The Scope of eCrime Campaigns Against US Financial Institutions & the Solutions Deployed Against Them

Peter Cassidy
Secretary General – APWG
www.antiphishing.org
pcassidy@antiphishing.org
Director of Research – TriArche Research Group
www.triarche.com
pcassidy@triarche.com

APWG

Committed to wiping out
Internet scams and fraud

ID Theft Top Consumer Complaint

- ID Theft is the top consumer complaint to the US Federal Trade Commission (FTC) for the last 7 years
- Between January and December 2006, the FTC received over **670,000** ID theft complaints
  - **1 Identity Theft 246,035 (36%)**
  - **2 Shop-at-Home/Catalog Sales 46,995 (7%)**
  - **3 Prizes/Sweepstakes and Lotteries 45,587 (7%)**
- Consumers reported losses from fraud of more than $1.1 billion.
- Through its online complaint form and toll-free hotline, the Commission receives approximately 15,000 to 20,000 contacts **each week** on ID theft

2007 ID Theft Victim Statistics

- **Javelin Strategy & Research Survey - February 2007**
  - **Survey findings Include:**
- The number of US adult victims of identity fraud decreased from 10.1 million in 2003 and 9.3 million in 2005 to 8.4 million in 2007
- Total one year fraud amount decreased from $55.7 billion in 2006 to $49.3 billion in 2007
- The mean fraud amount per fraud victim decreased from $6,278 in 2006 to $5,720 in 2007
- The mean resolution time was at a high of 40 hours per victim in 2006 and was reduced in 2007 to 25 hours per victim

Cyber Gets the Headlines But ID Data Theft Mostly Low-Tech

- Stealing postal mail to get credit card applications, new checks or tax information
- Rummaging through consumers' home trash, businesses trash or municipal dumps
- Bribing an employee of a company with access to the consumers' financial records
- Purchase directly from consumer credit companies
  - ChoicePoint
- Tricking information out of employees of companies with personal financial information via telephone or email
- Tricking information out of consumers via telephone
  - Pretending to be a bank
  - Pretending to conduct a survey
  - Pretending to a police officer
- Illegally obtaining credit reports
  - Abusing employers' authorized access to credit reports
  - Posing as a landlord, employer or someone with legal authority to access consumer credit information
  - Using a corrupt collaborator with legal authority to access consumer credit information
- Skimming credit and debit card account numbers at retail establishments
- Stealing wallets and purses containing identification and credit and bank cards.
- Completing a change of address at the local form at the local Post Office to divert consumers' mail to a new location controlled by the ID thieves

IT Abuse in ID Theft

- Hacking into companies to steal costumers data
  - TJ Maxx
- Phishing by Social Engineering via email
  - Please contact company or gov't agency for:
    - Security issue, special offer/opportunity or charitable opportunity (Katrina)
- Crimeware (keyloggers; session hijackers, etc.)
- Interactive response telephone systems
  - Push #1 to re-authorize your account, etc.
- Instant Messaging (IM)
- Direct telephone interviews
- SMS (Cell phone text messages)
- Phishing by Technical Subterfuge
  - Infecting PCs with Crimeware (email; instant messaging; web pages)
  - Pop-ups
  - Session hijackers
  - Pharming (corrupting Web navigation infrastructure)
    - Local and remote variants
  - Technical Man in the Middle Attacks coordinating crimeware on the desktop with a intermediating server that replays dynamic passwords used in two-factor systems
  - Social Engineering-style Man in the Middle Attacks with phone calls from fake 'security personnel' going directly to employees' desks asking for passwords and token serial numbers

Statistics on ID Fraud

- According to *ID Analytics,* Fictitious identities – synthetic IDs – account for 88.38% of identity fraud, and 73.8% of financial damage caused in the US
- Theft of existing identities acounted for 11.7% of identity fraud
  - Less than 25% of the damage caused was by abuse of an identity belonging to a human being – or an actual existing customer

Trends in
IT Abuse, Internet-based Crime & ID Theft

“Classic” Social Engineering Attack Still Predominant

- Vast majority of phishing campaigns are based on classic social engineering scheme:
  - A ‘call-to-action’ e-mail compelling a consumer to visit a counterfeit Web site.
  - There he or she is tricked into giving his personal financial data and credentials for some reason:
    - Your account needs to be reauthorized
    - There has been suspicious activity on your account
    - The company needs to update your accounts
    - There’s a special opportunity or offer for you
    - A charity needs your help

CITIZENS BANK
Not your typical bank.®

Citizens Bank Instant $5 reward survey

Get credited $5 to your account just for answering 5 easy questions!

Dear Valued Customer,

You have been chosen by the Citizen's bank online department to take part in our quick and easy 5 question survery, In return we will instantly credit $5 to your account - Just for your time!

Helping us better understand how our customer's feel benefits everyone. With the information collected we can decide to direct a number of changes to improve and expand our online service. The information you provide us is all non-sensitive and anonymous - No part of it is handed down to any third party groups.
It will be stored in our secure database for a maximum of 7 days while we process the results of this nationwide survey.

We kindly ask you to please spare 2 minutes of your time in taking part with this unique offer!

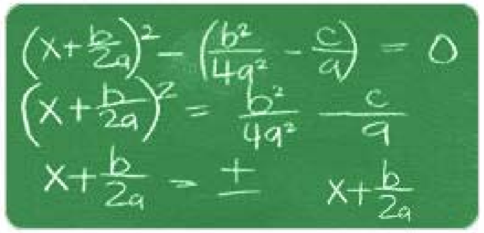
To Continue click on the link below :

http://www.citizensbankonline.com/logon/securesurvey.asp

Many Thanks & Kind Regards -

Citizens Bank Customer Department

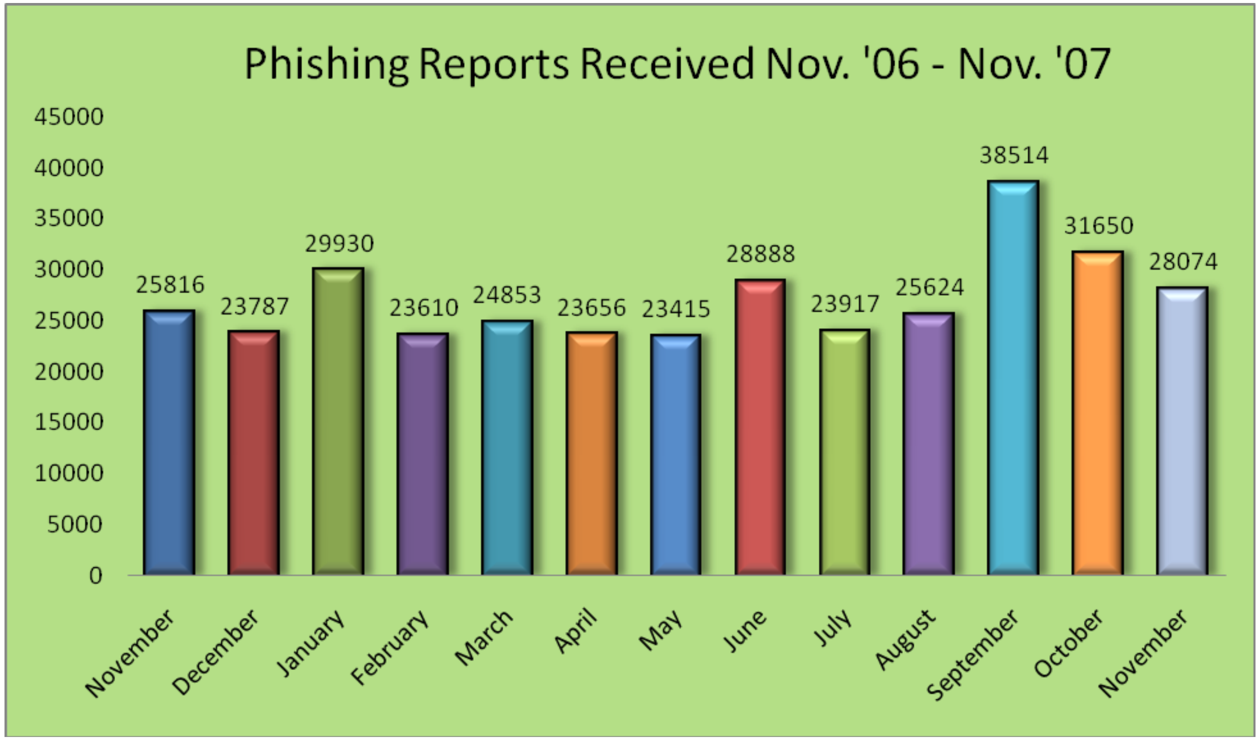
0% APR
No Annual Fee
Enhanced Security and Services
on purchases and balance transfers for 10 full months



Member FDIC Equal Housing Lender

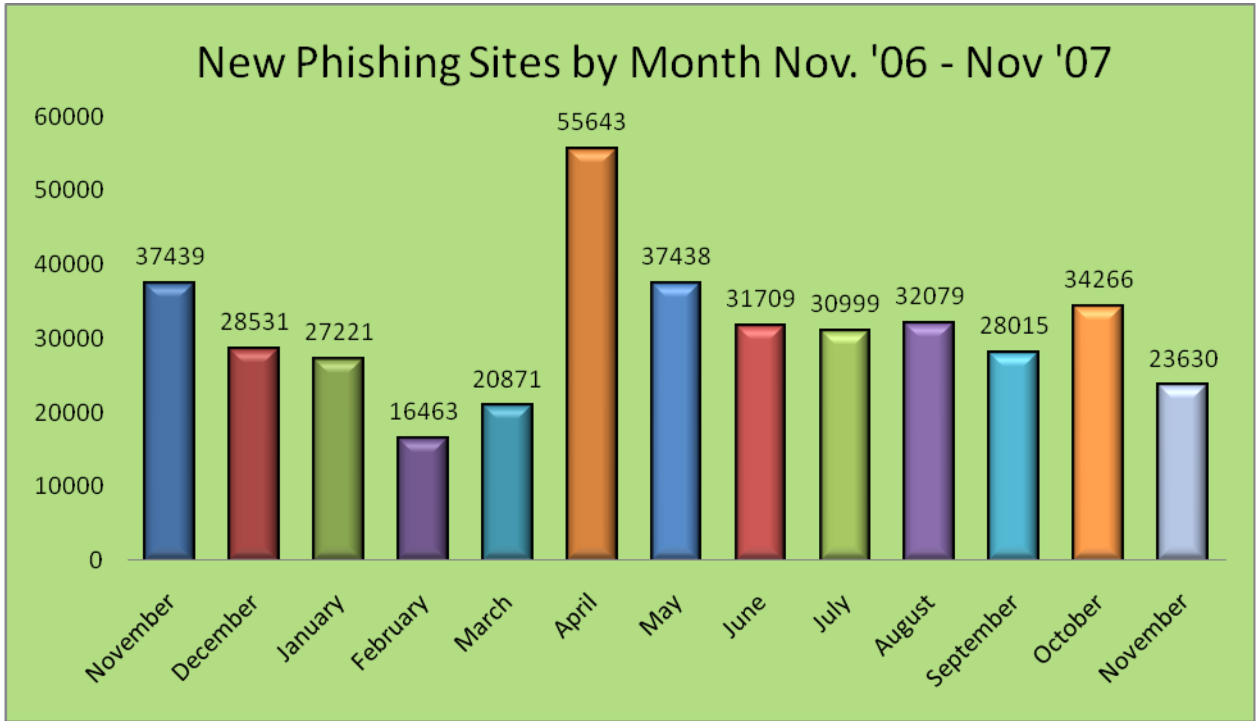
To contact Customer Service please call 1-800-922-9999.

Trend: Conventional Phishing Campaign Numbers Flat



Phisher's focus on targeted phishing campaigns against executives with access to intellectual property bank accounts may explain some of the reduction in conventional phishing attacks against consumers

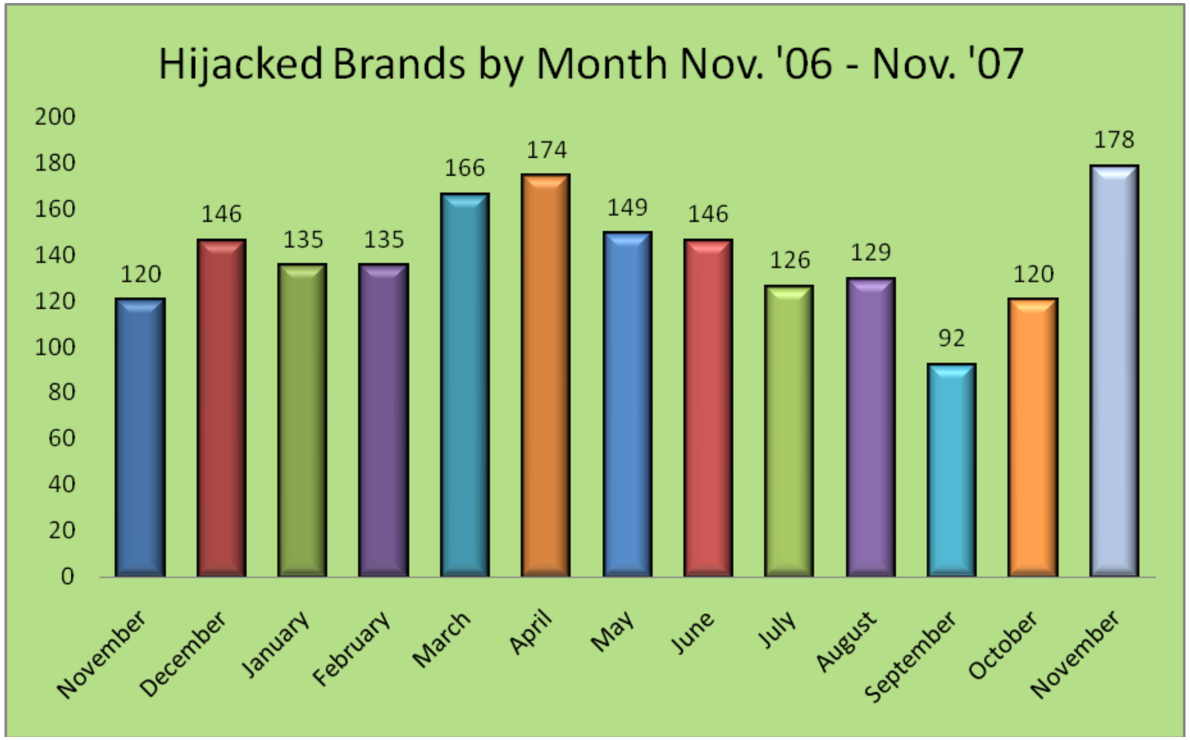
Trend: Emphasis on Campaign Durability By Using Multiple Phishing Websites



Large-scale URL Variation: Phishers send out phish mails pointing to URLs using multiple subdomains attached to spoof domains (e.g. http://123.phishsite.com, http://234.phishsite.com, http://345.phishsite.com.) Intent: defeat spam filters and URL-filters on anti-phishing toolbars

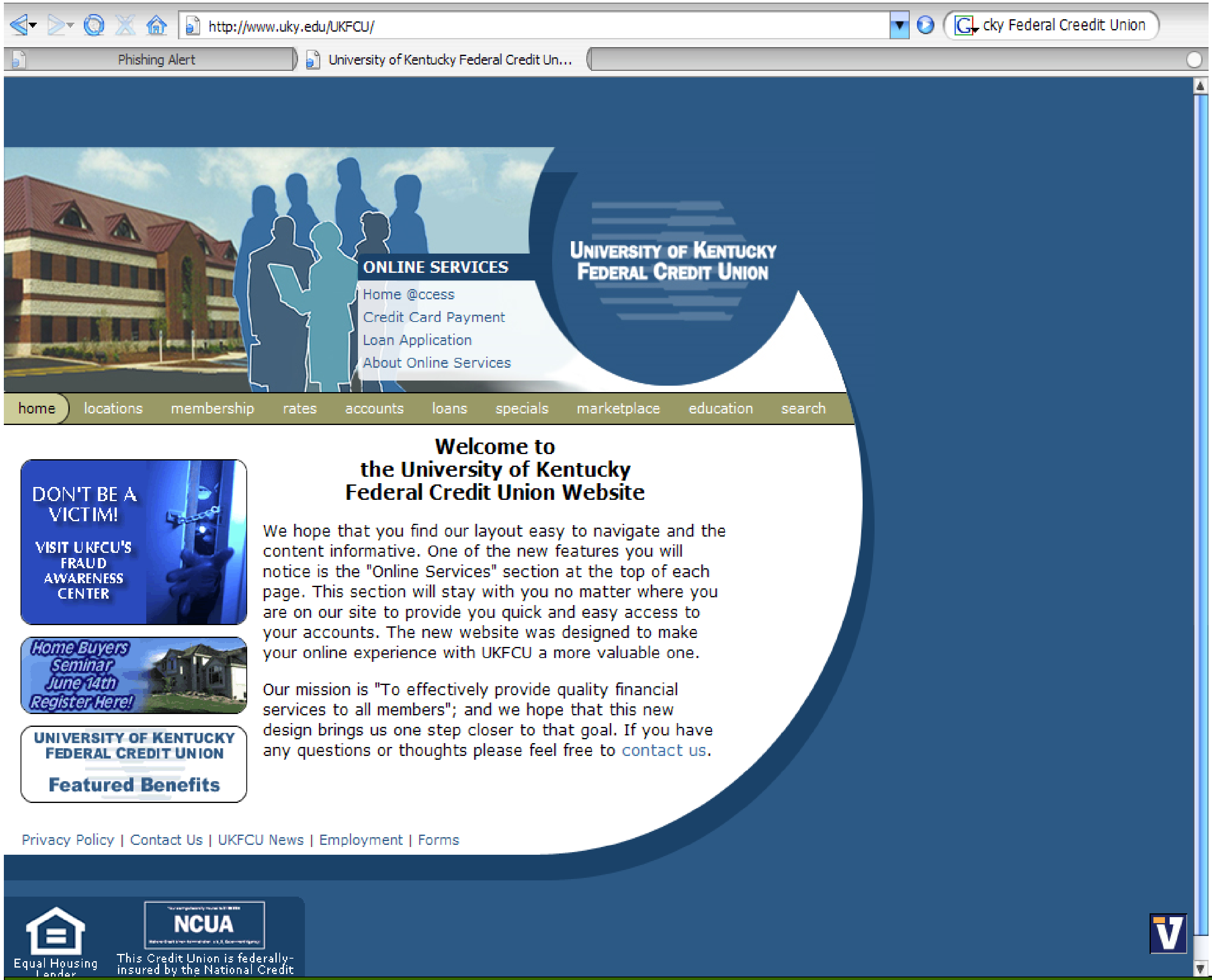
FastFlux:Rapid changing of IP address associated with a domain – hundreds – changing every few minutes to frustrate take-down attempts. Often IP addresses resolve to proxies to redirect consumers to one of a large number of phishing sites.

Trend: Target Fragmentation



APWG is seeing increasingly smaller institutions attacked. Phishers are also attacking larger numbers of financial institutions in Europe and the Middle East over the last two years and increasing numbers of equity brokerages and mutual fund companies. In US, UK, Australia and Latin America, government agencies' IDs are spoofed in phishing campaigns

Trend: Phishers Targeting Smallest



http://www.uky.edu/UKFCU/
cky Federal Creedit Union
Phishing Alert
University of Kentucky Federal Credit Un...
University of Kentucky Federal Credit Union
Online Services
Home @ccess
Credit Card Payment
Loan Application
About Online Services
home
locations
membership
rates
accounts
loans
specials
marketplace
education
search
Don't be a victim!
Visit UKFCU's Fraud Awareness Center
Home Buyers Seminar June 14th Register Here!
University of Kentucky Federal Credit Union
Featured Benefits
Equal Housing Lender
NCUA
This Credit Union is federally-insured by the National Credit

Welcome to the University of Kentucky Federal Credit Union Website

We hope that you find our layout easy to navigate and the content informative. One of the new features you will notice is the "Online Services" section at the top of each page. This section will stay with you no matter where you are on our site to provide you quick and easy access to your accounts. The new website was designed to make your online experience with UKFCU a more valuable one.

Our mission is "To effectively provide quality financial services to all members"; and we hope that this new design brings us one step closer to that goal. If you have any questions or thoughts please feel free to contact us.

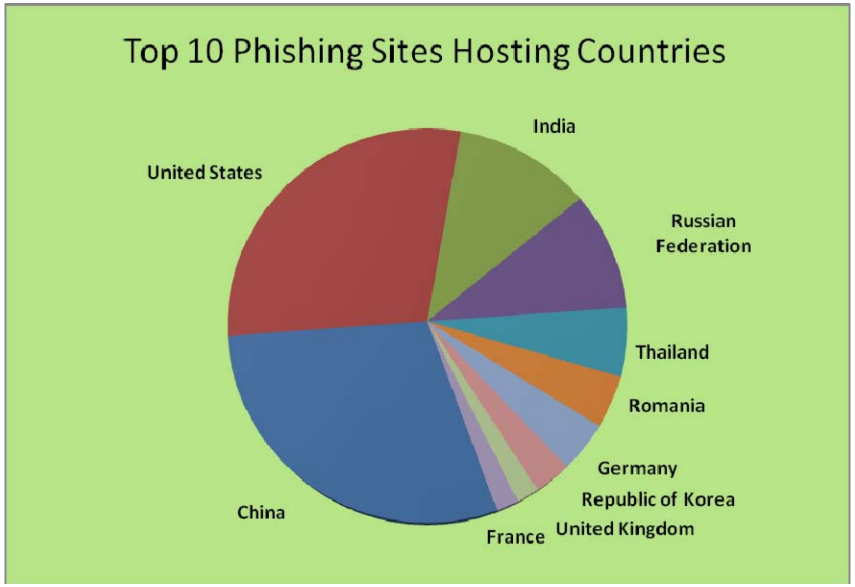
Privacy Policy | Contact Us | UKFCU News | Employment | Forms

- May, 2005, Phishers use university email addresses to attack UK Federal Credit Union customers. 3,000 members and assets of $152 million
- Phishers learning to work probabilities in their favor with small cohorts collecting lists of email addresses of consumers with likely relationship with target FI

Trend: Targeting Key Employees with Access to Competitive Data & Treasury

- Phishers targeting executives inside enterprises, government agencies and laboratories
- Send phish mails to limited number of executives and key employees to phish data or infect their PCs with crimeware
- Corporate treasury increasingly the target of these phishing attacks
- Valuable competitive data are targeted goods that could be sold on the black market as ‘insider information’ and competitive intelligence

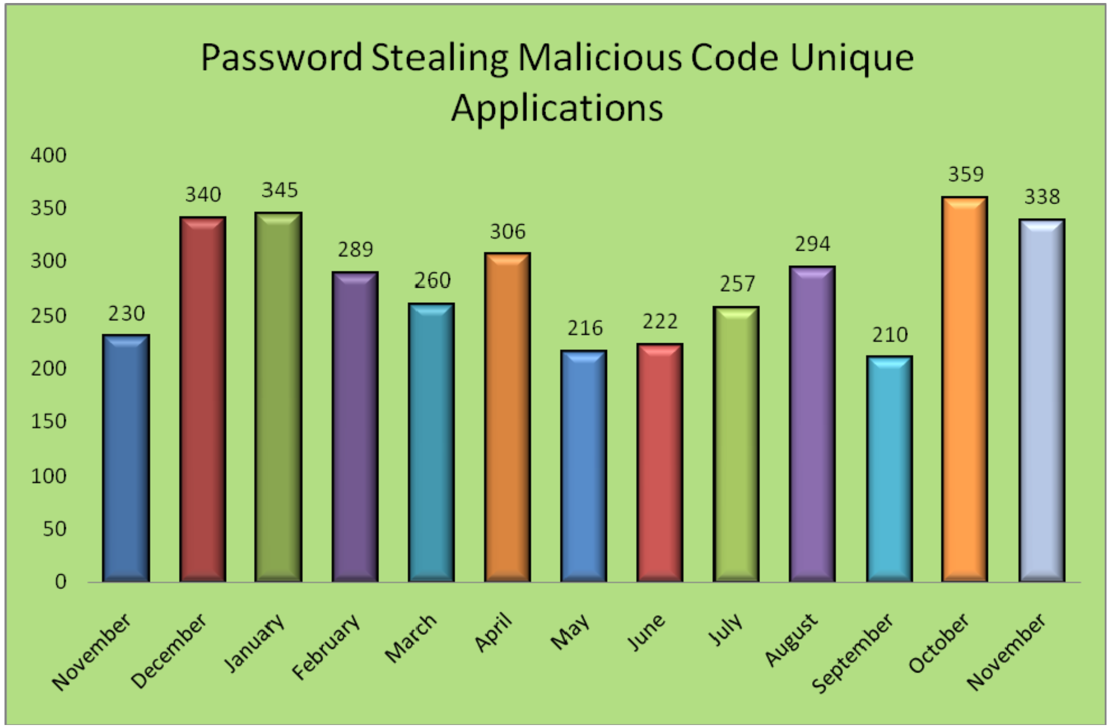
US and China Host Largest Numbers of Phishing Website



China	24.21 %
United States	23.85 %
India	9.39 %
Russian Federation	8.06 %
Thailand	4.64 %
Romania	3.53 %
Germany	3.41 %
Republic of Korea	2.42 %
United Kingdom	1.47 %
France	1.47 %

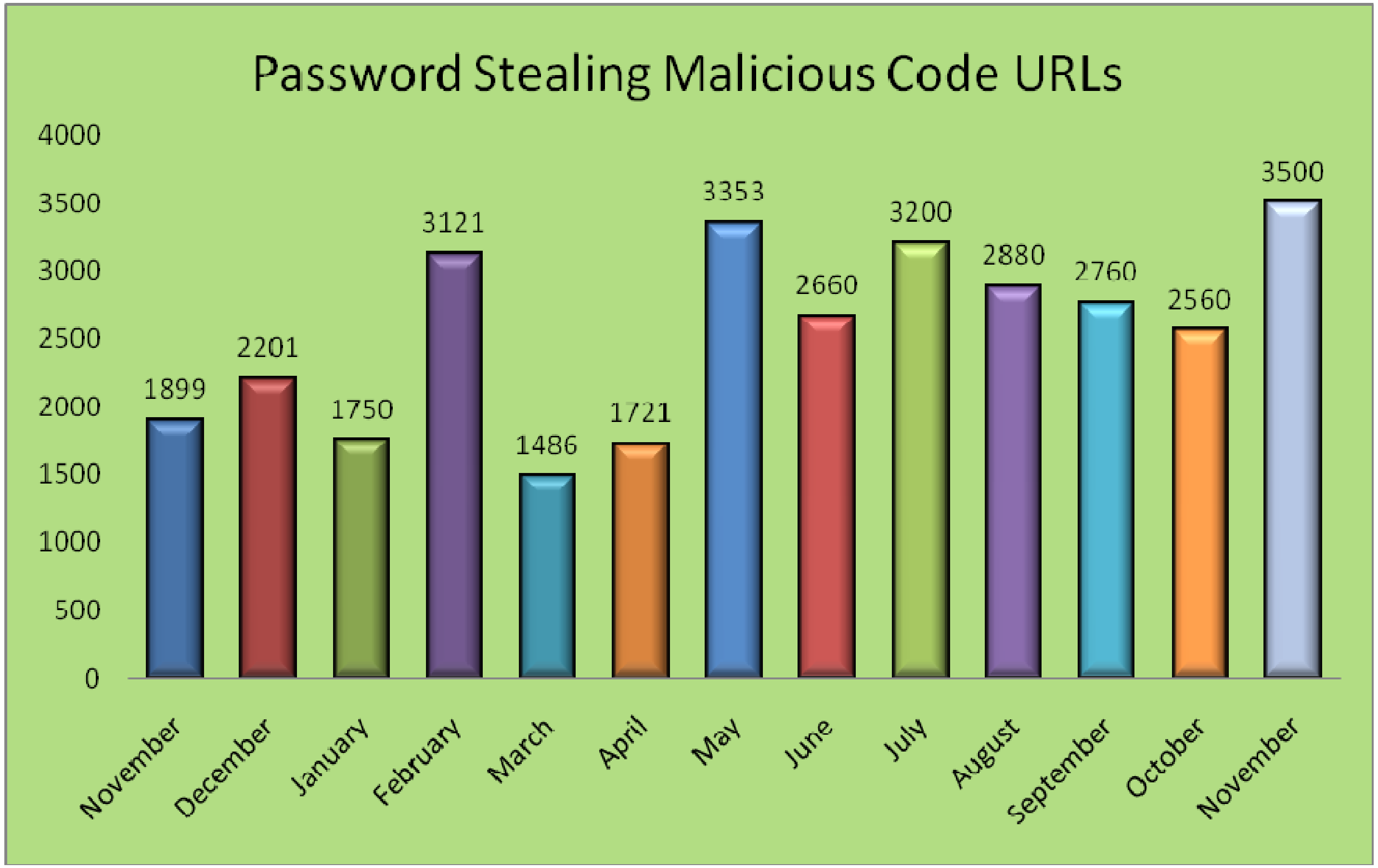
More countries being added to APWG’s list of host countries every year, but US runs close to half of the sample from month to month, passed this year in one month period by China

Crimeware: Mostly Keyloggers
Completely ‘New’ Crimeware Code Rare



Most innovation in crimeware is invested in survivability, assuring that crimeware will not be detected or neutralized by anti-virus or anti-spyware systems. Brazil CERT reports: The best detection rate for AV software in 2005 was 88% - decreasing to 79% in 2007. Crimeware invisibility shields increasingly frustrate anti-virus technology

Trend: Emphasis on Increasing Websites to Spread Crimeware

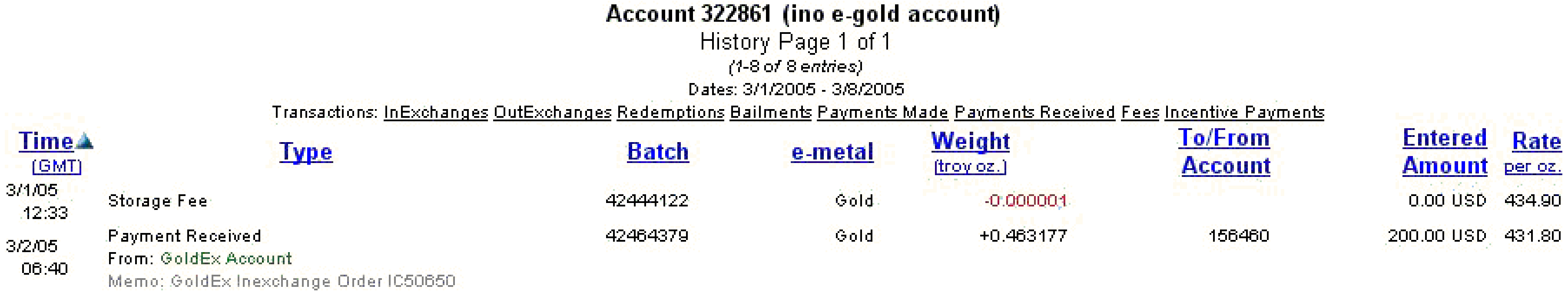


Full Automation in Phishing

- Most all of the phishing crimeware we've inspected has been developed to intercept the consumer's user name and password
- In 2005, we witnessed the deployment of a trojan system designed specifically to wait until *after* the user logged in to interrogate the account and **complete funds transfers automatically**
- Bottom line: completely automated phishing is at hand now with all the components required reported in the field

Automated Account Theft

- Secretly perform transactions after you log in



Account 322861 (ino e-gold account)

History Page 1 of 1

(1-8 of 8 entries)

Dates: 3/1/2005 - 3/8/2005

Transactions: InExchanges OutExchanges Redemptions Bailments Payments Made Payments Received Fees Incentive Payments

Time (GMT)	Type	Batch	e-metal	Weight (troy oz.)	To/From Account	Entered Amount	Rate per oz.
3/1/05 12:33	Storage Fee	42444122	Gold	-0.000001		0.00 USD	434.90
3/2/05 06:40	Payment Received From: GoldEx Account Memo: GoldEx Inexchange Order IC50650	42464379	Gold	+0.463177	156460	200.00 USD	431.80

Win32.Grams waits for a user to log into an e-Gold account, then creates a hidden browser session in the background which uses OLE automation to transfer the money from their account directly to another e-Gold account

Measuring the Total Threat Potential of ID Theft and eCrime

Scope of Threat

- It started with card skimming and ‘white plastic’ card schemes using phished data for small-scale, high-volume thefts
- But ID theft can and is being leveraged for much larger individual and corporate losses today
- Tomorrow could even substantially distort investment markets, injuring far many investors and public companies

Individual Consumer Threat

- Credit Accounts (Credit Cards)
- Savings and Checking Accounts (ATM Cards)
- Retirement Accounts (Brokerage accounts and Mutual Funds)
- Property
  - Real Estate
    - Increasing numbers of cases in US and Canada of mortgage frauds, based on ID theft
      - Discharge existing mortgage
      - Apply on line for a new one
      - Go to closing and walk away
- Next?
  - Loans against actual assets of persons and businesses:
    - Boats
    - Planes
    - Private Businesses
      - Business Assets and Property

Enterprise Threat

- Corporate treasury accounts are under attack
        - Increasing reports of focused phishing attacks on treasurers, CFOs and accounts managers
    - ‘Reverse phishing’ attacks
        - Phishers spoof IDs of companies and send trading partners notice of changes to bank account numbers
        - Company pays invoices – and funds end up in accounts controlled by phishers
    - Keylogging attacks on corporate treasury accounts
        - Credentials intercepted by keylogger and sent to criminals
        - Funds transferred out by ACH or international wire transfers, often through a number of accounts controlled by phishers or the mules they employ
    - Conventional Phishing Attack: North Kentucky Chamber of Commerce
    - $160,000 in losses in 2006
- *Smoldering issue: determining insider collusion in a corporate phishing attack*
- Customer Data and Data Assets in Company’s Care
    - Monster.com – Employer/jobs advertisers were phished for credentials to gain access to the resume database to fuel targeted phishing attacks against job seekers
    - Salesforce – Saleforce’s own employee’s credentials phished. Phishers went through customers client lists to drive targeted phishing attacks
- Intellectual property
    - Phishing is now being used as a corporate espionage tool
        - APWG has taken reports about manufacturers being phished (email and crimeware) specifically to mine data about products in development

Investment Markets Threat

- Internet ‘pump and dump’ scams almost as old as email
- Securities and Exchange Commission has had to suspend trading dozens of penny stocks over the years due to large-scale hyping of stocks
- Targets until this year thinly traded stocks, using only spam emails
- January, 2007 Aleksey Kamardin of Tampa charged by SEC for using multiple compromised accounts to pump up prices of shares he later sold at inflated prices for personal profits in his own account
  - Kamardin allegedly netted more than $82,000
- March, 2007, SEC charged three Indian nationals, Jaisankar Marimuthu, Chockalingam Ramanathan and Thirugnanam Ramanathan with breaking into consumer brokerage accounts to buy stocks and inflate their values
  - Sun
  - Google (put options)
- SEC alleged profits of $121,500 and damages of more than $875,000
- Question: How long before scammers use more subtle techniques to move markets to their favor, the way they are crafting hard-to-detect crimeware? Have they already?

Solutions in Use and in Development

- Authentication Technologies for Online Accounts
  - Operated by consumer
    - Session
    - Transaction
  - Required to open sessions and complete transactions
- Fraud Detection
  - Operated by online enterprise or 3rd Party vendor
  - Can work to stop transactions even if authentication technologies have been compromised
- Bank operations often blend authentication & fraud detection for layered security approach

Authentication Technologies

- Passwords
- Mutual Authentication schemes
  - Consumer is given signal that he or she is on the correct bank website and accounts page during connection to website or at the start of banking session
- Graphical Keyboards (Randomized alpha numerics and symbol systems) for mouse-driven password entry
- One-time-password tokens
- Trusted Platform Module (UK's 'Chip and Pin' program combining a chip-based smart card with a handheld card reader)
  - RBS deployed 3 Million card readers to customers; Barclays deployed 0.5 Million (planning another ~ 2 Million); Nationwide announced deployment of 3 Million for 2008
- Scratch Cards with single-use shared secrets
  - Scratch cards and grid cards
- Out of channel confirmation – SMS to cell phone with response
- Browser-based filtering software to detect phishing and alert consumers to fraudulent Web sites
  - A broad filter – differ from the mutual authentication like SiteKey or SecureBrain
- Authentication technologies overlap with bank-controlled fraud detection technologies

Fraud Detection & Deflection Approaches

- Combining and analyzing *all* of the consumer’s accounts history for fullest picture of consumer behavior
  - Once separate and analyzed separately
- Internet Protocol (IP) address location and user geo-location
  - Allow banks to detect fraud activity without first knowing the credentials have been compromised
- Internet Protocol (IP) address history archives abusive IP addresses
  - Allows bank to detect when a session is trying to connect from an IP address or IP space associated with abuse
- Device authentication (cookies and soft tokens)
- Device history (both of customer and attacker devices)
  - Allows bank to detect when a session is trying to connect from a device historically associated with abuse
- Banks deploy these schemes as 3rd party solution integrated into bank operations or developed and managed by bank personnel

Fraud Detection Can Become Forensic Tool

- It’s good to stop a fraudulent transaction from being accepted and losing money
- It’s better to record all the data, archive them and correlate them and use them to map and neutralize the phishers’ activities
- Done right, this approach turns a defensive perimeter into an offensive frontier

End Game

- No one technology or approach will eliminate electronic crime against consumer and businesses
- Layers of detection and protection are now being put into place to neutralize attacks
- Adoption will be accelerated by enterprises demanding high-quality protection for their treasury accounts – accelerating adoption and lowering prices
- High-quality protection will reduce the number of gangs capable of exploiting technical windows of opportunity
- Internet-based fraud becomes a normally manageable part of the security risks faced by financial institutions

APWG's Institutional Role

eCrime Data Clearinghouse

- Clearinghouse model forces examination of data governance and usage issues in private and public sectors
  - Clearinghouse success owes a lot of governance innovation established by APWG in user agreement
    - Banks would not cooperate in reporting without it
  - User agreement that assigns no new liability
    - Role of NDAs, User Agreements often underappreciated in technical community
      - APWG woken up by vocal brandholder reluctance to share phish data in 2004
  - Some 130+ Signatories from CERTs, brandholders, telecommunications companies, security companies, software developers, academic researchers
  - **Clearinghouse model** operates similarly to the genomic databases used by life sciences researchers in the US and Europe
  - Third-party position gives important assurance of neutrality

Data Resources

- IODEF Extensions for eCrime Reporting
  - Purpose-built XML Schema for eCrime
- APWG Phishing Attack Data Repository
- Phishing Attack URL Block List (UBL)
- APWG eCrime Abuse Contact Database
- Data Resouces In Development
  - Network data related to cash-out attempts
  - Rockphish domains used for phishing attacks

- Counter-eCrime Operations Summit
  - Program developed just for operations personnel who protect consumers and track electronic crime gangs
- May 26 and 27 in Tokyo
  - First APWG Conference in Asia
- http://www.antiphishing.org/events/2008_operationsSummit.html
- International data sharing protocols
- DNS Registry policy
- Coping with Insider Abuse Threats
- International case studies
- Much more. . . To be added to the agenda

Thank You from APWG

- Peter Cassidy
- pcassidy@antiphishing.org
- +1 617 669 1123