



# **Online Threats: Brandjacking and Security Landscape**

**Matt Serlin**  
**Senior Director, Domain Management**  
**MarkMonitor**

**June 2010**

# Agenda

- About MarkMonitor
- Brandjacking 2009 Year in Review
  - Brand abuse trends
  - Phishing statistics
- Recent Domain Name Security Breaches
  - Understanding the Vulnerabilities
  - Mitigating the Risks
- Domain Security Best Practices

# About MarkMonitor

- Experience and expertise
  - Founded in 1999 - 10+ years experience protecting brands
  - ICANN accredited registrar
  - Unique corporate-only approach
- Customer-focused market leader
  - 50+ of Fortune 100
  - 5 of 6 most trafficked Internet sites under management
- Global Presence
  - San Francisco, Boise, London, New York, Los Angeles, Washington DC

*Most Trusted Corporate Domain Name Registrar*



# Brandjacking 2009 Year in Review

# Brandjacking Index Overview

- Tracking 30 of the most popular brands as ranked by Interbrand
- Weekly sampling of more than 225,000 potential brand abuse incidents conducted throughout 2009 for the overall brand analysis
- Nine vertical segments (Automotive, Apparel, Media, Consumer Packaged Goods, Consumer Electronics, Pharmaceutical, Food & Beverage, High Tech and Financial) for the overall brand analysis
- Spam feeds from leading international Internet Service Providers (ISPs), email providers, and other alliance partners to detect phishing and other fraud

# Incidents of Abuse Across Top 30 Brands

Threat Type	Q1-09	Q2-09	Q3-09	Q4-09	YOY
Cybersquatting	215,820	221,927	225,524	229,498	8%
Pay Per Click Scams	34,317	35,299	34,862	36,359	8%
eCommerce	25,148	28,206	24,489	24,648	0%
Offensive Content	1,586	1,609	1,297	850	-49%
False Association	87,095	89,327	82,899	136,430	57%

# Quarterly Brand Abuse by Industry

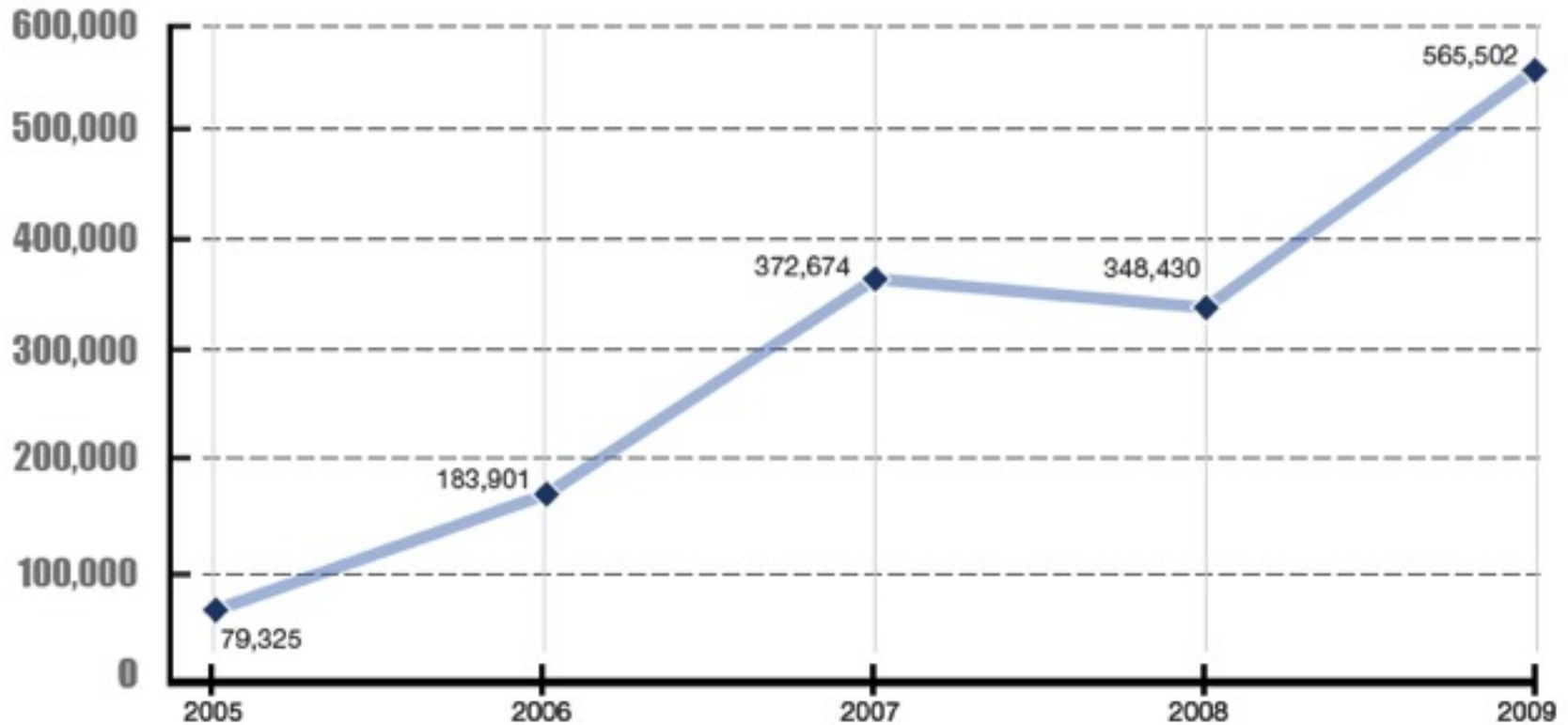
Industry	Q1-09	Q2-09	Q3-09	Q4-09	YOY
Apparel	5,084	5,271	5,352	5,640	14%
Auto	14,000	14,405	14,505	14,950	7%
Consumer Electronics	7,733	7,972	8,110	8,306	6%
CPG	1,544	1,598	1,636	1,714	13%
Financial	4,675	4,693	4,728	4,750	2%
Food Beverage	4,230	4,314	4,370	4,458	7%
High Tech	6,029	6,210	6,323	6,505	10%
Luxury	2,551	2,655	2,796	3,076	23%
Media	21,280	21,927	22,966	22,747	14%

# Geographic Location of Sites Hosting Abuse

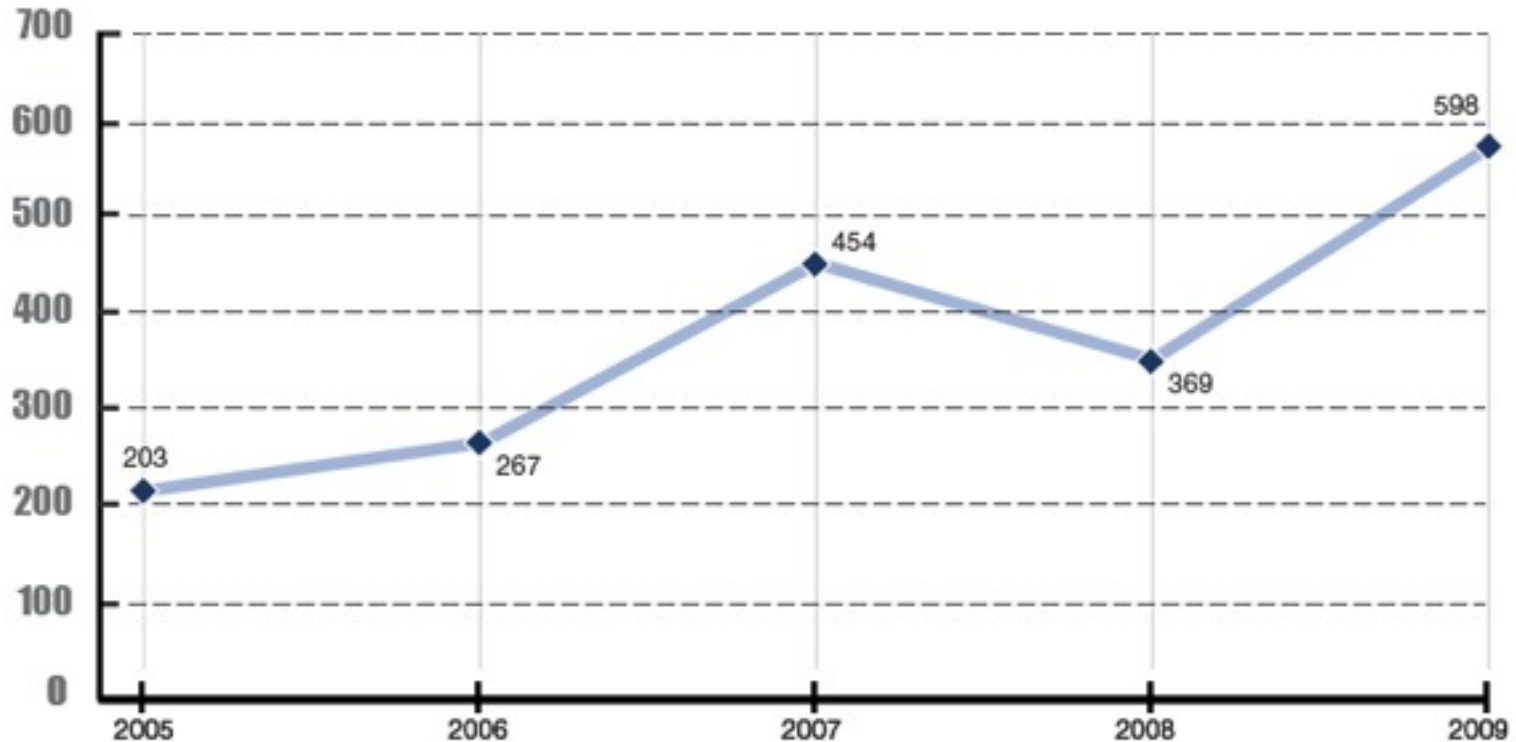
Country	Domains	% of Domains
United States	151,045	69%
Germany	14,747	7%
United Kingdom	10,017	5%
Canada	5,892	3%
Japan	4,035	2%
Netherlands	3,379	2%
Korea, Republic of	2,821	1%
France	2,707	1%
China	2,451	1%
Cayman Islands	1,833	1%
Other	19,192	9%



# Phishing Trends



# Record Levels of Phish Attacks per Organization





# Domain Name Security Issues

# Domain Name Security Breaches on the Rise

- Hackers now recognizing that domain security can be breached
- Registries and registrars are exploited as technical and social vulnerabilities are uncovered
- Attacks against domain registrants are resulting in compromised credentials

# Various Vulnerabilities Exploited



The screenshot shows a CNET News article from April 27, 2009, at 4:23 PM PDT. The article is titled "Puerto Rico sites redirected in DNS attack" and is written by Elinor Mills. It discusses a DNS attack on the main domain name system registrar in Puerto Rico, which led to the local Web sites of Google, Microsoft, Yahoo, Coca-Cola, and other big companies being redirected for a few hours on Sunday to sites that were defaced, according to security firm Imperva. The article also mentions that these sites and others including PayPal, Nike, Dell, and Nokia, were redirected to sites that were black except for messages in hacker lingo saying that the sites had been hacked. However, the sites themselves were not hacked, Amichai Shulman, chief technology officer at Imperva, said on Monday. A group calling itself the "Peace Crew" claimed that they used a SQL injection attack to break into the Puerto Rico registrar's management system, he said. "We're seeing more and more of these DNS-related attacks and seeing them scale up," he added. While the sites that visitors were redirected to were obviously not the legitimate sites, DNS redirects could be used to send unsuspecting Web surfers to phishing sites pretending to be banks where they would be prompted to provide sensitive information. People should use the SSL (Secure Sockets Layer) protocol for encrypting communications with sensitive sites and use anti-phishing technology in the browser that colors part of the URL address bar green or red based on the safety level of the site being visited. Calls to Gauss Research Lab, the organization that manages Puerto Rico's top-level domain, were not answered late on Monday.



The screenshot shows a ZDNet article from April 21st, 2009, titled "Hackers hijack DNS records of high profile New Zealand sites". The article discusses a DNS hijacking of high profile sites such as Comcast, Photobucket, and ICANN/IANA domains that were taking place last year. Similar incidents are still happening. Today, a web site defacement group known as "The Peace Crew" has successfully hijacked the DNS records for high profile New Zealand web sites, through what Zone-H claims to be a SQL injection at New Zealand's based registrar Domainz.net, in order to redirect the visitors to a defaced page featuring the infamous Bill Gates pieing photo, as well as anti-war messages. The mass defacement affected major Microsoft sites in New Zealand including WindowsLive.co.nz, MSN.co.nz, Microsoft.co.nz, Hotmail.co.nz, Live.co.nz next to HSBC.co.nz, Sony.co.nz, Coca-Cola.co.nz, Xerox.co.nz, Fanta.co.nz, F-Secure.co.nz and BitDefender.co.nz.

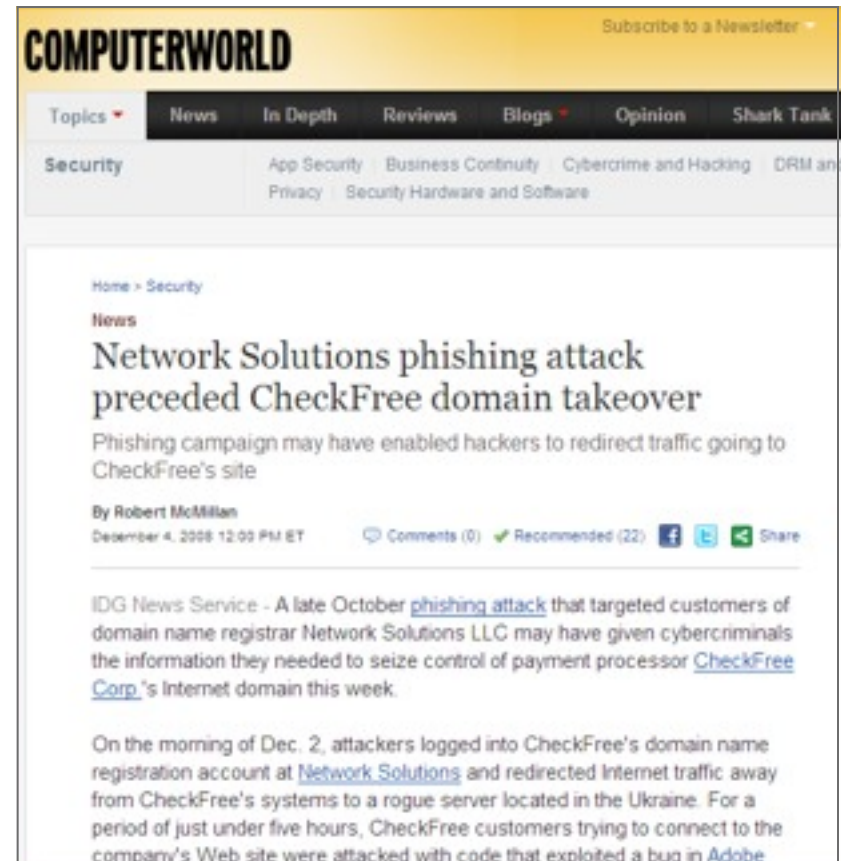
# Social Engineering Attacks

- Registrars need to evaluate how weak their human links are
  - Many are lax enough to be easily victimized by simple social engineering tricks
  - In many cases, a user ID and password is all that is needed



# Phishing Attacks

- Domain administrators can be tricked by phishing
  - Customers of Network Solutions were sent an email asking for their IDs and passwords
  - It is believed that one respondent was an employee of CheckFree
    - Information obtained gave the phishers the opportunity to redirect CheckFree's customers to a rogue server located in the Ukraine for 5 hours



# Malware

- The most recent development in domain name attacks is the targeted deployment of malware, such as keyloggers sent to corporate domain name administrators
- Keyloggers track logins and passwords for corporate domain name management portals
- With this credential information, scammers can
  - Unlock and hijack domains
  - Update name servers, or even change DNS settings
  - Effectively take sites down
  - Infect unsuspecting website visitors with malware



# Targeting Domain Related Vulnerabilities

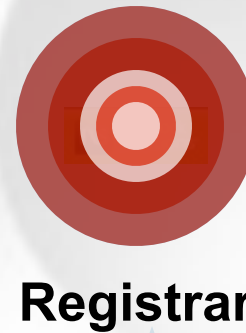
Hacker



- Social Engineering Attacks
- Infrastructure Breaches



DNS Administrator



Domain Administrator

- Infrastructure Breaches
- Process Exploits

- Social Engineering Attacks
- Domain Hijackings
- Infrastructure Breaches



- Credential Theft
- Identity Theft

# Securing Domain Related Vulnerabilities

Hacker



MarkMonitor



- Early Detection
- Ability to Quickly Respond

Registry



DNS  
Provider

- Operational Policies
- Hardened Infrastructure
- Two-Factor Authentication
- IP Address Restrictions



Registrar

- Operational Policies
- Third-Party Evaluations
- Hardened Infrastructure
- Two-Factor Authentication
- IP Address Restrictions
- Portal Locking
- Registry Locking

DNS  
Administrator




Domain  
Administrator



- Portal Locking
- Registry Locking

- Two-Factor Authentication
- IP Address Restrictions



# Mitigating the Risks – What we tell Clients

# Consolidate Domain Names

- Gain visibility into entire portfolio and protect against loss due to expiration, disgruntled employees or erroneous changes
- Compare trademark registrations against domain registrations
- Utilize Reverse Whois to uncover domain names by searching registrant name, nameservers, e-mail addresses and phone numbers
- Identify and contact individuals within the organization who are registering names:
  - Legal, IT, Marketing, E-Commerce, subsidiaries, divisions, etc.

# Utilization of Hardened Registrar

- Ensure that your registrar employs a “hardened” portal – one that employs constant checks for security and code vulnerabilities the same way the web security team does for your websites
- The registrar must have a track record of being able to stay on top of new exploits, and of researching and understanding new vulnerabilities
- In addition, the registrar must be able to demonstrate use of strong internal security controls and best practices.

# Registrar Domain Locking

- An elevated locking mechanism, sometimes referred to as a “Registrar Lock” or a “Super Lock,” that essentially freezes all domain configurations until the registrar unlocks them as the result of the completion of a customer-specified security protocol
- Companies can determine the level of complexity associated with their protocol and domains are made available for updating through the portal only when these security protocols are accurately completed
- This extra level of security should be applied to your most mission-critical domains such as transactional sites, email systems, intranets, and site-supporting applications

# Registry Domain Locking

- “Registrar Locking” can still be exploited by an attacker who updates name servers, thereby redirecting customers to illegitimate websites without transferring actual control of the domain from one registrar to another
- To combat this, another step is “registry locking,” or “premium locking,” which makes the domain unavailable for any updates at all
- This method of locking is currently available only for .com and .net registrations
- Where possible, Registry Locking should be applied to domains used for transactional sites, email systems, intranets, and site-supporting applications

# Domain Security Best Practices Checklist

- Employ two-factor authentication for accessing domain management portal
- Employ two-factor authentication for accessing DNS management portal
- Never share login credentials for your domain or DNS management portals
- Lock mission critical domains at the registry level, where possible
- Disable ability to edit core domains for all users
- Continually manage and review secondary user accounts
- Require mandatory password updates
- Implement IP access restrictions
- Receive automated notifications of every domain name update
- Utilize a corporate-only, hardened registrar





# Questions?