Trends in Impersonation Attacks: Technologies and Motivation

Lenny Zeltser

www.zeltser.com

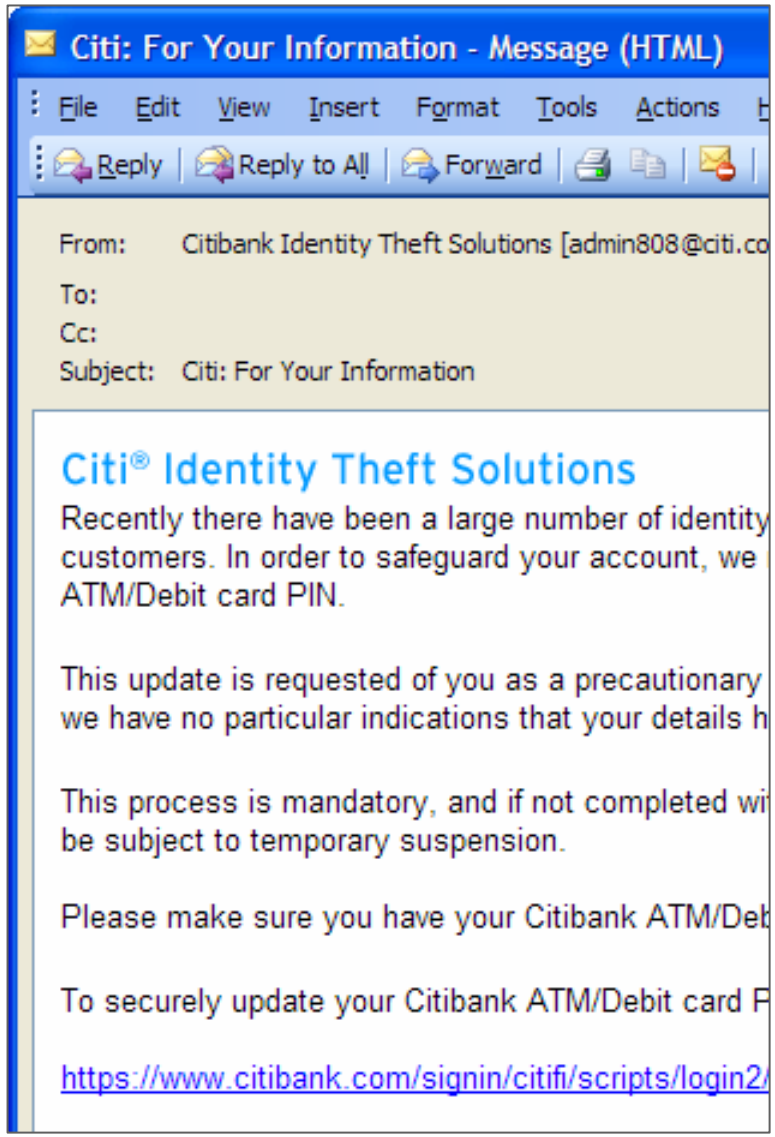
November 9, 2004

Impersonation attacks are becoming more complex and better organized

- Attractive financial incentives
- Organized groups and agents for hire
- Multi-faceted malicious code

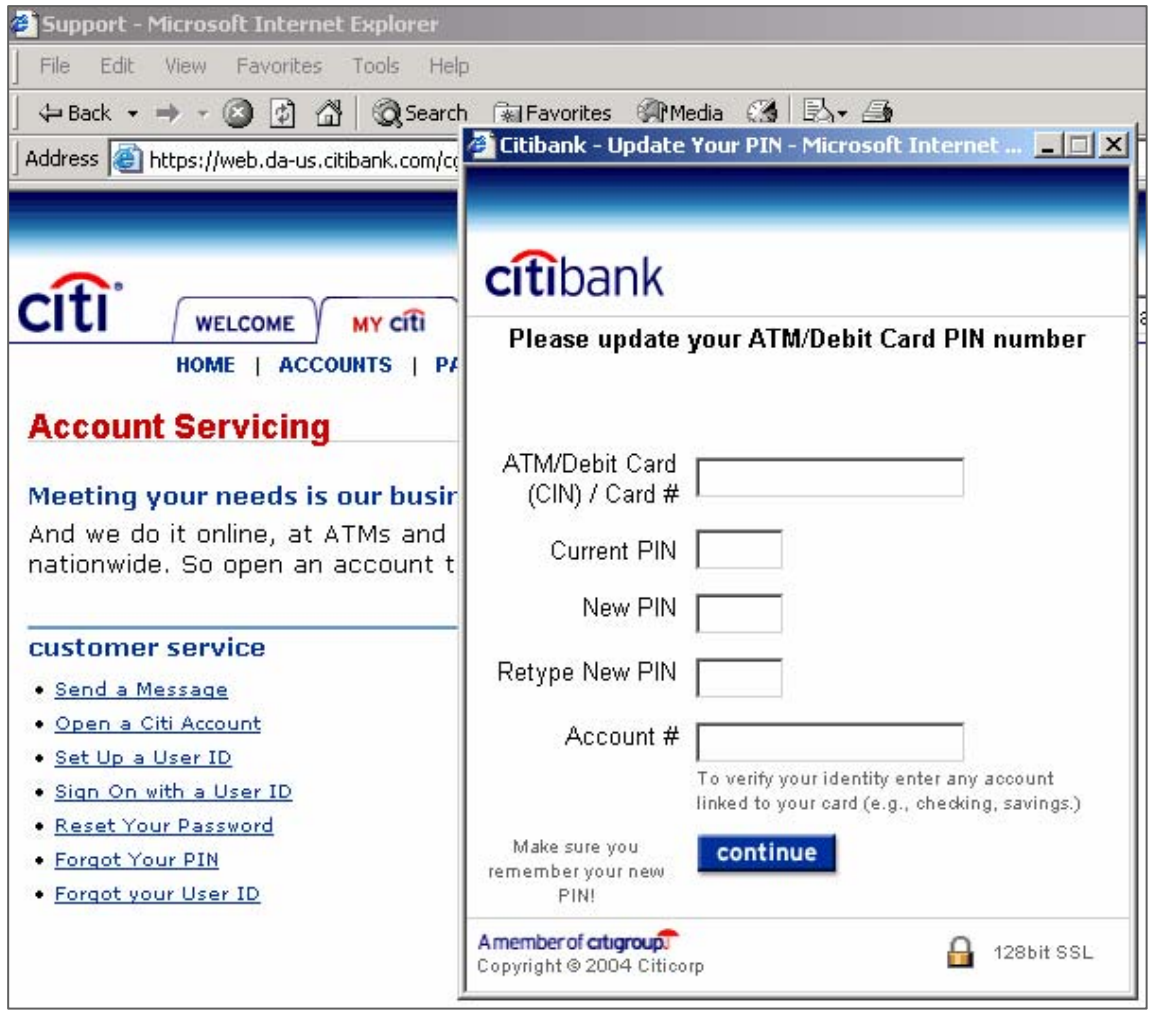
28% of consumers are fooled by phishing scams

- Messages crafted to look legitimate
- The link goes to a fraudulent website
- 41% of U.S. adults have, or think they have, received a phishing email



It can be very hard to visually detect a fraudulent financial website

- Real Citibank site opens on background
- Fraudulent window pops up on top
- Seems secure and authentic



Attackers can harvest as many as 6,000 records per day via phishing scams

Profitable AOL phishing scheme:

- Postal address
- Phone number

} Sold to a reputable mortgage company

- AOL username
- AOL password

} Used for sending more phishing SPAM

Harvested records can be sold, traded, or given away via on-line forums

- Users of stolen data vary in sophistication
- An example of a web forum where credit card information was given away

"Do you think they could catch me, if I buy stuff for work?

They'll catch you for sure, if you have them delivered at home.

But I could not care less. I will order up to about $100. Who will notice? Those people are filthy with money."

ShadowCrew.com sold financial data, personal info, drugs, attack services…

SSN and Other Information for Sale

Citizens of USA : 30$/record (min 300$)

Name, Address, City, State, ZIP, SSN, Phone1, Pnone2, Eploer, WorkPhone, WPhoneExt, Supervisor, Work Postion, Bank Name, Acc Type, Acc #, ABA

_____

ICQ 41781
E-mail: tron@counterfeitcards.com

Impersonation attacks are increasingly tied to organized crime

- Increasing presence of organized crime in phishing (Caltabiano, U.S. Secret Service)
- Definitely looks like there are organized groups (Curran, FBI)

> "Lawbreakers will shift much of their activity into cyberspace because it will increasingly be the venue where illicit profits are to be made and because it offers operational advantages." (Brenner, 2002)

Profitability of impersonation attacks has global implications

- Part of the larger identity theft epidemic
- Reported ties to financing terrorist operations

> "Law enforcement officials … believe that members of the Irish Republican Army and terrorists involved in the foiled plot to bomb Los Angeles International Airport relied heavily on identity theft schemes to finance their operations." (O'Brien, NY Times)

Software assisting with identity theft attacks is becoming more complex

- Phishing is merging with spyware
- High payoff potential encourages R&D in attack software
- Exploits target vulnerable users
- Network worms assist in spreading the software

Once on the victim's system, spyware can capture financial logon credentials

Attack:

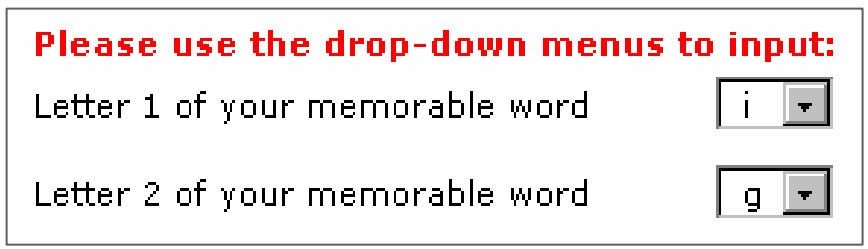
- Exploited a flaw in Internet Explorer

Result:

- Captured logon credentials
- Stole data despite browser encryption

Key-logging is being supplemented by screen-capturing capabilities

- Spyware can capture key strokes when the victim logs in
- Financial sites may require the user to select from a menu to authenticate
- Malware authors responded by capturing screen shots



Advanced specimens use the victim's own browser to steal money

- Spyware installed as browser component
- Activated when victim logs into the banking site (e-gold.com)
- Opens a hidden window while the victim browses the banking site
- Wires money out of the account

Attack automation techniques improve phishing and spyware capabilities

- Worms can distribute financial spyware
- Malware can be used to relay SPAM through infected systems
- Bots can host phishing and data sharing sites on infected systems
- Phishing toolkits ease attack creation

Impersonation attacks impact enterprises, not just individuals

- Weakening of the spoofed company's brand and credibility
- "At EarthLink, which suffers an average of eight unique phishing attacks each month, the cost per attack is more than $40,000."
  (CSO Magazine)

Companies' cost of recovering from spyware attacks is significant

- Up to 25% of enterprise desktops affected by "destabilizing software" (Meta Group)
- Spyware at least partially responsible for 50% of crashes reported to us (Microsoft)
- Impersonation attacks can target corporate confidential information

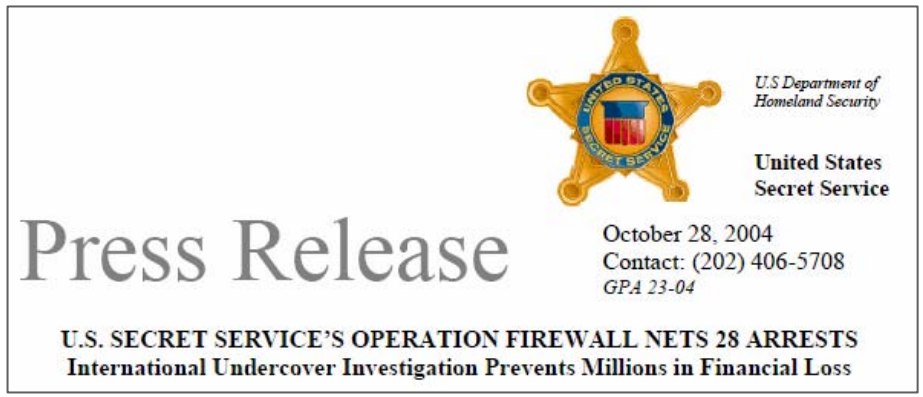
Law enforcement has stepped up its phishing-related efforts

- Brazil: 53 arrested ($30,000,000)
- Hong Kong: 12 arrested ($77,000)
- England: 12 arrested ($200,000)

"Organised Crime is targeting internet users in the UK to launder money stolen from online bank accounts where people have been duped into handing over their account detail." (Deats, National Hi-Tech Crime Unit)

Recent "operation firewall" led to 28 arrests internationally

- 1.7 million stolen credit cards
- $4,300,000 losses



U.S Department of Homeland Security

United States Secret Service

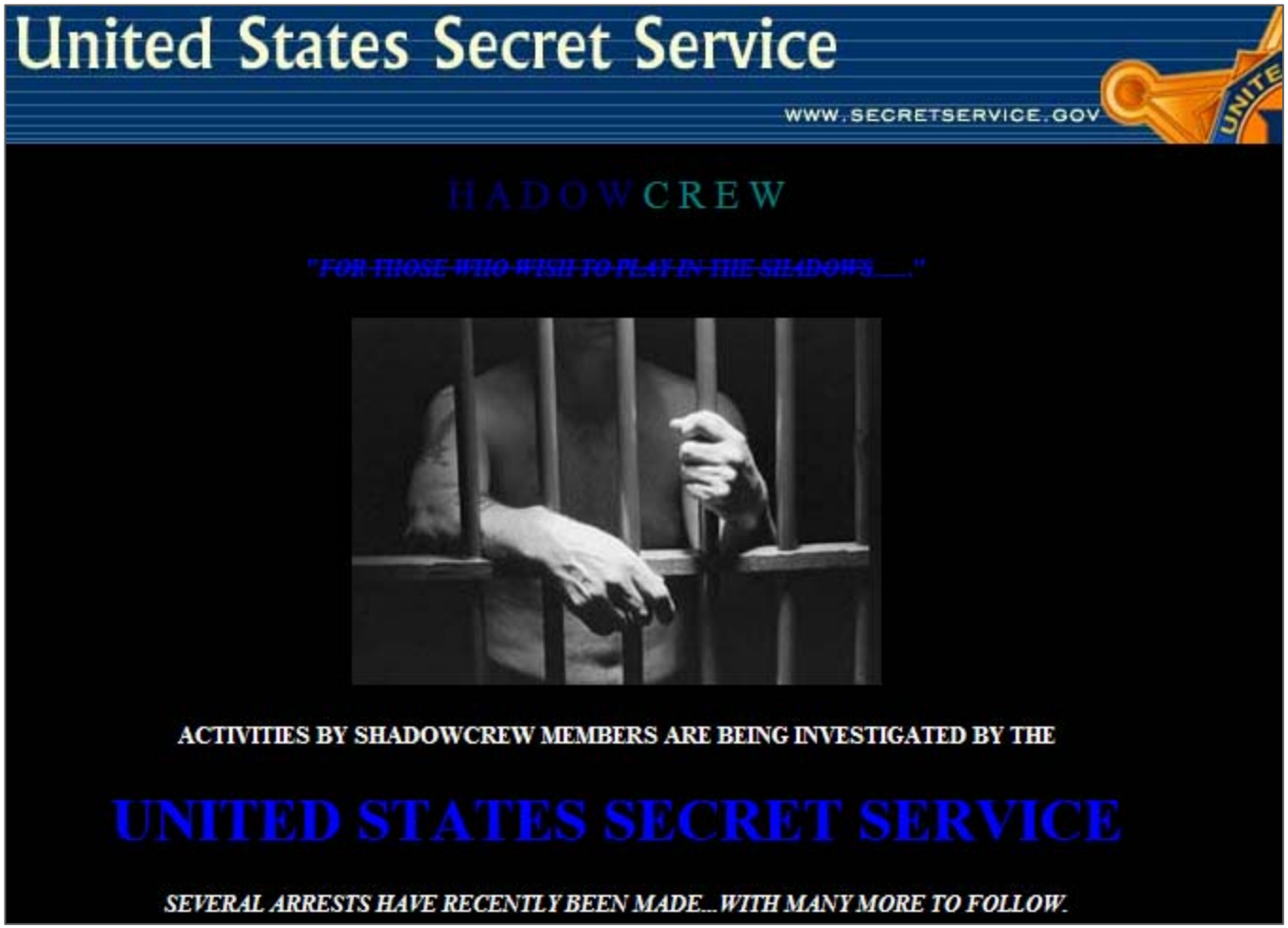
Press Release

October 28, 2004
Contact: (202) 406-5708
GPA 23-04

U.S. SECRET SERVICE'S OPERATION FIREWALL NETS 28 ARRESTS
International Undercover Investigation Prevents Millions in Financial Loss

- Led by Secret Service Newark Field Office
- Suspects "involved in a global cyber organized crime network"

U. S. Secret Service took over the NJ-based ShadowCrew.com site



I'm happy to answer any questions now or at a later time

- Impersonation attacks offer attractive incentives
- Attackers more professional and organized
- Malicious code is becoming more elaborate

Lenny Zeltser

www.zeltser.com