Challenges in Business Banking Authentication

- A Bank's Perspective

John Walp, CISSP, CISM
M&T Bank - Administrative Vice President and CISO

M&T Bank
Understanding what's important®

Problem: The Threat Has Changed

- Cybercrime: Well funded, state sponsored and increasingly sophisticated
- Castle and Moat Approach To Security Is No Longer Valid as Attackers Focus on Consumer PCs
- Traditional Client-side Controls failing – Anti-Virus, Firewalls are not enough
- Consumers and SMBs are at a Disadvantage and most are unaware of the sophistication of the Threat

M&T Bank

Problem: Cybercrime is profitable

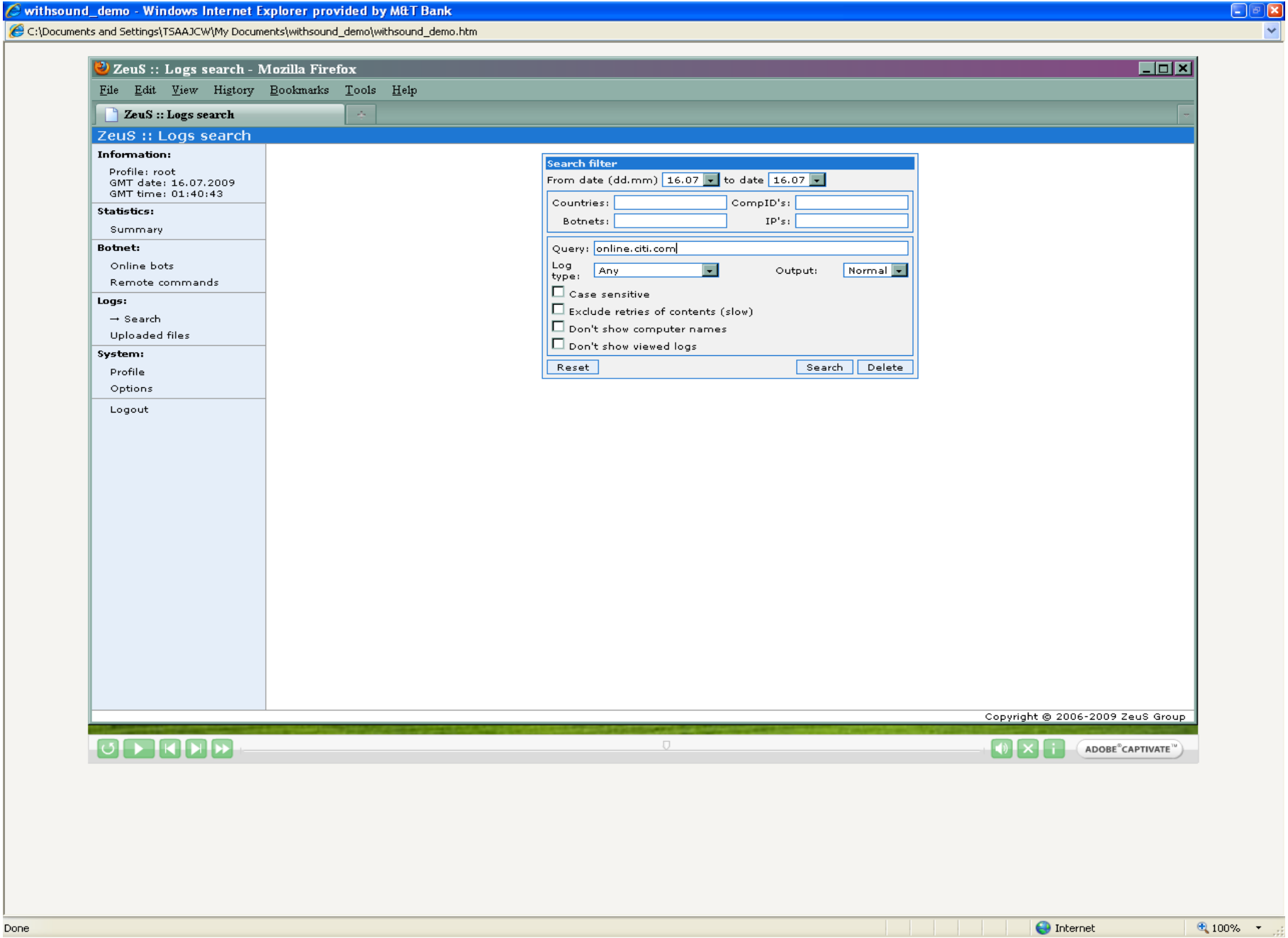
- Heartland Payment Systems
  - Est. 130 million cards compromised
- Hannaford – 4.6 million cards compromised
- RBS WorldPay - $9 million in 12 hours from 2,100 ATMs in 280 cities worldwide
- ACH and Wire Fraud – $120 million (est.) in 2009

Problem: Law Enforcement & Education

- Shortage of forensic skills needed to investigate and gather evidence related to cybercrime
- More collaboration and information sharing needed in order to counter the social-media-aware threat
- Cross-channel nature of frauds makes investigations and evidence gathering increasingly complex
- Cyber Security Awareness of majority of online population is sorely lacking and aids attackers

Problem: Trojan Horse

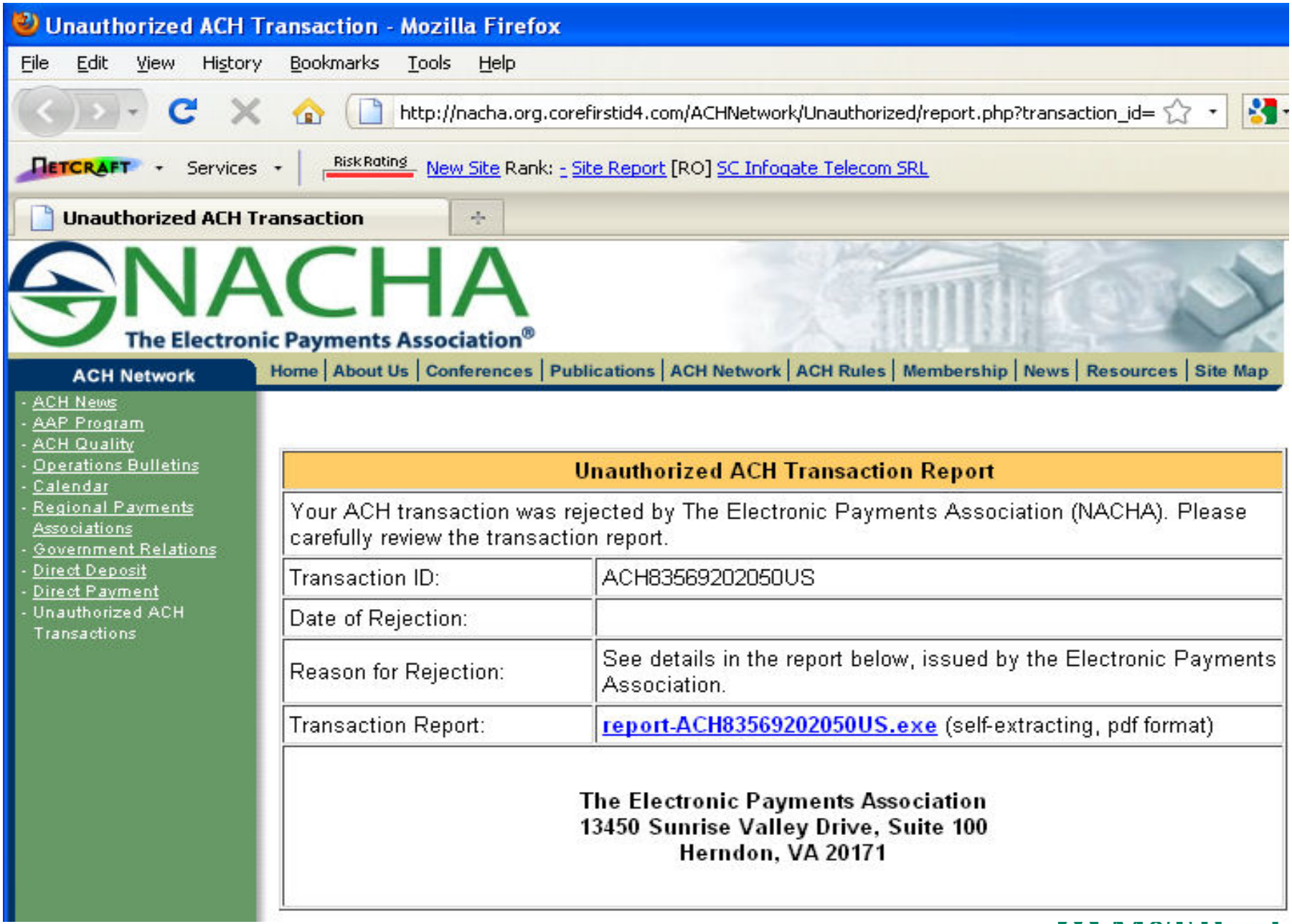
M&T Bank


withsound_demo - Windows Internet Explorer provided by M&T Bank
C:\Documents and Settings\TSAAJCW\My Documents\withsound_demo\withsound_demo.htm
ZeuS :: Logs search - Mozilla Firefox
File Edit View History Bookmarks Tools Help
ZeuS :: Logs search
ZeuS :: Logs search
Information:
Profile: root
GMT date: 16.07.2009
GMT time: 01:40:43
Statistics:
Summary
Botnet:
Online bots
Remote commands
Logs:
→ Search
Uploaded files
System:
Profile
Options
Logout
Search filter
From date (dd.mm) 16.07 to date 16.07
Countries:
CompID's:
Botnets:
IP's:
Query: online.citi.com
Log type: Any
Output: Normal
Case sensitive
Exclude retries of contents (slow)
Don't show computer names
Don't show viewed logs
Reset
Search
Delete
Copyright © 2006-2009 ZeuS Group
ADOBE CAPTIVATE
Done
Internet
100%

M&T Bank

Challenges with Authentication

- Fraudsters understand business process and structure transactions to avoid detection
- Transactional behavior modeling is only part of the solution as “normal” can change over time
- Velocity Checking and IP Geo-location controls are easily fooled by proxy-aware trojans and root kits
- Global nature of business can lead to false positives as more transactions are originated internationally


Unauthorized ACH Transaction - Mozilla Firefox
File Edit View History Bookmarks Tools Help
http://nacha.org.corefirstid4.com/ACHNetwork/Unauthorized/report.php?transaction_id=
NETCRAFT Services Risk Rating New Site Rank: - Site Report [RO] SC Infogate Telecom SRL
Unauthorized ACH Transaction
NACHA
The Electronic Payments Association®
ACH Network
Home | About Us | Conferences | Publications | ACH Network | ACH Rules | Membership | News | Resources | Site Map
- ACH News
- AAP Program
- ACH Quality
- Operations Bulletins
- Calendar
- Regional Payments Associations
- Government Relations
- Direct Deposit
- Direct Payment
- Unauthorized ACH Transactions
Unauthorized ACH Transaction Report
Your ACH transaction was rejected by The Electronic Payments Association (NACHA). Please carefully review the transaction report.
Transaction ID: ACH83569202050US
Date of Rejection:
Reason for Rejection: See details in the report below, issued by the Electronic Payments Association.
Transaction Report: report-ACH83569202050US.exe (self-extracting, pdf format)
The Electronic Payments Association
13450 Sunrise Valley Drive, Suite 100
Herndon, VA 20171

M&I Bank

Critical Update

Update for Microsoft Outlook / Outlook Express (KB910721)

Please download and install the file:

officexp-KB910721-FullFile-ENU.exe

Brief Description

Microsoft has released an update for Microsoft Outlook / Outlook Express. This update is critical and provides you with the latest version of the Microsoft Outlook / Outlook Express and offers the highest levels of stability and security.

Quick Details

- File Name: officexp-KB910721-FullFile-ENU.exe
- Version: 1.4
- Language: English
- File Size: 81 KB

System Requirements

- **Supported Operating Systems:** Windows 2000; Windows 98; Windows ME; Windows NT; Windows Server 2003; Windows XP; Windows Vista
- **This update applies to the following product:** Microsoft Outlook / Outlook Express

M&T Bank

Solution: People, Process, Technology

- Make customers, employees, students aware of the real and rapidly growing cyber security threat
  - **“America's economic prosperity in the 21st century will depend on cyber security,” President Barack Obama**
- Encourage customers to buy fraud prevention services (ACH block, payee positive pay, etc.)
  - Consumers: Must practice good Internet Hygiene
  - Banks: Know Your Customer
- Liaison with peers, law enforcement and academia
- Use isolated, separate PC with restricted admin privileges for all financial transactions