
# Where Online Fraud Is Going

## Emerging Threats & Changing Fraud Patterns

Sam Curry
Vice President Product Management & Strategy
*RSA, The Security Division of EMC*

# Things to Ponder……..

- One identity = new keys to the kingdom?
- We're combating fraud together!
- Are you prepared for emerging threats?
- Thinking beyond web portal "identity"

RSA
The Security Division of EMC

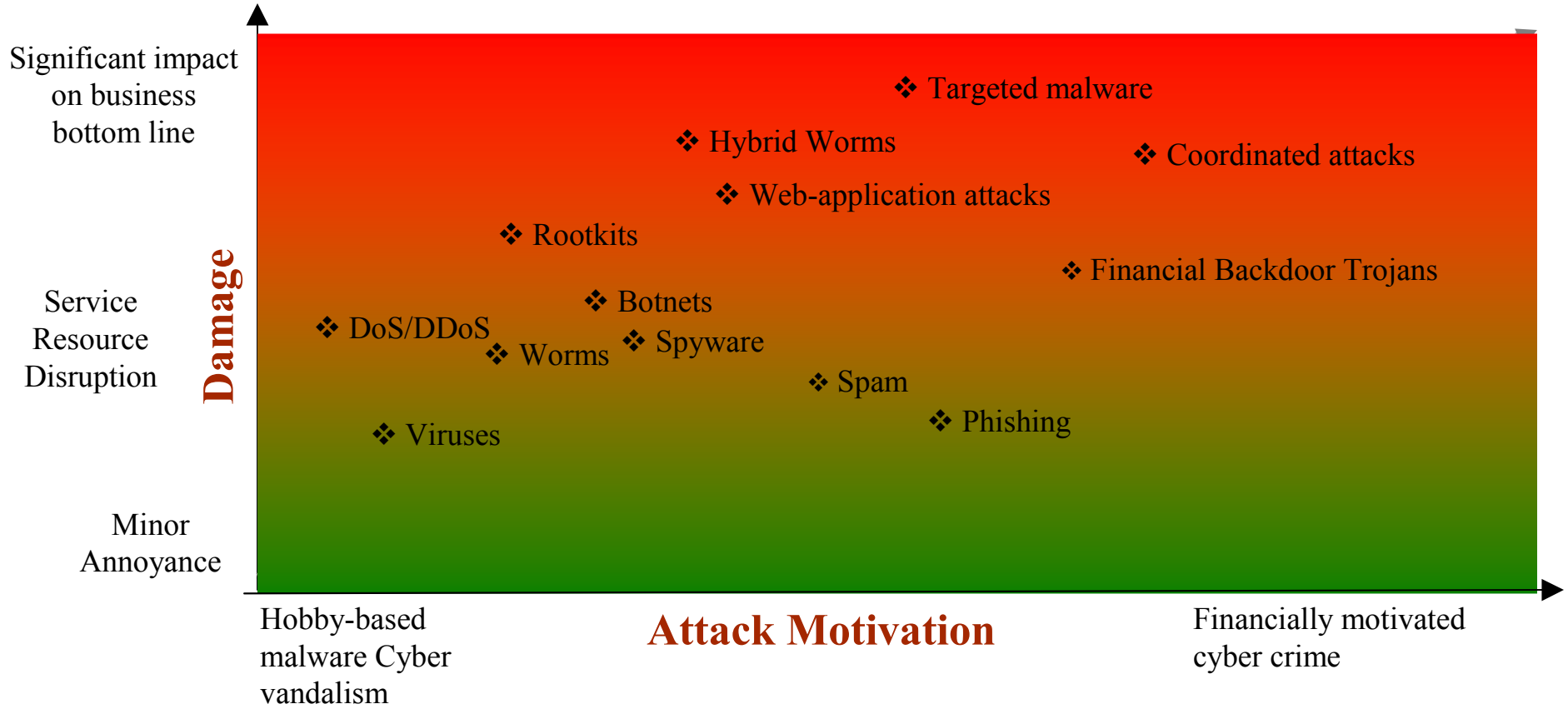
# The Good News….

Federated Identity gives you:

- ☑ Less points to secure and authenticate
- ☑ Centralized identity & audit controls
- ☑ Ability to initially pinpoint fraud up front
- ☑ Less personal data distributed amongst providers

# The Bad News…

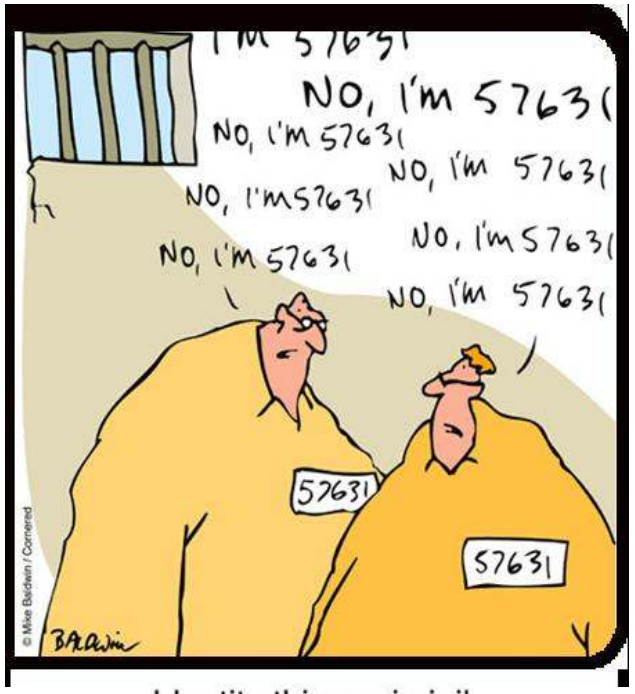
**Just when we thought we figured it out….*it keeps changing!***




RSA
The Security Division of EMC

# Fraudulent Enrollment & Origination

- Enrolling offline users to online account
  - Long-time customers
  - Most vulnerable
    - Elderly
    - Poor
    - People without Internet access
- New account fraud
  - Use false/synthetic identities
    - Information does not match real person
    - Created on the spot or developed over years
  - Use well-known sites for identity theft
    - Person assumes identity of real individual (dead or alive)
  - Use as a “mule account”
  - Understand how site security works




Identity thieves in jail

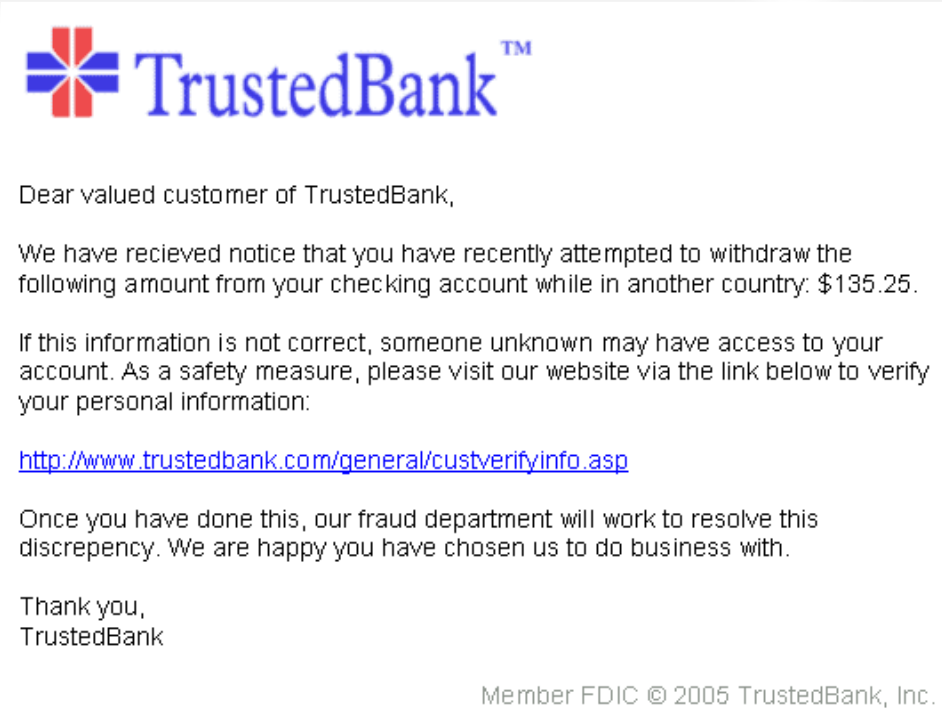
# One Identity = One Stop Shopping?
## *What will be the new "Keys To The Kingdom"?*

- SSNs – old keys to the kingdom
  - never intended for authentication ➔ used for identity
- DarkMarket FBI sting shut down notorious Russian Fraudster selling SSN automatic checker
- Fraudster underground commonly sell SSN – **WHAT NEXT?**


RSA
The Security Division of EMC

# Emerging Authentication & Authorization Threats?

- Phishing
- Malware
  - Trojans
  - Man-in-the-browser (MITB)
- Distribution Tools



TrustedBank™

Dear valued customer of TrustedBank,

We have recieved notice that you have recently attempted to withdraw the following amount from your checking account while in another country: $135.25.

If this information is not correct, someone unknown may have access to your account. As a safety measure, please visit our website via the link below to verify your personal information:

http://www.trustedbank.com/general/custverifyinfo.asp

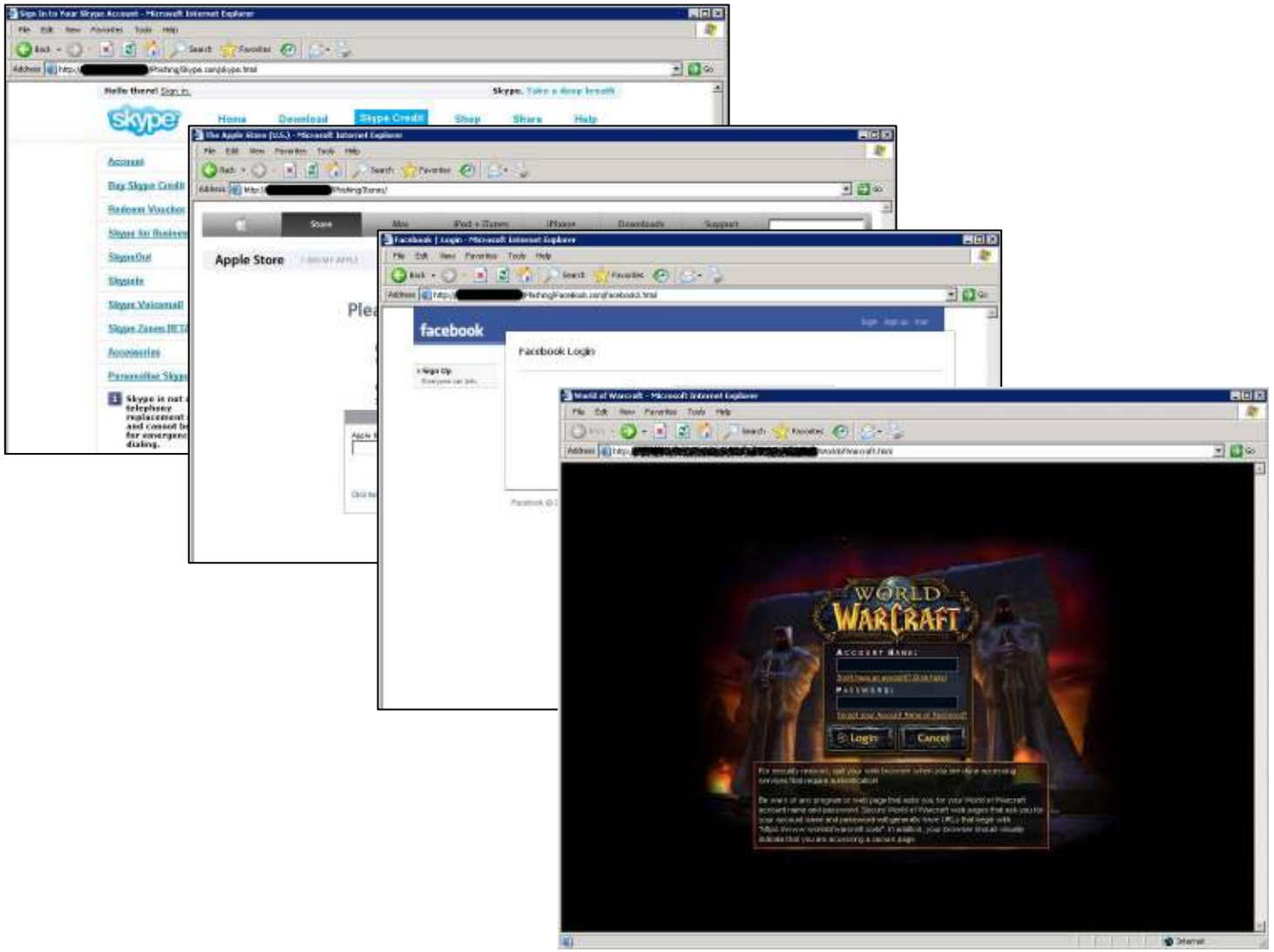
Once you have done this, our fraud department will work to resolve this discrepency. We are happy you have chosen us to do business with.

Thank you,
TrustedBank

Member FDIC © 2005 TrustedBank, Inc.

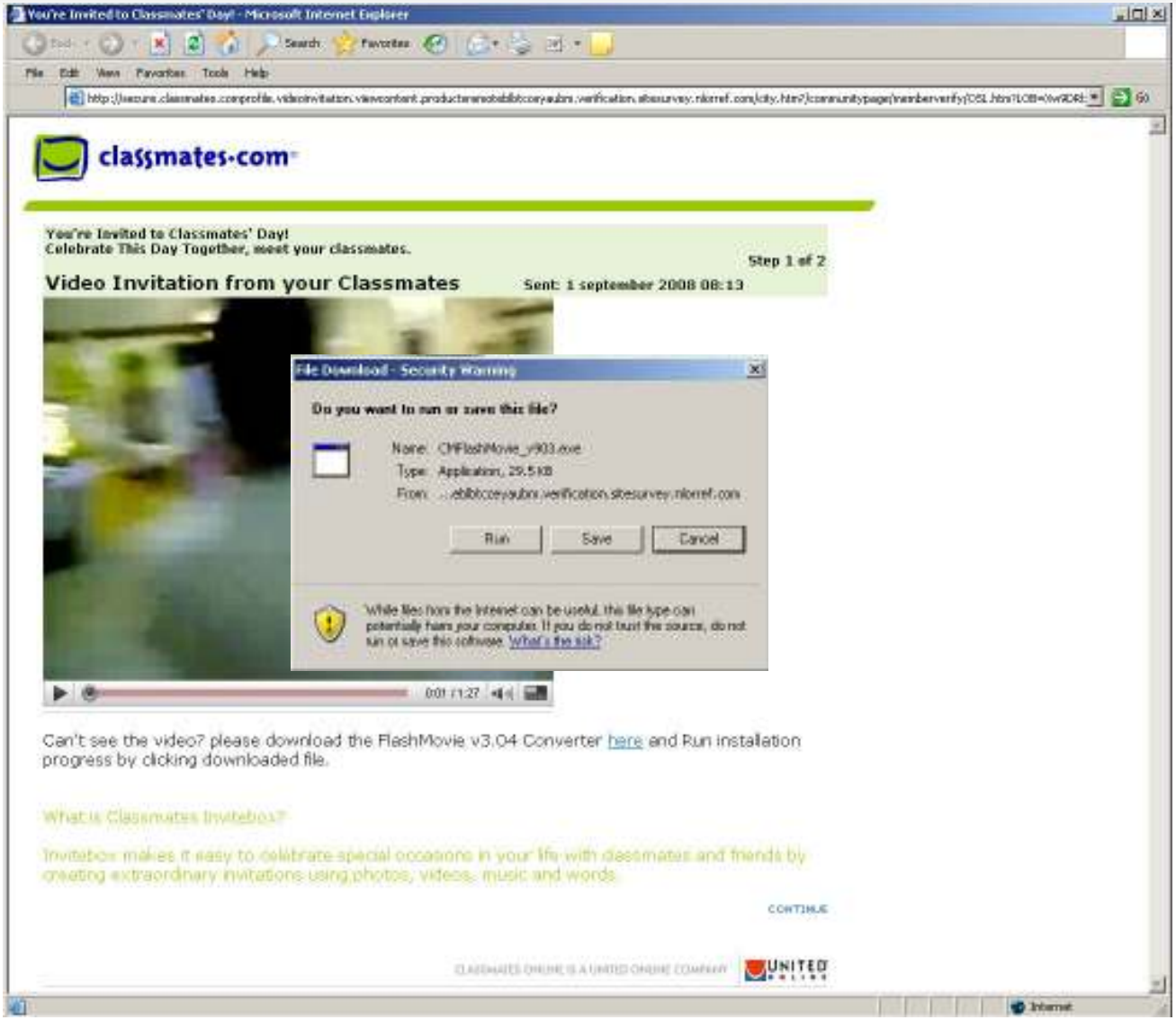
RSA
The Security Division of EMC

# Phishing: Diversifying Targets



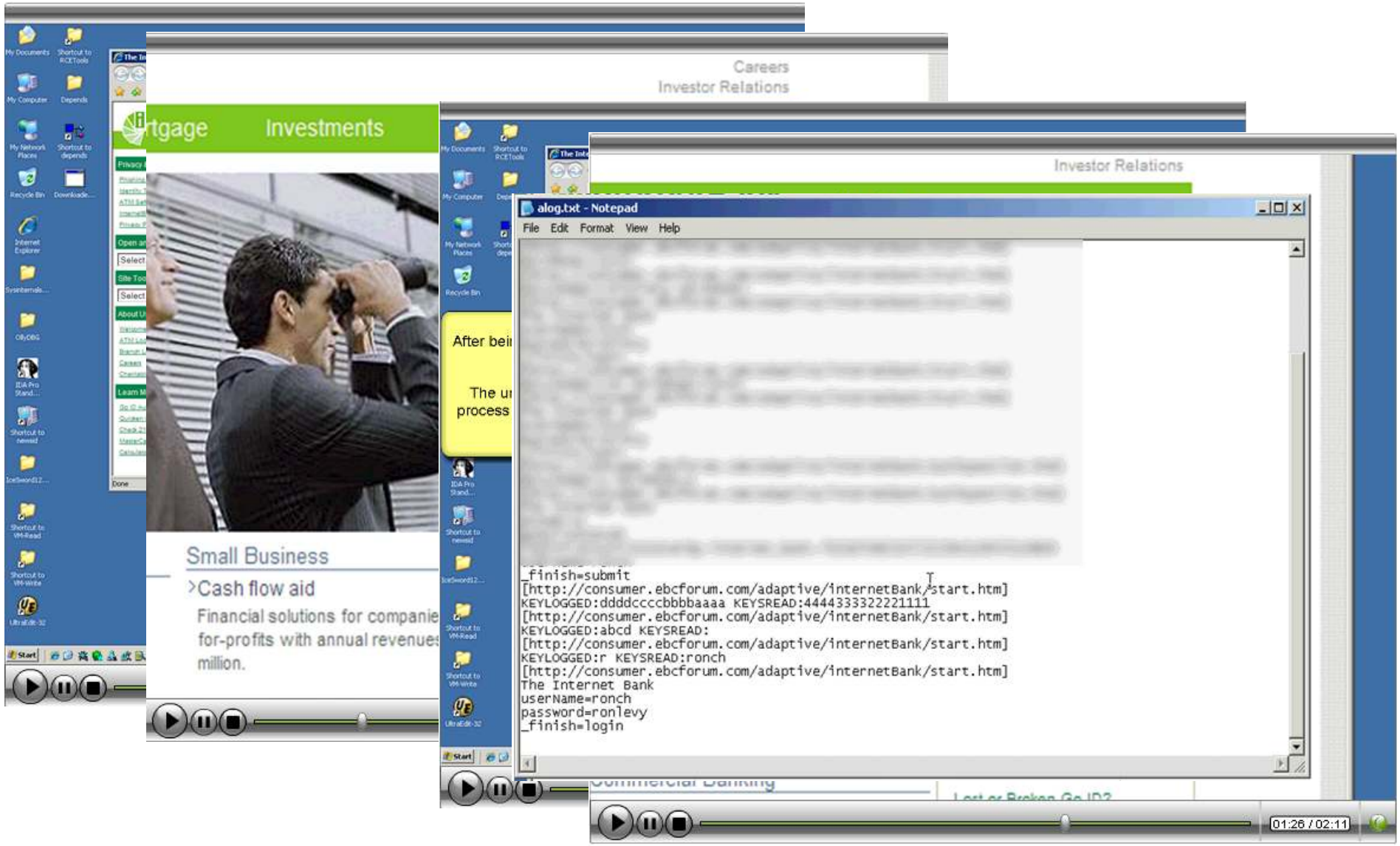

RSA
The Security Division of EMC

# Blend of Phishing and Crimeware



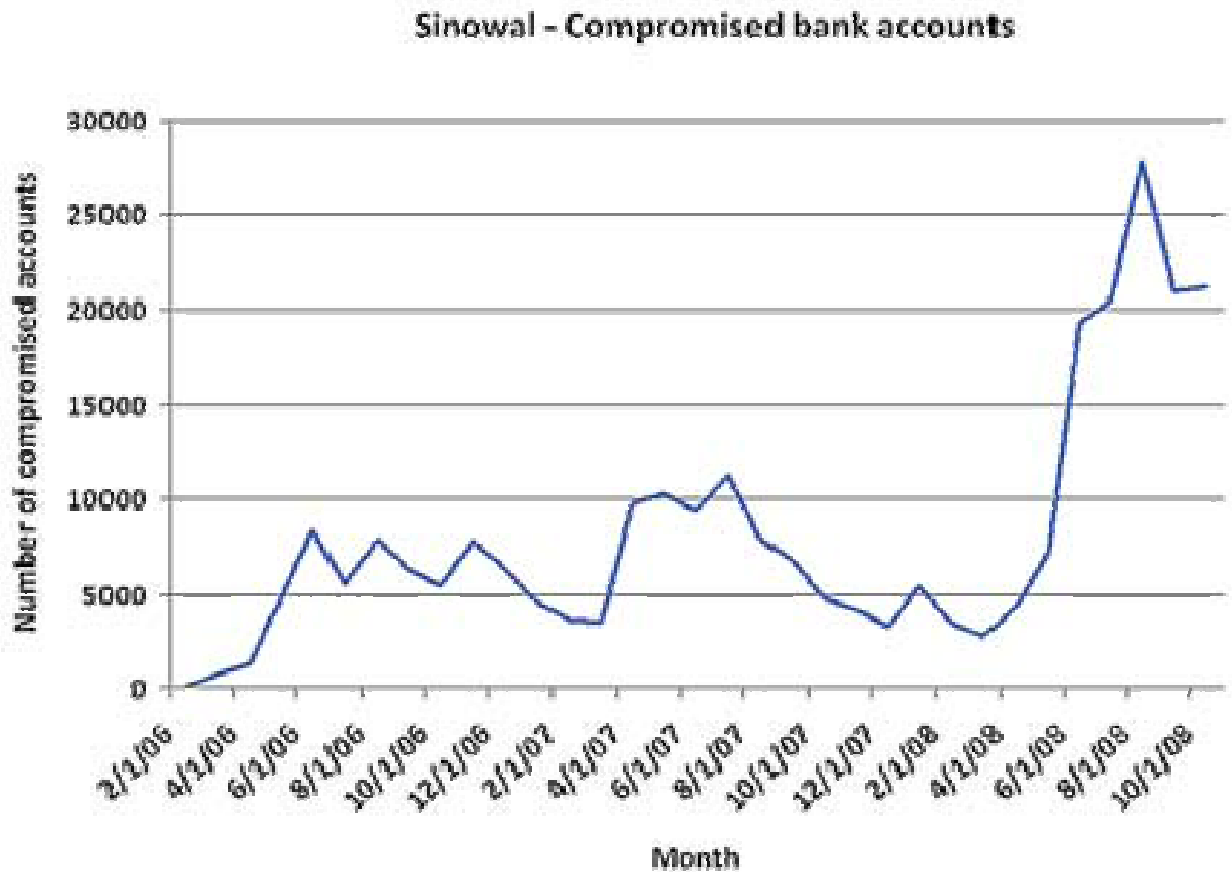

RSA
The Security Division of EMC

# A Basic Trojan Attack



# Sinowal Trojan

- **Over 500,000 Compromised Credentials since 2006**
- **More than 2,000 Bank Domains impacted, non-financial institutions impacted as well**




RSA
The Security Division of EMC

# How Is Malware Distributed?

## Cease-Fire Trojan Attack

- Social engineering scam designed to lure people, via an email spam attack to fake news website designed to look like CNN.com.
- Near real-time response to breaking news
- Similar to other social engineering attacks


Israel offers short respite from strikes
Israel will halt its bombardment of Gaza for three hours every day to allow residents of the Hamas-ruled Palestinian territory to obtain much-needed supplies, a military spokesman says. The images broadcast here were graphic and striking. The Al Jazeera English report below captures the extent of the devastation caused by the initial strikes.
http://edition.cnn.2009.WORLD.meast.01-07.bigvideo.2009.israel_and_gaza israel-gaza.htm

2009 Cable News Network. A Time Warner Company. All Rights Reserved.

s

RSA
The Security Division of EMC

# Fraud-as-a-Service
## *We need to combat fraud together!*


*"You know, you can do this just as easily online."*

RSA
The Security Division of EMC

# Fraud-as-a-Service
## Example: Universal MITM Phishing Kit

Genuine domain

- "Universal": *Any* entity can be readily targeted

VVhymybrand

Whymybrand.com

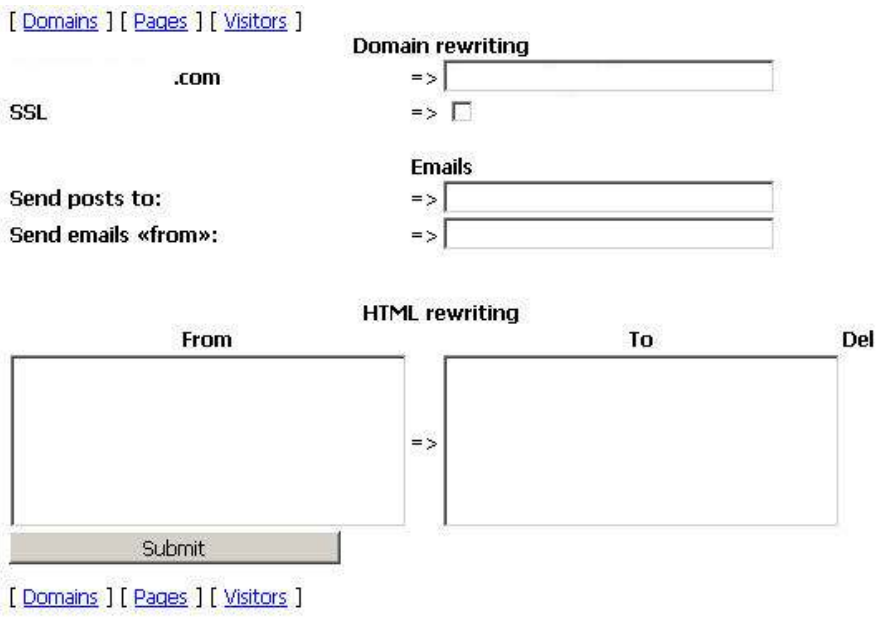
Spoofed Domain

- Sophist hing-based MITM attacks easy to implement
- Compelling: After unsuspecting user clicks on link, genuine site is referenced via proxy

Iamathief@fraudster.com

Rollingindough@fraudster.com

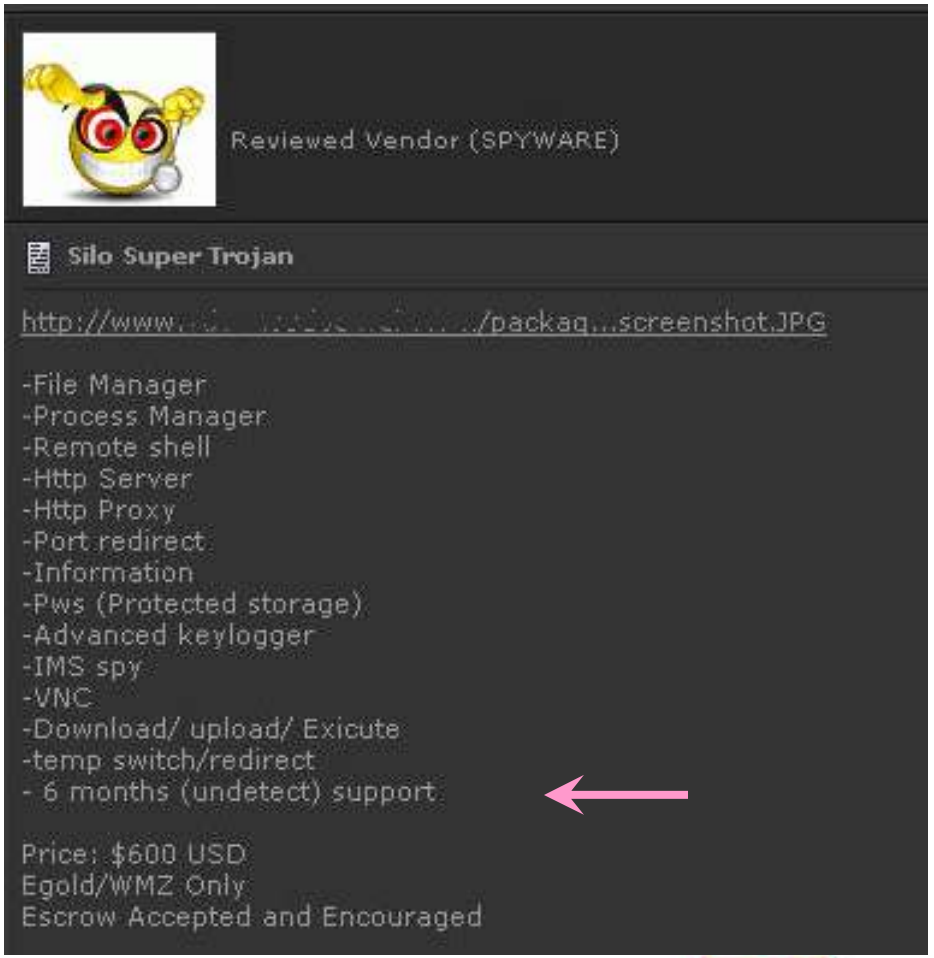
- Powerful: Collects *any* credentials
- Easy, easy, easy




RSA
The Security Division of EMC

# Fraud-as-a-Service
## Crimeware Testing Tools & Warranty

Anti-Virus “tester” and “fixer” with **guarantied** replacement if detected


RSA
The Security Division of EMC

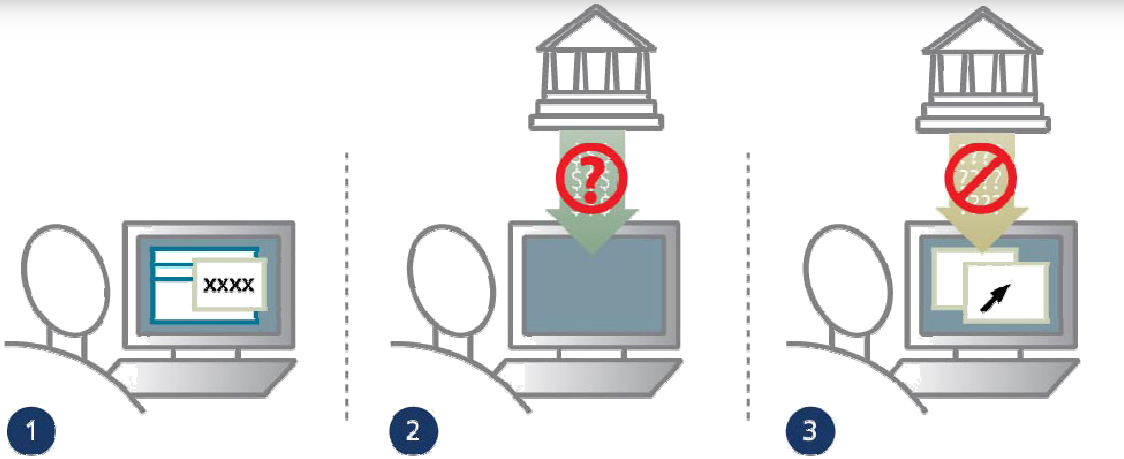
# Combating Fraud End-to-End

## Think beyond portal “Identity" - *Multiple Attack Vectors & Channels*

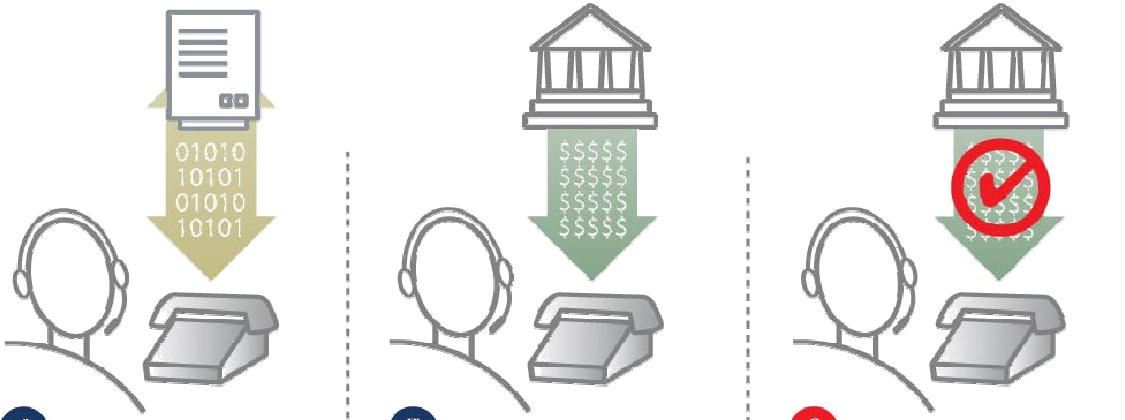


RSA
The Security Division of EMC

# How Multi-Channel Fraud is Perpetrated




1. Fraudster phishes credentials and logs in to account
2. Fraudster attempts a money transfer and gets challenged by the financial institution
3. Fraudster fails challenge and navigates account / Internet to learn about customer




4. Fraudster uses information gathered on the Web to authenticate on the phone
5. Fraudster tries to transfer money out of account
6. Fraudster successfully steals money via IVR / Call Center

RSA
The Security Division of EMC

# So What Can You Do?

***Victory is not found in destroying the opponent, it is found in reducing them!***

***As with fighting any intelligent opponent, the goal must be…***

- To analyze
- To act
- To achieve measurable *reductions* in fraud
- To adapt
- To repeat the above

RSA
The Security Division of EMC

# So What Can You Do?
## *Layered Defense Strategy*

- Holistic
  - Take proactive countermeasures to stop ‘harvesting’ fraudsters
  - Monitor and detect ‘cash-out’ fraudsters
  - Implement vulnerability & configuration polices – then AUDIT
- In-Depth
  - Protect enrollment, login, transactions & other post-login activities
  - Protect sensitive data, prevent ID theft and account takeover
  - Detect early ‘signs’ and fraud-enabling steps (e.g. profile changes)
- Adaptive
  - Tune security according to level risk and changing threats
  - Balance with cost and usability
  - Monitor (invisibly), block, or authenticate (visibly)

RSA
The Security Division of EMC


The Security Division of EMC

Thank you!