legal, compliance, tax or accounting advice. Accordingly, any statements contained herein as to tax matters were neither written nor intended by us to be used and cannot be used by any taxpayer for the purpose of avoiding tax penalties that may be imposed on such taxpayer. If any person uses or refers to any such tax statement in promoting, marketing or recommending a partnership or other entity, investment plan or arrangement to any taxpayer, then the statement expressed herein is being delivered to support the promotion or marketing of the transaction or matter addressed and the recipient should seek advice based on its particular circumstances from an independent tax advisor. Notwithstanding anything that may appear herein or in other materials to the contrary, the Company shall be permitted to disclose the tax treatment and tax structure of a transaction (including any materials, opinions or analyses relating to such tax treatment or tax structure, but without disclosure of identifying information or, except to the extent relating to such tax structure or tax treatment, any nonpublic commercial or financial information) on and after the earliest to occur of (i) public announcement of discussions relating to such transaction, (ii) public announcement of such transaction or (iii) execution of a definitive agreement (with or without conditions) to enter into such transaction; provided, however, that if such transaction is not consummated for any reason, the provisions of this sentence shall cease to apply. Copyright 2012 Bank of America Corporation.