Mapping the Frontiers of the Electronic Crime Threat From Consumers' Desktops to National Equities Markets

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

What is Phishing Used For?

- Acquiring personal financial data for sale to criminal data brokers
- Acquiring credentials of corporate employees with treasury authority for access to corporate treasury accounts
- Acquiring network credentials to gain access to intellectual property
- Acquiring corporate client data to enable phishers to stage highly focused, personalized phishing attacks
  - Salesforce.com
  - Monster.com
- Stealing from accounts – or “cashing out”
- Setting up secondary bank accounts for laundering money and transferring money out of the ‘host’ country after successful scams
- Gaining personal financial data to ‘extend’ a real identity – ID theft activities
  - Create new lines of credit
  - Acquire assets to be liquidated
- Gaining control of investment accounts to distort equities markets by creating appearance of legitimate info-driven market activities around them

Much U.S. ID Data Theft Low-Tech

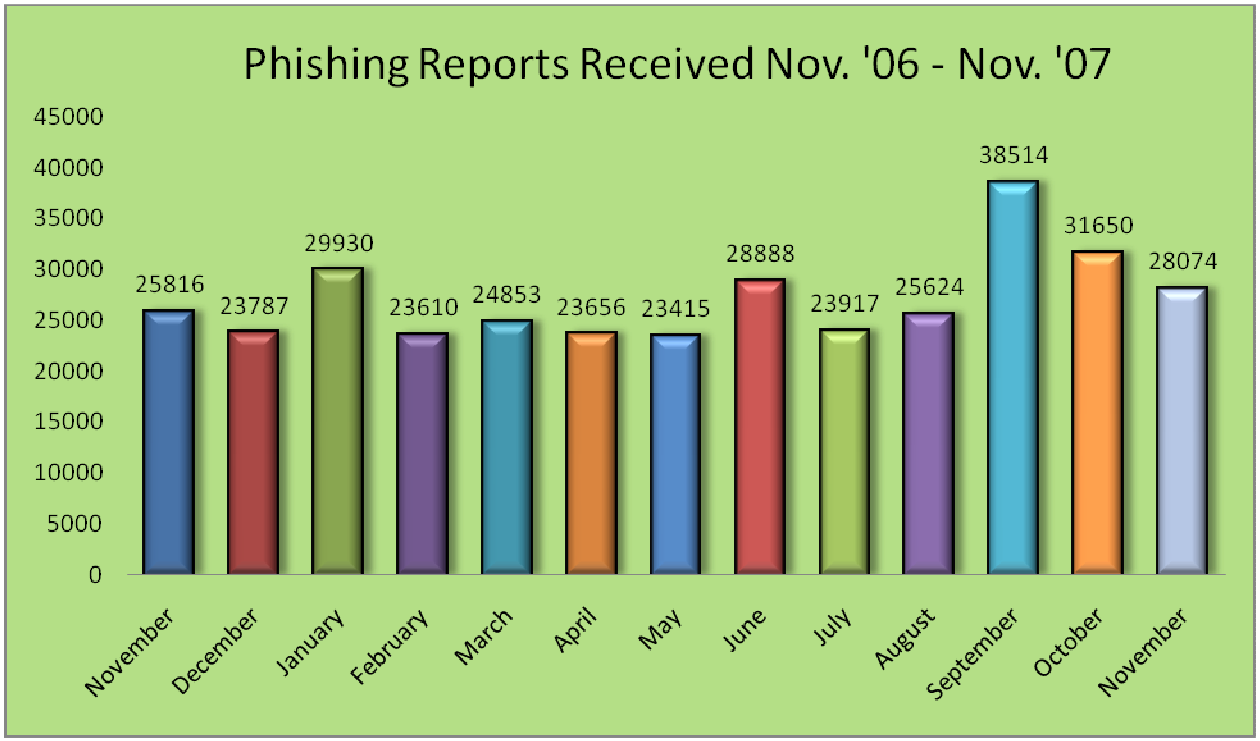
- Stealing postal mail to get credit card applications, new checks or tax information
- Rummaging through consumers' home trash, businesses trash or municipal dumps
- Bribing an employee of a company with access to the consumers' financial records
- Purchasing directly from consumer credit companies – (e.g.. ChoicePoint)
- Tricking information out of employees of companies with personal financial information via telephone
- Tricking information out of consumers via live telephone interview
  - Pretending to be a bank
  - Pretending to conduct a survey
  - Pretending to a police officer with a warrant
- Tricking information out of key company employees live telephone interview to gain access to corporate treasury accounts and intellectual property
- Illegally obtaining credit reports
  - Abusing employers' authorized access to credit reports
  - Posing as a landlord, employer or someone with rights to access consumer credit information
  - Using a corrupt collaborator with legal authority to access consumer credit information
- Hand copying credit and debit card account numbers at retail establishments, stores and restaurants
- 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
- Mailing scam offers to consumers via ordinary postal mail

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)
  - Increasingly, the emails include a number to call, rather than an email address for response
- Crimeware (keyloggers; session hijackers, etc.)
- Interactive response telephone systems: "Push #1 to re-authorize your account"
- Instant Messaging (IM)
- SMS (Cell phone text messages)
- Phishing by Sophisticated Technical Subterfuge
  - Infecting PCs with Crimeware (email; instant messaging; web pages)
  - Pop-ups (Please re-enter your username and password)
  - 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

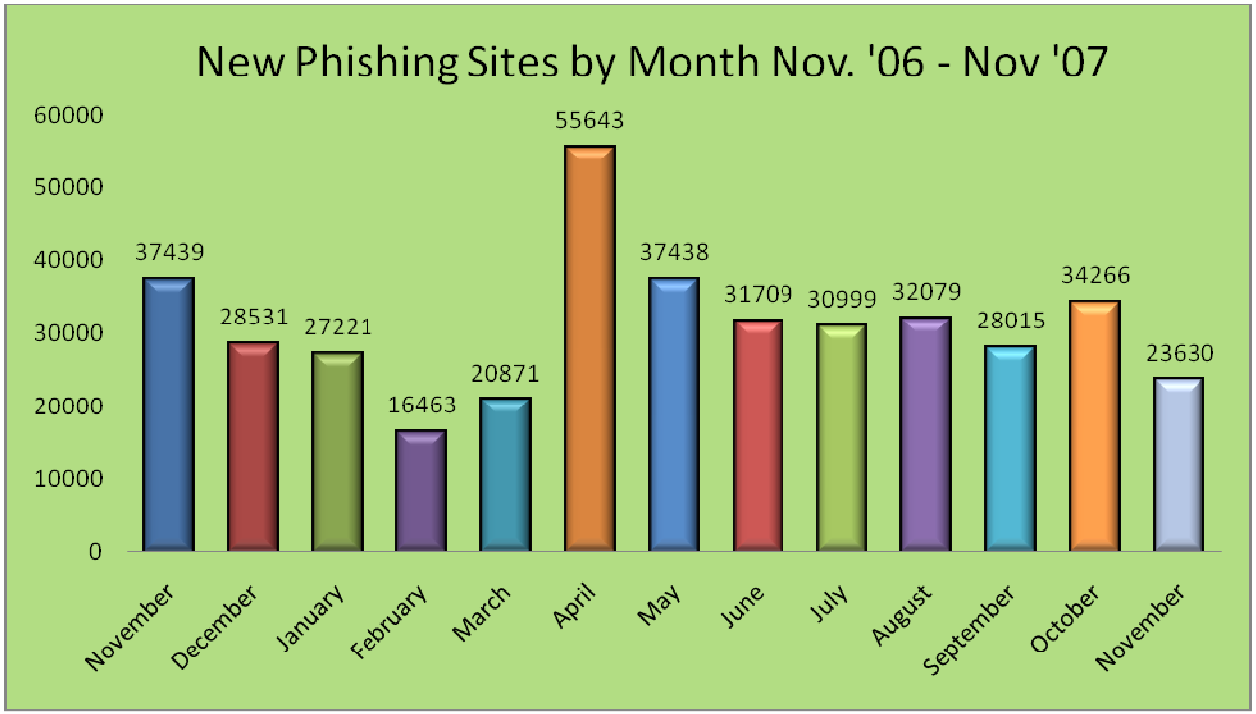
Trends in
IT Abuse, Internet-based Crime & ID Theft

Trend: Conventional Phishing Campaign Numbers Flat



Phisher's focus on targeted phishing campaigns against executives with access to corporate bank accounts and intellectual property may explain the reduction in conventional phishing attacks against consumers near the end of 2007

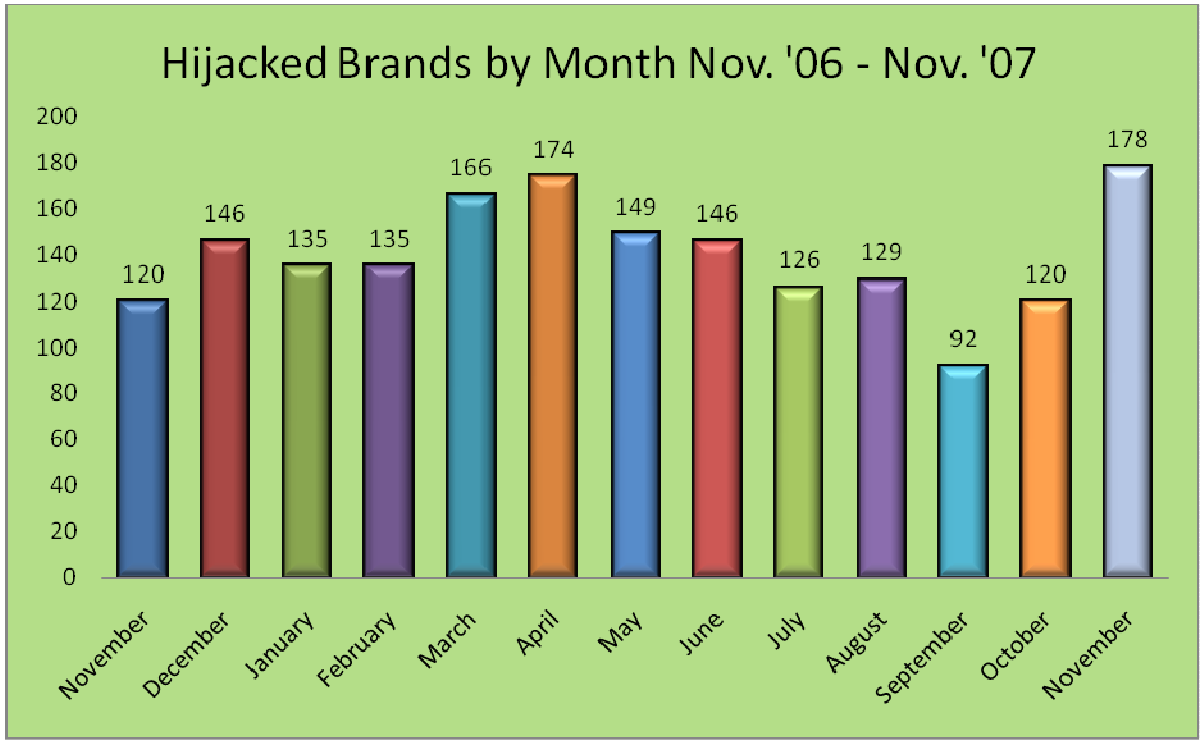
Trend: Emphasis on Phish Campaign Durability By Using Multiple Phishing Websites



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 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 sees smaller institutions being targeted. Phishers are also attacking larger numbers of financial institutions in Europe and the Middle East over the last two years. Recently, more equities brokerages and mutual fund companies have been targeted. In US, UK, Australia and Latin America, government agencies are spoofed in phishing campaigns.

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

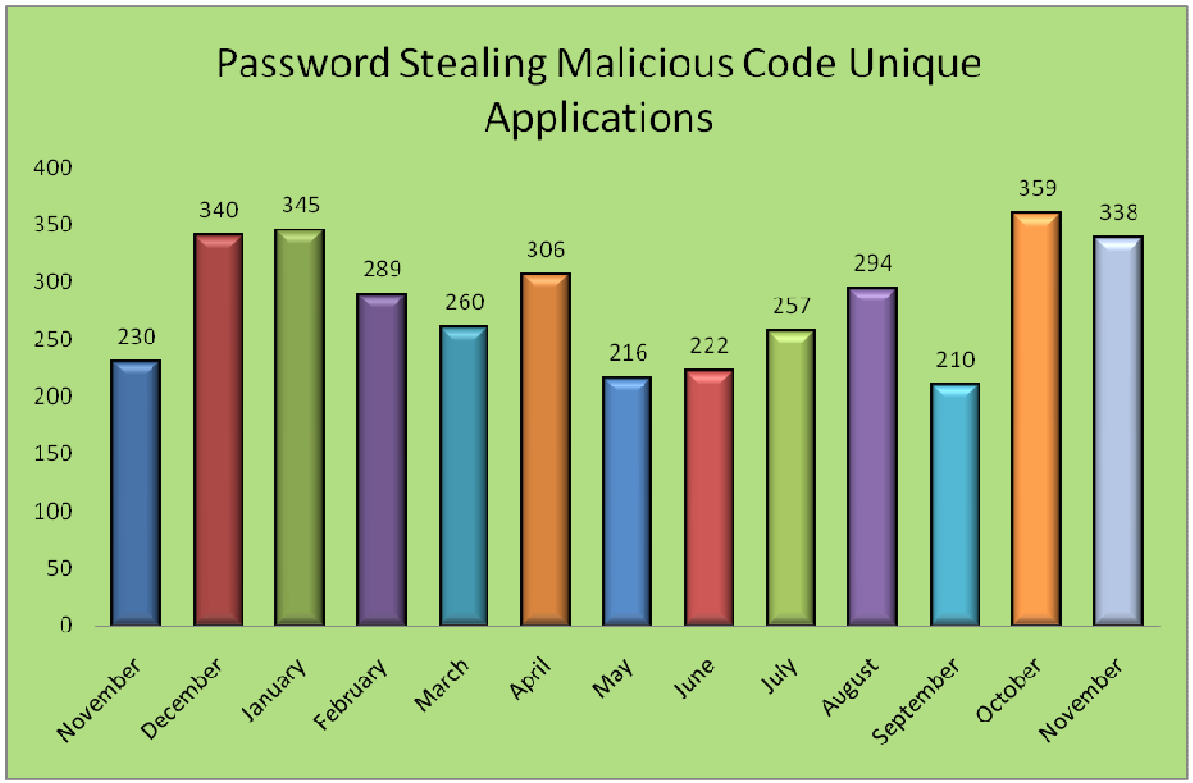
- Phishers targeting executives inside enterprises, government agencies and government laboratories
- Send phish mails to limited number of executives and key employees to phish data or infect their PCs with crimeware
- Corporate treasury increasingly the target of these phishing attacks - up to the CFO level
- 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 %

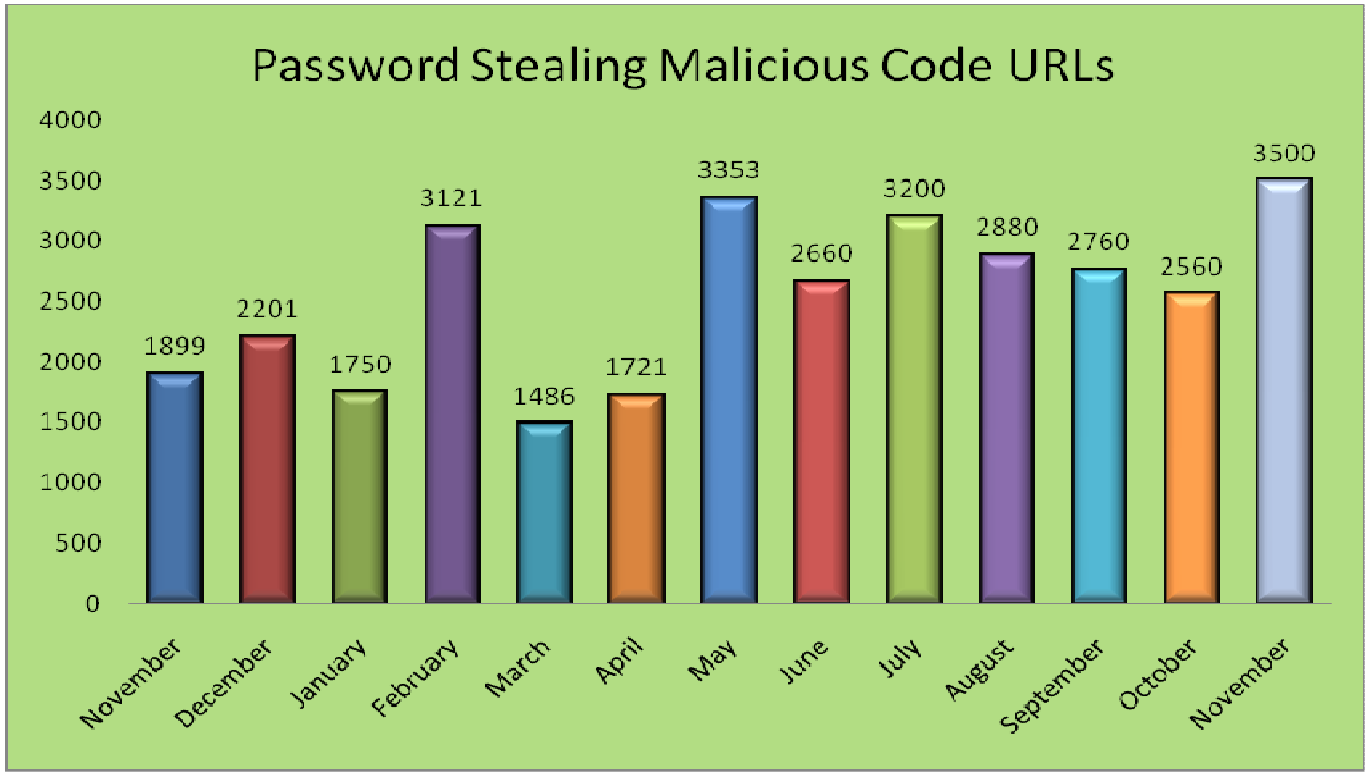
More countries being added to APWG's list of host countries every year, but US runs close to half of the sample from month to month, passed this year in one month period by China

Crimeware: Slow Fade to Invisibility



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 technologies

Trend: Emphasis on Increasing Websites to Spread Crimeware



Botnet researcher Randy Vaughn of Baylor University reports that all indications are that crimeware is achieving deeper and broader geographical distribution - increasingly so in the last 18 months

Measuring the Total Threat Scope of ID Theft and eCrime

Scope of Threat

- Phishing scams started with ‘white plastic’ card schemes using phished data for small-scale, high-volume thefts against ATM cards
- But phishing and other ecrime is being used to inflict much larger and more important individual and corporate losses today
- Tomorrow some forms of phishing could even substantially distort investment markets, injuring many investors and stock-held 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 (if there is one on the house)
      - Apply on line for a new one
      - Go to closing and walk away
- Next?
  - Loans against more real assets of persons and businesses:
    - Boats
    - Planes
    - Private Businesses
      - » Business Assets and Property

Enterprise Threat

- Corporate treasury accounts are under attack
  - Increasing reports in the last year 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 criminal gangs
    - 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: conclusively determining insider collusion in a corporate phishing attack – and measuring the risk of that uncertainty*

Enterprise Threat – Customer Data

- Customer Data and Data Assets in Company's Care are Prime Targets
  - 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
- In both cases the data was valuable for creating much more focused and convincing phishing attacks

Enterprise Threat – Intellectual Property

- 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
- Methods
  - Emails with attachments bearing crimeware payloads to infect PCs and intercept credential data
  - CD-ROMs mailed directly to targeted employees, also with crimeware payloads to infect PCs and intercept credential data

Investment Markets Threat

- Internet ‘pump and dump’ scams on penny stocks 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 criminal profits of $121,500 and damages of more than $875,000
- How long before scammers use more undetectable techniques to move markets to their favor, the way they have crafted hard-to-detect crimeware?

- 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
  - Or go to http://www.antiphishing.org and click on the owl
- Reports from INTERPOL, APJ, global CERTs and worldwide security and technology companies and researchers
- DNS Registry policy
- International case studies
- Much more. . .

Thank You

- Peter Cassidy
- pcassidy@antiphishing.org
- +1 617 669 1123 (US)
- +44 (0)753 002 1313 (Until Thursday)