FEDERAL RESERVE BANK of ATLANTA

Regulator's Perspective of Best Practices in Combatting Cybercrime

Executive Fraud Forum
October 30, 2013

Tony DaSilva, AAP, CISA
Senior Examiner
Federal Reserve Bank of Atlanta

FEDERAL RESERVE BANK of ATLANTA

Disclaimer

The views and opinions expressed in this presentation are those of the individual presenter and do not necessarily represent the views and directives of the Federal Reserve Bank of Atlanta, the Federal Reserve System, or the FFIEC. The content of the presentation should not be construed as regulatory guidance.

FEDERAL RESERVE BANK of ATLANTA

Topics

- DoS & DDoS
- Fraud – The Primary Reason
- FFIEC Guidance June 28, 2011
- Requirements
- FRS Guidance
- Best Practices

FEDERAL RESERVE BANK of ATLANTA

Denial of Service Attack

DoS & DDoS

FEDERAL RESERVE BANK of ATLANTA

What is a denial of service attack?

- Objective(s):
  - Render a service unavailable
  - Cripple the infrastructure
- Typical targets:
  - Bank
  - Credit card payment service
- Mode of attack: Saturate the target with external requests for connectivity or communication

FEDERAL RESERVE BANK of ATLANTA

What's the end result?

- Result: Target server is so saturated with attack requests that it cannot respond to legitimate requests
  - Server crashes and reboots
  - Services slow to a crawl or are halted
- Is it a crime?
  - 18 U.S.C. Sect. 1030
  - Felony – 10 years

FEDERAL RESERVE BANK of ATLANTA

DoS Types

- **Bandwidth drain:** The target computer is overwhelmed by the number and size of files being simultaneously sent to it, thereby draining its available Internet connection.

- **Resource drain:** The target computer is inundated with requests, draining its resources to the point where it is no longer able to respond.

FEDERAL RESERVE BANK of ATLANTA

Distributed DoS (DDoS)

- A DDoS attack is performed when hundreds, or possibly thousands, of computers simultaneously request services or bandwidth from the same target computer.

- The attack is executed with networks of computers which are controlled by malicious software which has been installed on a user's computer.

- The antivirus detection rate for botnet malware is less than 40 percent. For additional information, visit: https://zeustracker.abuse.ch/index.php.

FEDERAL RESERVE BANK of ATLANTA

Readily Available Mayhem

- Botnet malware development kits are available for purchase over the Internet.
- The most recent versions may cost less than two thousand dollars.
- Older versions can be obtained for a few hundred dollars for free.
- Botnet administrators also lease their botnets on a per-project basis.
- The DDoS attack application software called Low Orbit Ion Cannon is available for free download from sourceforge.net.

FEDERAL RESERVE BANK of ATLANTA

DoS & DDoS

Denial of Service & Distributed Denial of Service

- Most community banks need to work with their core processors and ISPs to help prevent or at least contain the attack.

- The last thing an administrator wants to deal with is a Distributed Denial of Service (DDoS) attack. Yet, together with the recent rise of hacktivism, DDoS attacks are increasingly becoming a threat that IT admins need to prepared for.

- The worst thing about DDoS attacks is that they do not prey on the victim's weaknesses; therefore being cautious and using the right tools and protection, as in the case of hacking attacks, is not enough.

FEDERAL RESERVE BANK of ATLANTA

DDoS (continued)

- Despite the threat, there's still an effective way to protect your network against these attacks – network design decisions. The only way to protect against this is by having a system to identify the DDoS source and block it.
- This is easier said than done. Identifying the source of a DDoS attack can be tricky and, in most cases, involves tweaking an intrusion detection system (IDS) to differentiate between legitimate requests and attacks. Testing its effectiveness is not easy either. In any case, this will cause quite a few false positives.

FEDERAL RESERVE BANK of ATLANTA

DDoS (continued)

- Once an attack source is identified, all you need to do is configure the Firewall to block that source until the attack stops. Even so, if your Internet bandwidth is overwhelmed by requests, your site will still probably be inaccessible.

FEDERAL RESERVE BANK of ATLANTA

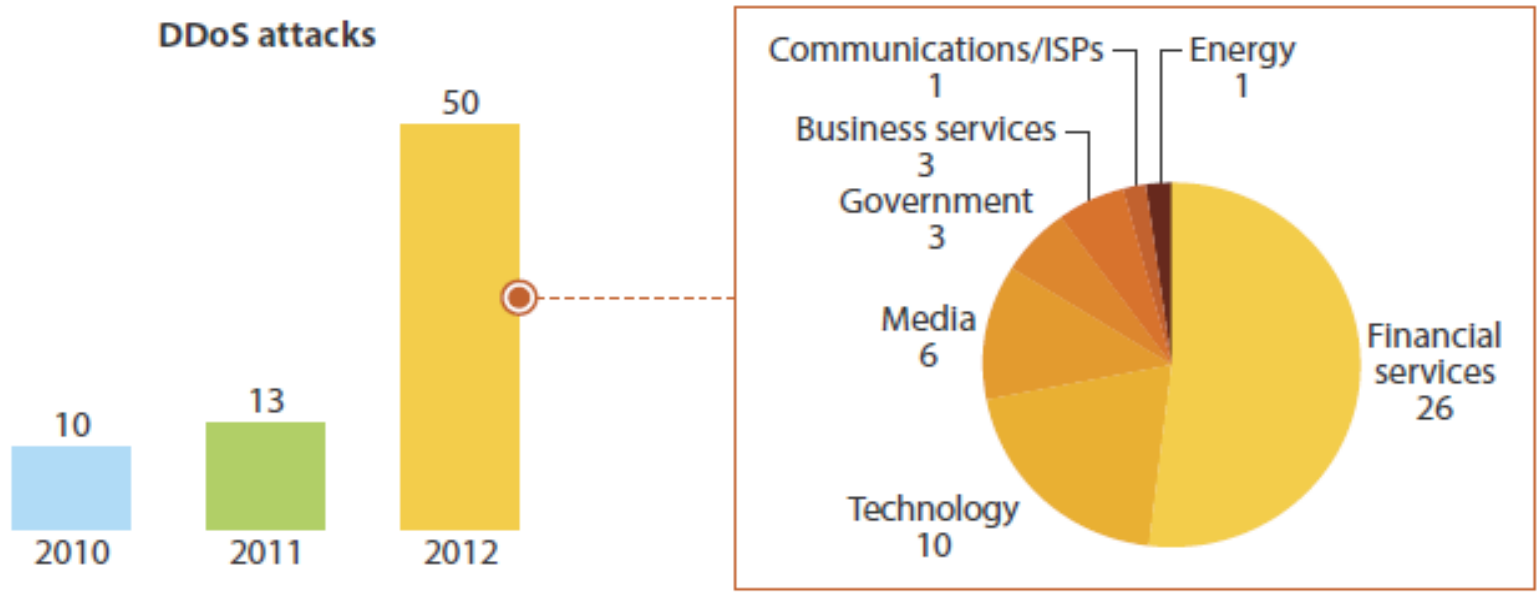
Financial Institution Mitigating Actions

- Targeted banks have been very successful in employing numerous means of thwarting the DDoS attacks.
- There has been unprecedented sharing of information amongst the targeted banks as well as with their regulators and other government agencies.
- Banks are working with service providers to address the problems and to scrub/reduce the attack volumes.
- Leading DDoS protection providers (Prolexic,
- VeriSign, Akamai, etc.)
- Internet Service Providers - AT&T, Verizon, etc.

FEDERAL RESERVE BANK of ATLANTA

DDoS Attacks 2012

Figure 1 DDoS Attacks Are On The Rise



Base: Publicly reported DDoS attacks*

Source: CyberFactors, a wholly owned subsidiary of CyberRiskPartners and sister company of CloudInsure.com
*Countries where these attacks occurred and were reported include: Australia, Brazil, China, France, Germany, India, Myanmar, Russia, Sweden, Thailand, Turkey, the US, and the UK

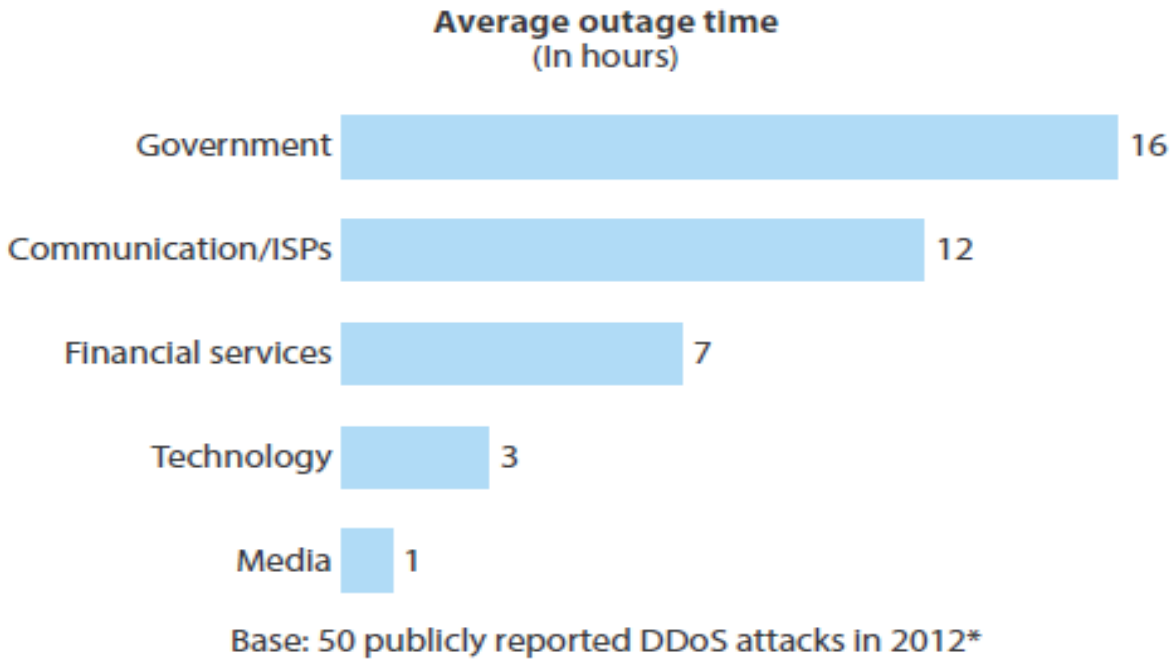
86101

Source: Forrester Research, Inc.

FEDERAL RESERVE BANK of ATLANTA

Average Downtime

Figure 2 Downtime Caused By DDoS In 2012 Varied By Industry



Source: CyberFactors, a wholly owned subsidiary of CyberRiskPartners and sister company of CloudInsure.com
*Countries where these attacks occurred and were reported include: Australia, Brazil, Germany, Myanmar, Russia, Sweden, the US, and the UK

86101

Source: Forrester Research, Inc.

FEDERAL RESERVE BANK of ATLANTA

Developing Concerns

- Bank service providers as possible future targets
  Overload of key service providers attempting to mitigate the effects of DDoS attacks

- Attacks moving down to banks of lower asset size and with potentially less capability for managing the attacks

- DDoS attacks being used as a diversion while fraudulent wire transfers are being transmitted

FEDERAL RESERVE BANK of ATLANTA

Payments Cybercrime

ACH & Wire Transfers

FEDERAL RESERVE BANK of ATLANTA

Technology Enabling Fraud

As payments have evolved significantly, largely due to technological advancements, so has the sophistication of EFT fraud. Expertly crafted emails, malicious links on legitimate websites (such as social networking sites), and other methods are used to place malware within the networks of corporate customers. The malware then harvests security information, including login credentials, subsequently allowing the criminals to initiate electronic payments through hijacked accounts.

FEDERAL RESERVE BANK of ATLANTA

Just a Few Examples

- SpyEye– A Zeus variant that “wakes-up” and steals credentials in real time.
- OddJob–Keeps online sessions open after logout by the user
- Tatanga– Caused a screen freeze or displays a “please wait” message as it conducts transactions in the background.
- Zeus Mitmo– Steals SMS one-time passwords via Social Engineering. Can utilize Smishing to get user to download malware that forwards SMS messages
- Ramnit Worm – It was paired with source code from the Zeus botnet, and began targeting financial institution and has the ability to “bypass two-factor authentication and transaction signing systems.

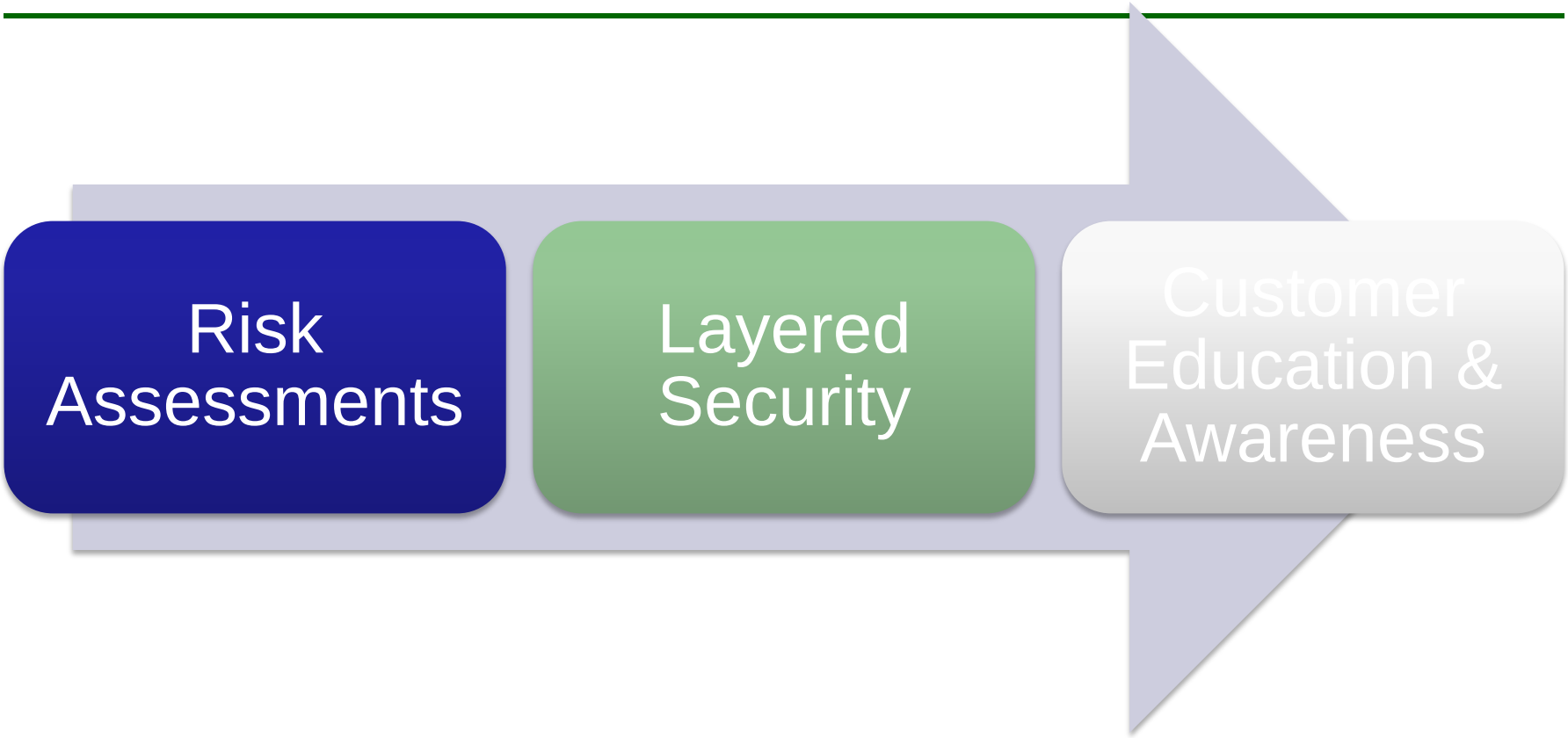
The FFIEC Guidance Supplement

Effective 1/1/2012:

On June 28th, 2011 the Federal Financial Institutions Examination Council FFIEC) released a supplement to the 2005 “Authentication in an Internet Banking) Environment” guidance that describes the measures financial institutions should take to protect Internet banking customers from online fraud.

FEDERAL RESERVE BANK of ATLANTA

Three Primary Requirements



FEDERAL RESERVE BANK of ATLANTA

FRS Guidance

- In recognition of the constant evolution in online threats, institutions should review and update risk assessments prior to implementing new electronic financial services or at least every twelve months.

- Institutions should implement a layered approach to security for high risk Internet-based transactions (i.e. access to sensitive customer information and/or movement of funds to other parties), including at a minimum processes to detect and respond to anomalous or suspicious behavior relating to initial login and to transactions that transfer funds to other parties.

FEDERAL RESERVE BANK of ATLANTA

FRS Guidance

- For business/commercial online accounts, layered security at a minimum should include enhanced controls for users granted access or change permissions to administrative and configuration functions.

- Institutions' customer awareness and education programs should clearly explain the applicability of Regulation E protections to each account type accessible over the Internet. Further, institutions should take steps to see that customers are informed of security control options and alternatives.

FEDERAL RESERVE BANK of ATLANTA

Note

None of the supplement's risk management expectations are specific mandates, nor does the supplement promote any specific automated or manual technologies or processes. An individual institution's control environment should be a function, in part, of the characteristics, size, and nature of its activities and customers.

FEDERAL RESERVE BANK of ATLANTA

Note

- Similar to the 2005 guidance, the June 2011 supplement applies to all electronic banking delivery channels, including the mobile banking channel.

- Whether financial institutions provide all or part of their electronic banking activities to customers through in-house systems or outsourced, service-provider arrangements, the institutions are responsible and accountable for conformance with the 2005 guidance and the 2011 supplement.

FEDERAL RESERVE BANK of ATLANTA

Specific Practices to Mitigate Risks

- To mitigate some of the risk of fraudulent transactions, bank management should consider the following risk management practices:
- Assess risks and implement technologies that address current threats (many strong authentication technologies have been compromised)
- Deploy robust, multi-factor authentication;
- Use out-of band authentication methods (i.e., call backs, text messages) to documented contacts;
- Implement layered security (defense-in-depth) for high-risk transactions;

FEDERAL RESERVE BANK of ATLANTA

Specific Practices to Mitigate Risks

- Ensure centralized fraud detection systems facilitate monitoring across payment channels (i.e., ACH transactions, wire transfers, cards, checks, ATM transactions);
- Review security provisions in customer agreements (agreement alone may not alleviate bank from liability);
- Implement procedures for monitoring new and existing accounts (for new accounts, monitor for ACH credits "money mule activity");

FEDERAL RESERVE BANK of ATLANTA

Specific Practices to Mitigate Risks

- Disallow ACH debits unless specifically approved by customer;
- Regularly review ACH customer exposure limits (be aware that LOCs may increase potential funds accessible to criminals);
- Consider having the ACH Operator implement a threshold amount for origination;
- Implement transaction risk profiling;

FEDERAL RESERVE BANK of ATLANTA

Specific Practices to Mitigate Risks

- Monitor debit transaction returns including bill payment accounts;
- Implement third-party service provider governance and due diligence;
- Provide customers with robust account activity monitoring/ alerting tools; and
- Focus on strong customer education regarding information security management requirements and monitoring practices.

FEDERAL RESERVE BANK of ATLANTA

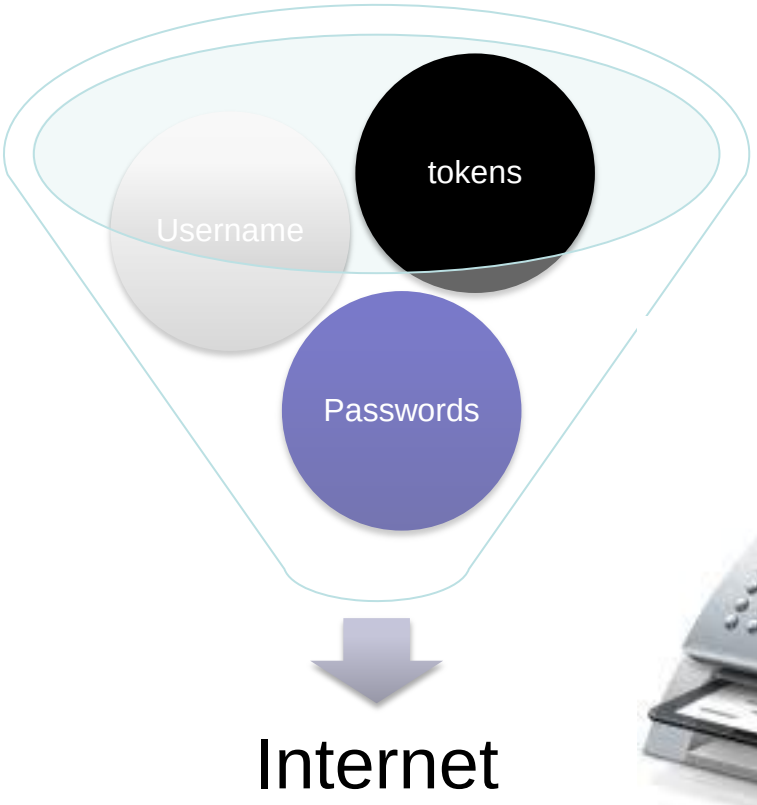
Specific Practices to Mitigate Risks

Some points for banks to consider emphasizing in customer education include:

- Use of a single purpose, stand-alone computer for Internet banking (no email/web surfing/downloading);
- Monitor accounts daily for unusual activity – notify FI immediately of any errors;
- Implement dual controls and separation of duties;
- Maintain up-to-date anti-virus, spyware and firewall protection;
- Use the strongest form of authentication provided by the bank; and,
- Apply security patches quickly, consistently and comprehensively.

FEDERAL RESERVE BANK of ATLANTA

Out-of-Band



FEDERAL RESERVE BANK of ATLANTA

For More Information

- FBI Alert: Fraudulent ACH Transfers
  http://www.fbi.gov/pressrel/pressrel09/ach_110309.htm
- FDIC Special Alert: Fraudulent Electronic Funds Transfers
  http://www.fdic.gov/news/news/SpecialAlert/2009/sa09147.html
- FDIC Special Alert SA-185-2009 Fraudulent Funds Transfer Schemes
  http://www.fdic.gov/news/news/SpecialAlert/2009/sa09185.html
- NACHA Bulletin: Corporate Account Takeovers
  http://www.nacha.org/docs/NACHA%20Operations%20Bulletin%20-%20Corporate%20Account%20Takeover%20-%20December%202,%202009.pdf

FEDERAL RESERVE BANK of ATLANTA

For More Information

- FFIEC Guidance Authentication in an Internet Banking Environment
  http://www.ffiec.gov/press/pr101205.htm
- Identity Theft Red Flags Rule
  http://www.federalreserve.gov/BoardDocs/srletters/2008/SR0807.htm
- FDIC Guidance on Mitigating Risks from Spyware
  http://www.fdic.gov/news/news/financial/2005/fil6605.html
- Interagency Guidelines Establishing Information Security Standards (GLBA)
  http://www.federalreserve.gov/bankinforeg/interagencyguidelines.htm