Practices for Reducing the Risks of Corporate Account Takeovers

Texas Department of Banking
United States Secret Service
January 25, 2012

Reducing Risks of Corporate Account Takeovers

- Presented by:
  - Texas Department of Banking
    - Banking Commissioner Charles G. Cooper
    - Deputy Commissioner Bob Bacon
    - Chief IT Security Examiner Phillip Hinkle
  - United States Secret Service, Dallas Field Office
    - Special Agent Steven Bullitt
- Co-sponsored by:
  - Independent Bankers Association of Texas
  - Texas Bankers Association
  - Moderated by SWACHA
- Corporate Account Takeover is a crime carried out through all financial institutions, regardless of charter

Agenda

- Introduction & Overview
- Description of Corporate Account Takeover and Money Mules
- Special Reviews by Department of Banking
- Standards & Practices for Risk Management of Corporate Account Takeovers
- Questions & Answers

To Ask a Question

- Submit questions at any time using the chat feature on the left side of your screen.

Introduction to Corporate Account Takeovers

- What is Corporate Account Takeover?
- Impacts Businesses, Communities, and Banks
- First significant incident in 2008
- Complex and varied techniques
- Increasing frequency and size of thefts

Overview – Texas Bankers Electronic Crimes Task Force (ECTF)

- Texas Bankers Electronic Crimes Task Force
  - Senior operational executives from diverse group of state-chartered banks
  - IBAT, TBA, and SWACHA
  - Banking Department's Chief IT Security Examiner
  - Secret Service's Electronic Crimes Task Force Special Agent
  - Representatives from Texas Department of Public Safety
- Focused on Corporate Account Takeover
- www.ectf.dob.texas.gov

Texas Bankers ECTF (Continued)

- Task Force Actions
  - Developed “Best Practices” to Reduce Risks
  - Developed Tools & Resources
  - Recommended issuances of the practices to the banking industry
- Department of Banking issued Supervisory Memorandum 1029

Texas Bankers ECTF Recommendations and FFIEC Guidance

- FFIEC Supplemental Guidance on Authentication in an Internet Banking Environment issued June 2011
- Task Force recommendations include the expectations of the FFIEC Supplemental Guidance,
- Task Force recommendations more specific to Corporate Account Takeover
- Special Reviews will begin in March 2012

United States Secret Service
One Agency – Two Missions

Investigations

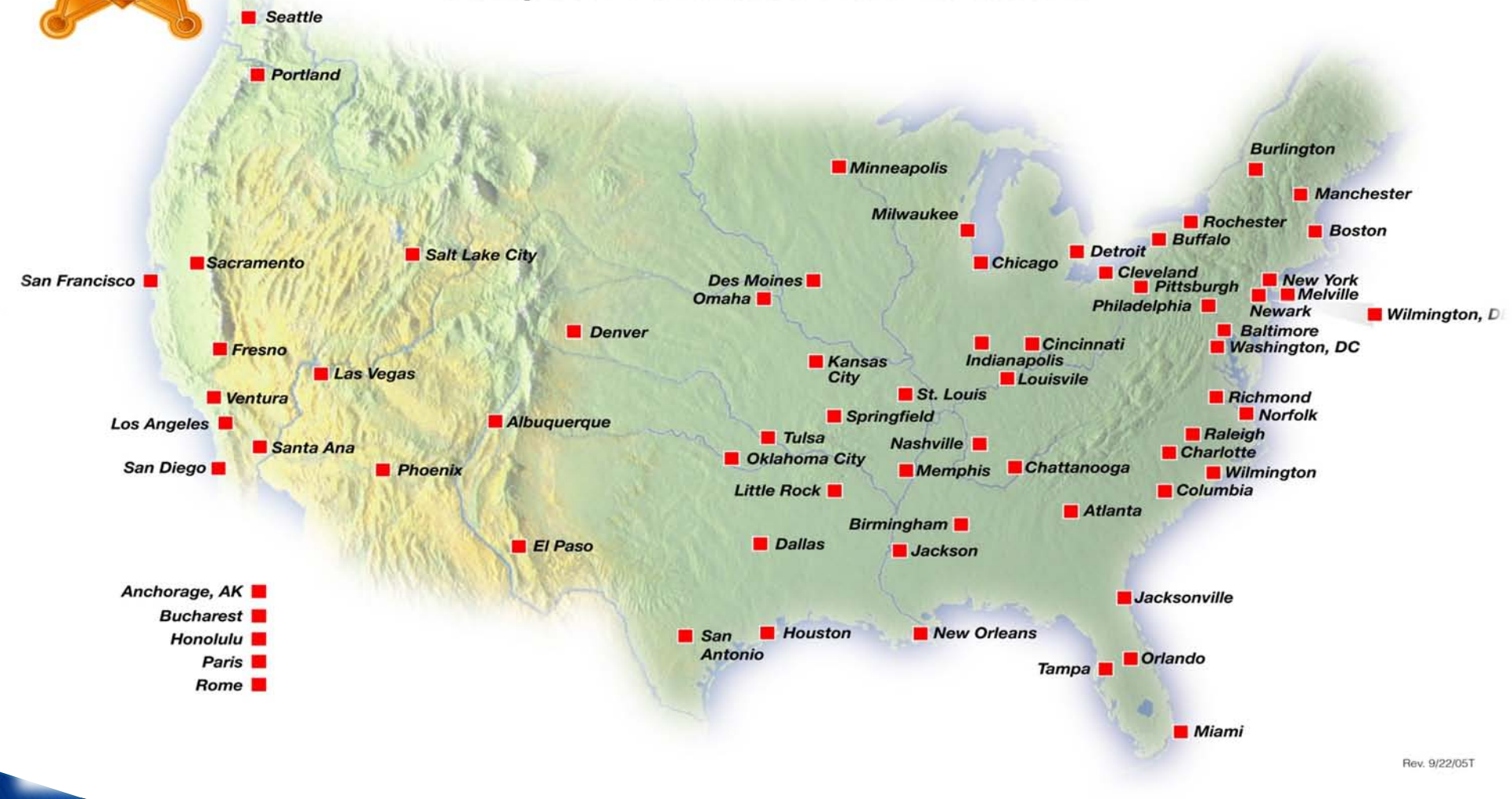
- 1865 – established within Treasury Department to suppress counterfeiting during U.S. Civil War

Protection

- 1902 – formally authorized to protect presidents after 1901 assassination of President McKinley

United States Secret Service

Electronic Crimes Special Agent Program
Computer Forensics Field Locations



USA PATRIOT ACT OF 2001

What Is Corporate Account Takeover?

- Recruitment – Utilize Command & Control network to recruit Money Mules and Target victim companies
- Target – Small to midsized business and organizations
- Infiltration – Attackers utilize numerous tactics to gain access to your network or computer, Banking Trojans
- Exfiltration – Transferring electronic funds out of your account(s) through coordinated effort
- Money Mules – Victims or Suspects/Money laundered.

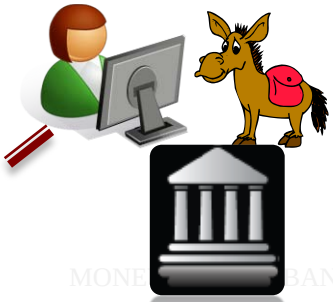
How Does This Scheme Work?

BOTMASTER

STEP 1

THE WORLD WIDE WEB

STEP 5



Money Mule's Bank

STEP 4

TSPY_SPYEYE

VICTIM COMPANY

STEP 2

BOTNET

www.bank.com
Victim Company's bank

STEP 3

How Does This Scheme Work?

BOTMASTER

STEP 1

COMMAND & CONTROL

How Does This Scheme Work?

STEP 2

VICTIM COMPANY

TSPY_SPYEYE.EXEI

COMMAND & CONTROL

How Does This Scheme Work?

STEP 3

VICTIM COMPANY

TSPY_SPYEYE.EXEI

BOTNET

VICTIM COMPANY's BANK

www.bank.com

How Does This Scheme Work?

STEP 4

How Does This Scheme Work?

STEP 5

MONEY MULE

COMMAND & CONTROL

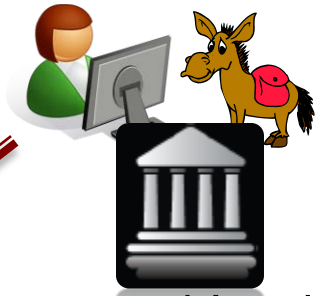
How Does This Scheme Work?

BOTMASTER

STEP 1

THE WORLD WIDE WEB

COMMAND & CONTROL



Money Mule's Bank

STEP 4

TSPY_SPYEYE

VICTIM COMPANY

STEP 2

BOTNET

www.bank.com
Victim Company's bank

STEP 3

Operation Texas Money Mule

- Target Foreign and domestic criminals who are utilizing a series of banking botnets and malware to compromise Online banking accounts
- Utilize the banking system against the criminals
- Utilize the anonymity of the internet against the cyber criminals
- Disrupt the organized market the cyber criminals control

Special Reviews by Department of Banking

- Special Reviews begin in March
- Review implementation efforts on the 19 standards of Protect, Detect, and Respond
- Reviews conducted in phases

Special Reviews (Continued)

- Initial phase
  - Determine if banks have begun working on a risk management program
  - Determine if banks have begun working on a risk assessment
  - Determine if Board of Directors have been informed
  - Answer questions about the standards & practices
- Later phases will measure progress
- Progress will be evaluated on a case by case basis

Standards & Best Practices

- **Supervisory Memorandum 1029** (Standards for Risk Management of Corporate Account Takeovers)
  - Recognized need for banks to Identify, develop, and implement appropriate risk management measures
  - Establishes 19 minimum standards
  - Included in examination program
- **"Best Practices"** can assist in meeting the 19 standards
- www.ectf.dob.texas.gov

Standards & Best Practices

- Protect, Detect, and Respond
  - Co-developed by USSS to help businesses
- "Best Practices" are cross referenced to SM 1029 using Protect, Detect, and Respond
- Page 3 of SM outlines the elements of the Protect, Detect, and Respond framework

Standards for Risk Management Program

Supervisory Memorandum 1029 – Risk Management of Corporate Account Takeovers

The minimum standards for a risk management program to mitigate the risk of Corporate Account Takeover are as follows:

PROTECT

Implement processes and controls to protect the financial institution and corporate customers.

P1. Expand the risk assessment to include corporate account takeover.

P2. Rate each customer (or type of customer) that performs online transactions.

P3. Outline to the Board of Directors the Corporate Account Takeover issues. .....

DETECT

Establish monitoring systems to detect electronic theft and educate employees and customers on how to detect a theft in progress.

D1. Establish automated or manual monitoring systems.

D2. Educate bank employees of warning signs that a theft may be in progress. .....

RESPOND

Prepare to respond to an incident as quickly as possible (measured in minutes, not hours) to increase the chance of recovering the money for your customer.

R1. Update incident response plans to include Corporate Account Takeover.

R2. Immediately verify if a suspicious transaction is fraudulent.

R3. Immediately attempt to reverse all suspected fraudulent transactions. .....

Best Practices for Reducing the Risk of CATO

P1. Expand the risk assessment to incorporate Corporate Account Takeover.

The risk assessment should include risks of Corporate Account Takeovers and be reviewed/updated at least annually for threats and risks related to online payment services. After the risk assessment is updated, an analysis should be made to identify the bank's existing controls that need to be updated or controls that need to be implemented to achieve compliance with regulatory guidance. A sample Corporate Account Takeover risk assessment is available electronically on the Electronic Crimes Task Force page of the Texas Department of Banking website, www.ectf.dob.texas.gov.

An effective risk management assessment should:

1. Define the scope and complexity of the institution's payment and online banking services, noting any changes since the prior risk assessment;
2. Identify what functionality is offered or has changed regarding:
3. Assess if transaction limits have been set within the automated system and if those limits are appropriate;
4. Present a clear understanding of the bank's:

   Customer segmentation; Customer utilization of online banking; and Expected pmnt volumes
5. Assess reliance on third-party service providers for electronic payment processing and delivery…
6. Determine and assess on-going customer education and training practices;
7. Identify and assess all "automated pass-through" payment processing activities …

14. Assess the need for electronic theft insurance. …

"Protect"

- Broad Objectives:

  P1. Include CATO in Risk Assessment

  P2. Identify Higher Risk Customers

  P3. Brief Board on CATO

  P4. Communicate basic security practices

  P5. Provide CATO security education to customers

  P6. Enhance Bank Controls

  P7. Review customer agreements

  P8. Contact Vendors

"Detect"

- Broad Objectives:

  D1. Establish monitoring Systems

  D2. Educate Bank Employees

  D3. Educate Account Holders

"Respond"

- Broad Objectives:

R1. Update Incident Response Plan

R2. Immediately verify suspicious transactions

R3. Immediately reverse fraudulent transactions

R4. Send Fraudulent File Alert

R5. Immediately notify receiving bank(s)

R6. Suspend use of compromised accounts

R7. Contact LE and regulators

R8. Document recovery efforts

Best Practices – Appendices

Appendix A: Resources for Corp Customers

Appendix B: Deceptive Contact Techniques

Appendix C: Incident Response Plans

Appendix D: InfoSec Laws Affecting Businesses

Appendix E: Sample Fraudulent File Alert Request

Tools and Resources webpage

Texas Bankers ECTF

Electronic Crimes Task Force

Home

About the ECTF

Corporate Account Takeovers

Recommendations

Tools and Resources

TOOLS & RESOURCES

The following sample presentations and forms are not endorsed, recommended or required by the Texas Department of Banking.

Presentations on Corporate Account Takeover

Sample for Bank Employees

Sample for Bank Customers

Risk Assessment for Corporate Account Takeover

Sample Risk Assessment

Notice of Fraudulent Activity for Corporate Account Takeover

Sample Notice of Fraudulent Activity

ADDITIONAL RESOURCES

Compliance with Guidance

- Small community banks have said they are looking for help to comply with FFIEC Supplemental Guidance
- Bankers have said that following the broad goals of the "Best Practices" will assist.
- FinCEN requires filing of SAR for attempted Account Takeovers (FIN 2011-A016)

Questions?

Submit questions using the chat feature on the left side of your screen.

Questions that we don't have time to address during this session will be answered and posted on the Department of Banking website with the final webinar materials.

Additionally, you may contact Chief IT Security Examiner Phillip Hinkle with questions after this presentation via phone or email:

(817) 640-4050 or itex@dob.texas.gov

Thank you for joining us!

Contact Department of Banking via email at itex@dob.texas.gov

U.S. Department of Homeland Security

United States Secret Service