Protecting Your Business from Online Banking Fraud

Robert Comella, Greg Farnham, John Jarocki

October 2009

Objective

- According to Brian Krebs of The Washington Post, smaller organizations are suffering significant financial loss when accounting staff are identified and their machines compromised with malicious code that accesses passwords and banking credentials.

- This SANS Technology Institute (STI) Joint Written Project (JWP) will provide guidance organizations can use to mitigate the risk of this attack vector.

Threat Description

- "Organized cyber-gangs in Eastern Europe are increasingly preying on small and mid-size companies in the United States, setting off a multimillion-dollar online crime wave that has begun to worry the nation's largest financial institutions." *Brian Krebs, August 25, 2009*

- Smaller institutions have several disadvantages...
  - Smaller – or non-existent – IT staff and legal teams,
  - Larger bank balances than individuals, and
  - Fewer protections from fraud.

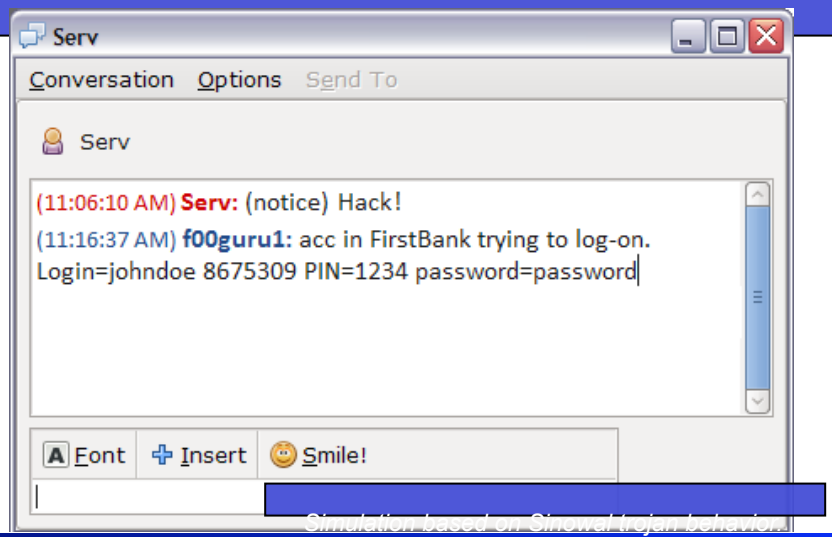
- The Bad Guys have figured this out

The Rise of the Bots

- In 1999, PrettyPark was the first worm to include remote Command and Control (C&C) via Internet Relay Chat. The botnet was born.
- Gradually, bots were sending billions of emails to sell Viagra and Cialis, and to pump and dump stock. Malware was stealing passwords.
- But sometime in the mid-2000's, malware authors learned how to create a lucrative service industry out of crimeware.
- Financial crimeware today is focused on direct theft of banking credentials, fraudulent transfer of funds to "money mules," and even hijacking live online banking sessions with Man-in-the-Browser (MITB) attacks.

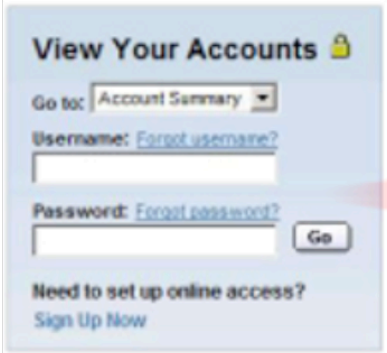
Analysis of Crimeware Features
(at viruslist.com)

"Form grabber. The Trojan intercepts all data entered in a form transmitted via the browser. The list of monitored addresses (to which data relating to will be stolen) is made up, as a rule, of banks and payment systems. This is how payment accounts are stolen."

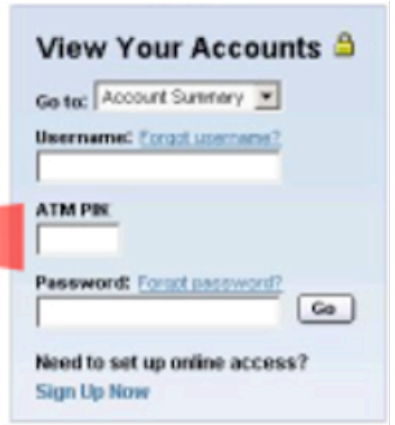


"The contents of the page are modified on the user's computer prior to the page being displayed by the browser."

Before



After



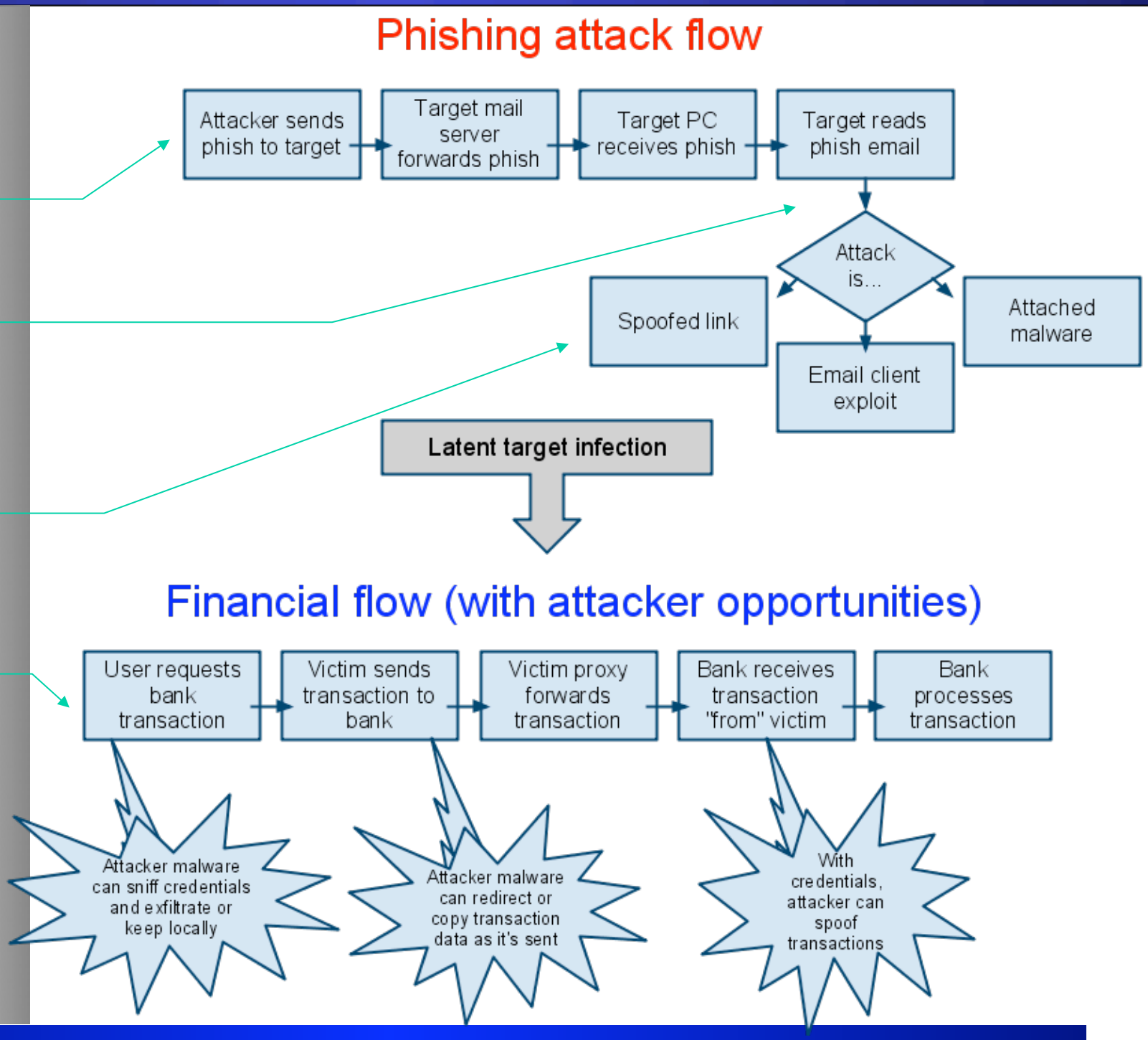
Defensive Opportunities

Protect comptroller email

Network Detection and Protection
- Web Proxy
- Email Gateway
- Detect Outbound Info Loss

Endpoint Protection
- Antivirus
- Reputation Filtering
- Whitelisting Applications

Dedicated Host for Financial Transactions
- Separate host
- Dual Boot
- Virtual Machine
- **ROBAM**
(Read-Only Bootable Alternative Media)



Protect Comptroller Email

- Protecting the finance staff from phishing and email-borne crimeware is key. Consider:
  - Using a separate email account dedicated to banking
  - Running the mail client in a sandbox, like Sandboxie: http://www.sandboxie.com/index.php?EmailProtection
- Most malware is delivered by HTML email or attachments, so also consider:
  - Reading email in plain-text format. Here are instructions: http://www2.slac.stanford.edu/comp/messaging/using/plaintext.htm
  - Saving attachments and reading them with a text editor or at least virus scanning them again manually

Network Protection

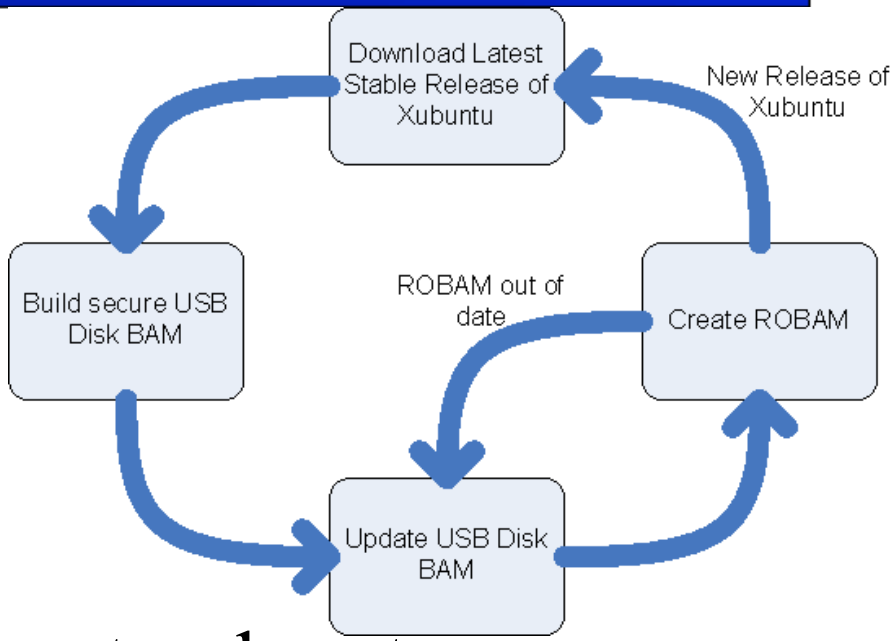
- Use a web proxy:
  - Bluecoat $$; Websense $$; Squid (FREE); DansGuardian (FREE)
  - Explicitly set proxy settings rather than using a transparent proxy
  - Use a whitelist to limit Internet sites your PCs can talk to
- Use a firewall:
  - Block inbound traffic of course, but
  - Also block outbound traffic except from web and email proxy servers
- Then watch the firewall logs!
  - Any outbound traffic not coming from your proxy servers are either misconfigurations... or EVIL
- Tools like BotHunter watch for suspicious activity on your network: http://www.bothunter.net/

Endpoint Protection

- Use antivirus software
  - Signature based as well as behavior based
- Use reputation filtering
  - Block sites on known bad lists
- Whitelist applications
  - Only approved binaries should run on your systems
- Use a dedicated host
  - Separate host, dual boot, virtual machines, or **bootable alternative media** (*see the next slide...*)

Read-Only Bootable Alternative Media (ROBAM)

- A separate computer for banking is a recommended best practice
- But, extra computers cost & software gets out-of-date
- Solution: ROBAM provides a step-by-step process for making bootable CD-ROMs and keeping them up-to-date
- This report includes full details as an Appendix



Monitor Financial Transactions

- Businesses are not alone in fighting fraud
  - Banks have responsibility and motivation as well
  - Most banks have some level of transaction monitoring
- Be aware that businesses don't have the same protection as a consumer:
  - FDIC Regulation E protects consumers from fraud if reported in 60 days
  - Small and medium-sized businesses need to monitor transactions carefully and constantly
- Ask your bank what anti-fraud features they offer
- You might have to pay more for these features, but they are worth it

Training & Security Awareness and Policy Changes

- Avoid risky behavior
  - Don't read email in HTML format first
  - Use a dedicated PC for finances
  - Use extra caution on untrusted networks
- Recognize threats as they are manifested
  - Slow computer; mouse moving by itself; unexpected pop-up windows; suspicious email
- Provide additional training for the Finance staff and Executives who are prime targets
- Policy Changes:
  - As a business becomes larger, information security practices need to be formalized

Summary

- There is a significant threat to Small/Medium Businesses (SMBs) for large financial losses
- SMBs need to recognize the risk and take actions
- A Defense in Depth approach is required
- Several Mitigation Steps are Required
- The top recommendation is to use read-only bootable alternative media (ROBAM) to provide a secure isolated environment for financial transactions