Brandjacking Index™

Summer 2007

MarkMonitor®

MAKING THE INTERNET SAFE FOR BUSINESS

Brandjacking Index

Summer 2007

Contents

Contents Cont.

Executive Summary

Criminals around the world continue to take advantage of the Internet to hijack well-known brands for their own profit. MarkMonitor® created the Brandjacking Index™ to measure how pervasive these attacks are and to identify the potential threats to the world's strongest brands. As in our inaugural report released in April, this Summer 2007 edition of the Brandjacking Index tracked millions of emails and billions of web pages to determine that exploits of all types are increasing, and some such as domain kiting have more than tripled since our first report.

This second edition of the Brandjacking Index includes a research focus on the online pharmaceutical market and shows how questionable business practices are more the norm than the exception. The vast majority of online sites selling the most popular prescription drugs are operating without proper credentials from the pharmacy regulatory bodies. Furthermore, our findings indicate that some of the drugs being sold on these sites may be fake, expired, stolen, diluted or alternatives. Finally, these sites do not use best practices for Internet security. Visitors to these sites in search of cheap medications are likely to compromise their credit card identities as well as their health.

We conducted three different types of analysis for this Summer 2007 Brandjacking Index: our quarterly analysis of Internet brand abuse that examines issues such as cybersquatting and domain kiting as well as a separate phishing analysis. We also examined the online pharmaceutical market in detail by analyzing specific brand abuse based on six popular drug brands.

Summary Findings

Pharmaceutical Brand Abuse

Buying prescription medications, especially in the U.S., can be costly, and many consumers are looking at ways to cut costs by getting their drugs online. However, the online dispensaries are a risky business, indeed. There are three major types of abuse that MarkMonitor has encountered:

- Questionable online pharmacies
- Spam messages
- Threats to the pharmaceutical supply chain

We found that the business practices at many online pharmacies are spotty at best, and traffic intended for legitimate web sites is being diverted to suspicious sites, diluting overall brand and marketing efforts. Many online pharmacies fake their accreditation deliberately, and so it is almost impossible for a visitor to know their provenance. And with the recent confirmed death of one Canadian woman[1] who ingested questionable drugs that she bought online, it is clear that buying drugs online can be hazardous to one's health unless shopping at a properly accredited online drugstore.

1 See the article " Internet Drug Death A Warning To Canadians," published 7/11/07 here: http://www.medicalnewstoday.com/articles/76431.php

We tracked more than 100,000 drug-related spam landing sites during June 2007, and found almost 400 listings on online business-to-business exchanges for the six drug brands in the study. On a daily basis, more than 6,000 unique sites originated these spam messages, with more than half of this traffic originating in China and the Russian Federation. Peak volume of spam messages measured almost 11,000 unique originating sites.

Further forensic analysis of the pharmacy sites and pricing practices led to troubling insights on the risks to consumers' health and identity information from sales of these drugs. Information gathered during the study indicated some of the drugs being sold were fake, expired, stolen, diluted or alternative.

While we can't determine whether the medications these online sites sell are real, there are strong indications that they aren't: a tenth of the sites boldly proclaim "no prescription required" and only four out of more than 3,000 sites have Verified Internet Pharmacy Practice Site (VIPPS) accreditation.[2] The most damaging indication? The average prices for medications in the study are about a fifth the price of the certified sites.

The problem is worse than just the volume of drug-related spam, and brings a level of risk to consumers' identity information during the shopping process as well as to consumers' health. We analyzed the actual servers hosting these pharmacy web sites and found that the majority of these do not protect customer transaction data with SSL (Secure Socket Layer) encryption. More than 20% of the post-purchase email captured in our analysis contained links to unprotected customer data.

The problem isn't confined to the retail drug dispensing vendors, but extends to the drug exchanges and drug distribution channel as well. These exchanges pose a serious risk to corrupting the overall drug supply chain, compromising product delivery by injecting phony or dangerous medications into the retail network.

Phishing

Phishing continues to be very profitable for scammers and is growing in three different and alarming directions. First, there is continuing growth in the number of organizations phished with a 45% increase in the second quarter of 2007 as compared to a year earlier. Financial sites continue to draw the majority of interest by phishers, representing 41% of total targeted brands. Higher-value targets are of particular interest to the Rock Phish Gang, so named because a group of criminals originally used "rock" in many of their URLs. Second, this group is focusing more attention on commercial banking credentials to facilitate larger monetary transfers and, potentially, money laundering. By June, almost 80% of all Rock Phish Gang activity was directed to commercial banking targets. Finally, the average phisher is becoming more sophisticated and adopting the technical rock phishing techniques of using multiple URLs more often as a means of avoiding browser security checks.

2 See http://www.drugstore.com/qxc52227_333181_sespider/concerns_about_illegal_online_pharmacies/concerns_about_illegal_online_pharmacies.htm

Brandjacking Trends

The risk for consumers being directed to a phony domain or web site continues to remain high and the number of attacks continues to increase in raw numbers and in sophistication (see the table below). Cybersquatting still accounts for the largest number of individual abuse cases, with more than 300,000 incidents reported in the second quarter of 2007. But the biggest increase in attacks is from domain kiting, the practice of exploiting a 'loophole' in the ICANN processes to setup and "own" a domain for a few days and then drop the ownership without actually paying for the domain. This practice, which saw a whopping 242% growth from the first to the second quarter, is often used by cybersquatters to divert legitimate traffic and squeeze pay-per-click revenue from well-known brands.

Summary Statistics

Threat Type	1Q-07 Results	2Q-07 Results	%Change
E-Commerce Sites	21,093	22,639	7%
Cybersquatting	286,801	311,050	8%
False Association	75,167	107,316	43%
Pay-Per-Click	50,743	73,774	45%
Offensive Content	1,395	2,138	53%
Domain Kiting	11,015	37,634	242%

Methodology and Background

The Brandjacking Index is produced quarterly by MarkMonitor and explores numerical trends and statistics about brand abuse. It contains anecdotal information about the business and technical methods used by brandjackers, along with analysis and discussion of the business and social implications of brand abuse.

The cornerstone of the Brandjacking Index is the volume of public data analyzed by MarkMonitor using the company's proprietary algorithms. MarkMonitor searches approximately 134 million public records and up to 16 million unique daily phishing email solicitations for brand abuse. These records come from various public domain data sources, along with Internet feeds and fraud broadcasting from leading international Internet Service Providers (ISPs), email providers and other alliance partners. None of this data contains proprietary customer information.

This report is based on the following information and analysis:

- Tracking 30 brands as ranked by Interbrand
- Weekly sampling conducted April through June 2007 for the overall brand analysis, and samples conducted during June 2007 for the pharmaceutical analysis
- Nine vertical segments (Automotive, Apparel, Media, CPG, Consumer Electronics, Pharma, Food & Beverage, High Tech and Financial)
- Insights based on an average of weekly samples of incidents
- More than 650 million email inboxes monitored with the largest ISPs and up to 16 million unique suspect daily emails studied for the phishing analysis

For the online pharmaceutical market analysis, MarkMonitor focused on six popular prescriptions drugs – three of the most popular drug brands according to trade industry reports along with three of the most searched-for drugs on popular search engines. Based on these drug brands, more than 3,100 online pharmacies were identified as selling one or more of the drugs to consumers while 390 individual listings on bulk exchange sites were identified.

Conclusions

As long as consumers are motivated to shop for cheap drugs, unscrupulous online pharmacies will continue to proliferate and take their money, risking consumer health and financial well-being. Overall, brand abuse is increasing, but more important than the sheer volume is the rise in the level of sophistication and the use of best practices by online criminals and fraudsters. Along with the increasing complexity of attacks is a continued increase in the number of phishing attempts, the number of brands targeted and use of multiple attacks from single domains.

Brandjacking Findings

Drug Brands & Channel Abuse

Methodology

- Six leading drug brands
  - Three highest ranking drug products*
  - Three most frequently searched drug products
- Web sites and spam
  - Billions of web pages searched
  - 60 million email solicitations (spam) processed
  - Data from four-week analysis (June 2007)
  - Electronic forensic analysis
  - NO customer data used in study

Observations

- Problem of scale
  - Six brands reviewed, 6,000 unique domains daily
  - Up to 11,000 unique domains at peak
  - Classic case of traffic diversion
- Online pharmacies
  - Questionable business practices
  - Poor Internet security
- Trade and exchange sites
  - Outside established distribution channels
  - High volumes and low prices
- Strong evidence of illicit versions of known drugs

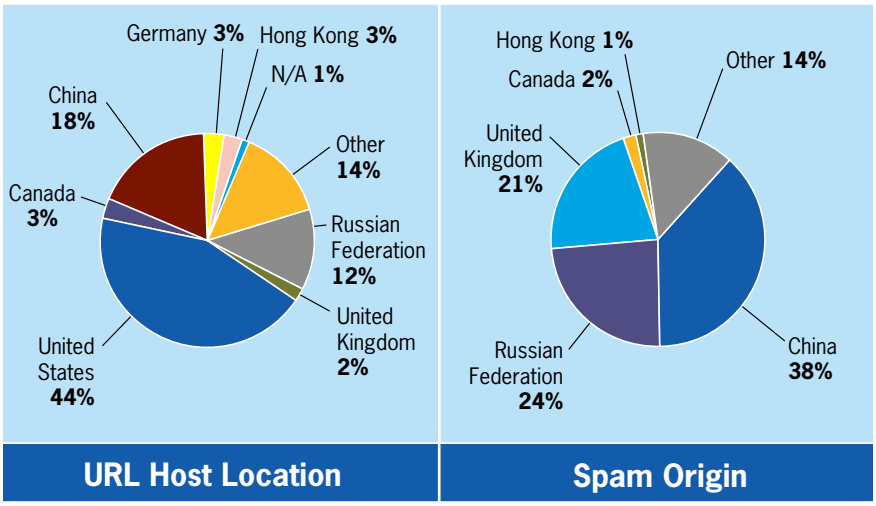
Summary

- Analysis of six top drug brands in June 2007

Threat	Results
Spam landing sites	110,902
Online pharmacies	3,160
Exchange/trade listings	390

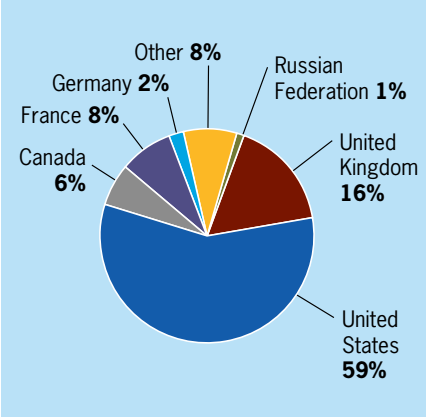
Spam

- Large scale: 6-11K unique sites daily
- 44% of spam landing sites hosted in the U.S.
- 38% of spam from China



Landing Sites

- 110K landing web pages
- 7,090 unique domains



Online Pharmacy Hosting by Country, Q2 '07

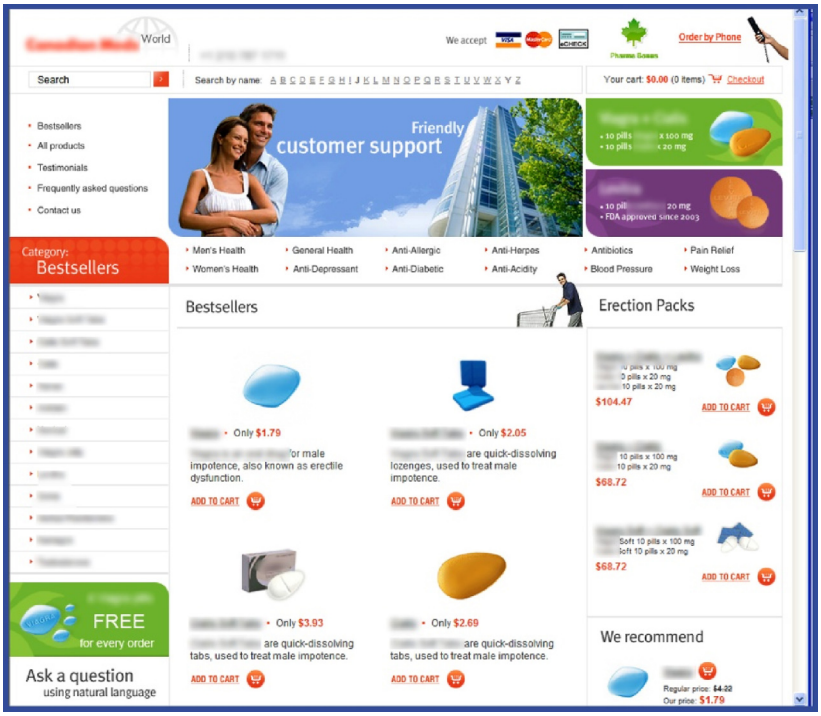
Online Pharmacies

- 3,160 online pharmacies
- One-third have Alexa rankings
- 32K average daily visitors per ranked site
- Four of 3,160 pharmacies are VIPPS certified
- > 50% do not protect customer data
- 10% of sites state: "No prescription required"
- U.S. hosts 59% of the sites
- Estimated $4 billion* in annual sales from ranked sites

* Based upon total annual traffic, 0.5% conversion rate, $70 average transaction

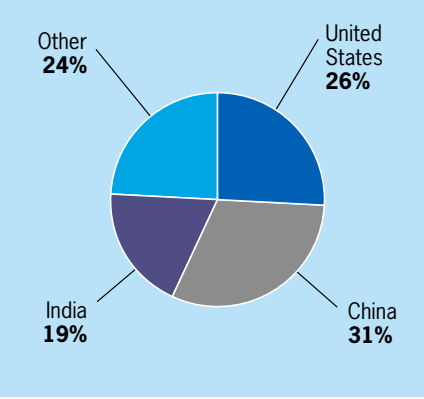
Online Pharmacies - site example

- "Canadian" online pharmacy with host server in Russian Federation
- Faked accreditation and certification
- Selling individual pills



Online Pharmacy Product Integrity

- Universe
  - Random sample of 30 non-certified pharmacies
  - 4 VIPPS certified pharmacies
  - 1 drug brand, same quantity across all listings
- Findings
  - VIPPS certified average price $10.85 and $2.10 range of variance
  - Non-certified average price $2.72 with $2.78 range of variance
- Conclusions
  - 75% discount from non-certified pharmacies
  - Much higher than channel discounts
  - Strongly indicative of fake, stolen, alternate, expired, gray market or diluted drugs



Exchange Listing by Origin, Q2 '07

Exchange Sites

- 390 exchange listings
- 21 listings analyzed
- 75 million pills available
- $150 million value*
- China is the primary source (31%)

* Estimated $2 per pill

Exchange Listings

- Site hosted in India
- $1.50 per pill
- Retail price for example is over $10 per pill
- This example is most likely fake, expired, stolen, alternate, gray market, or diluted

Phishing

Trends & Statistics

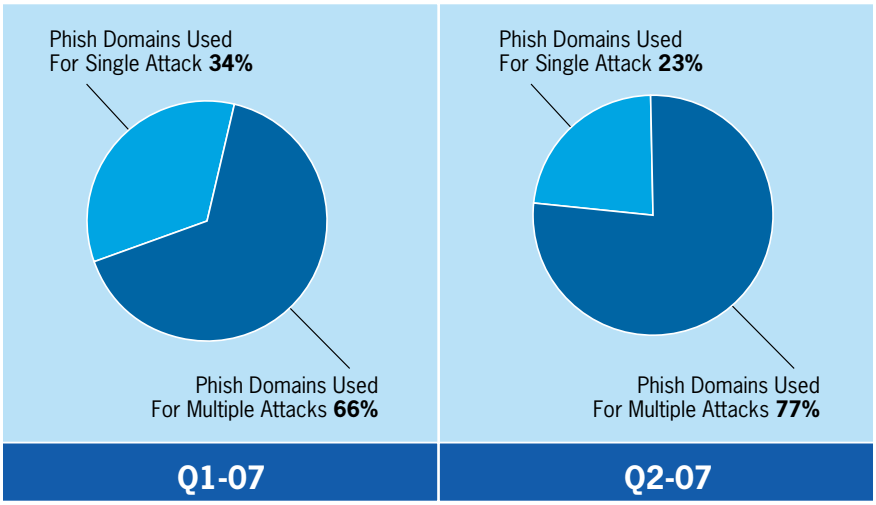
- Phishing data collected since November 2004
- 671MM email inboxes monitored in partnership with largest ISPs
- Up to16 million unique suspect emails processed daily
- Phishing threat analysis
- Vertical segment data
- Geographic segmentation

Observations

- Rock phish techniques are on the rise
- More criminals using successful rock phish methods
- Techniques target consumer security tools in browsers
- Tactics indicate sophisticated IT resources and infrastructure
- Rock Phish Gang seeks higher value targets such as commercial bank accounts for larger gains
- Creating business infrastructure to launder fraud proceeds
- Continued growth in number of organizations phished
- Diversity in targets
- Diversity of fraud

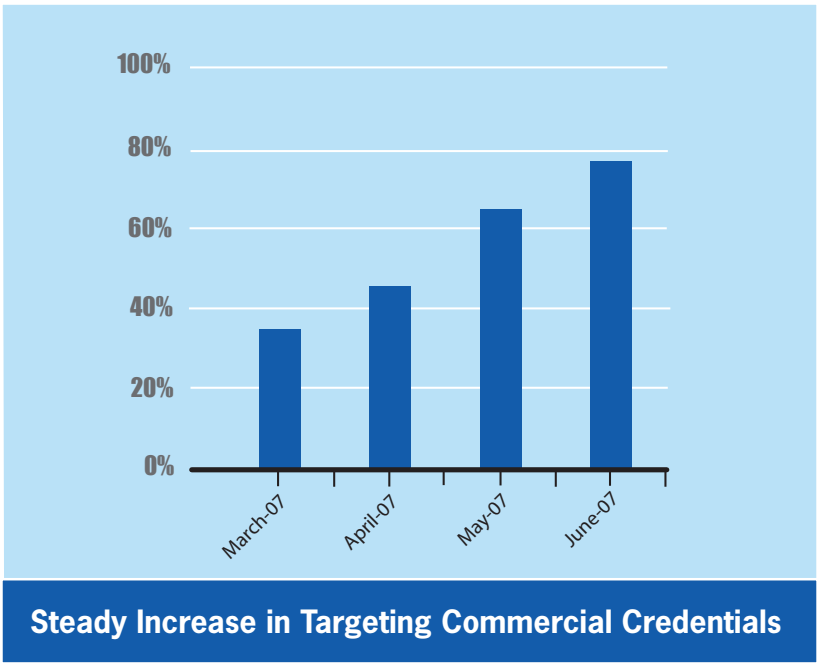
Rock Phish Tactics

- Further adapting to browser blocking of URLs
- Rise in multiple attacks hosted from one domain – key tactic of rock phishers
- 11% jump from Q1-07 to Q2-07



Rock Phish Gang

- Rock Phish Gang focusing on commercial accounts (77%)
- High value fraud
- Money laundering

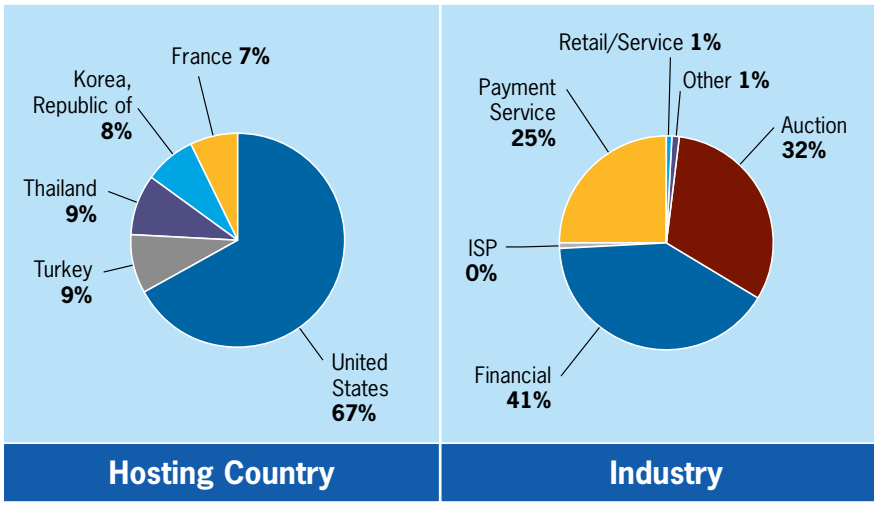


Increasing Number of Brands Targeted

- 45% increase in organizations targeted (Q2-06 to Q2-07)
- 8% increase in organizations targeted (Q1-07 to Q2-07)
- 240 organizations targeted in May 2007
- 189 new targets in Q2-07, 83% increase from Q1-07

Hosting Country and Industry

- Rock Phish Gang focusing on commercial acU.S. leads hosting countries with 67% of web sites
- 41% of all phishing attacks (unique URLs) targeted financial sector
- New targets for Q2-07 include Thailand, Turkey, and France



Brand Abuse

Methodology

- Brand abuse and phishing
- 134 Million domain records daily
- Billions of web pages searched
- Data sources
- Tracking 30 brands from Top 100 Interbrand study
- Weekly sampling from April - June, 2007
- 9 vertical segments (Automotive, Apparel, Media, CPG, Consumer Electronics, Pharmaceuticals, Food & Beverage, High Tech, and Financial)
- Over 300K abuse results weekly
- NO customer data used in study

Observations

- Growth of abuse continues – cybersquatting tops the list of threats with 311K incidents
- Consumers face an increasing risk of accidentally doing business with someone other than their trusted brand
- It is getting harder, not easier, to abate the problem
- Kiting is the fastest growing form of abuse
- Kiters are using adaptive and evasive practices
- Kiting allow cybercriminals to save money
- Kiters can avoid prosecution from brand holders for typosquatting and cybersquatting

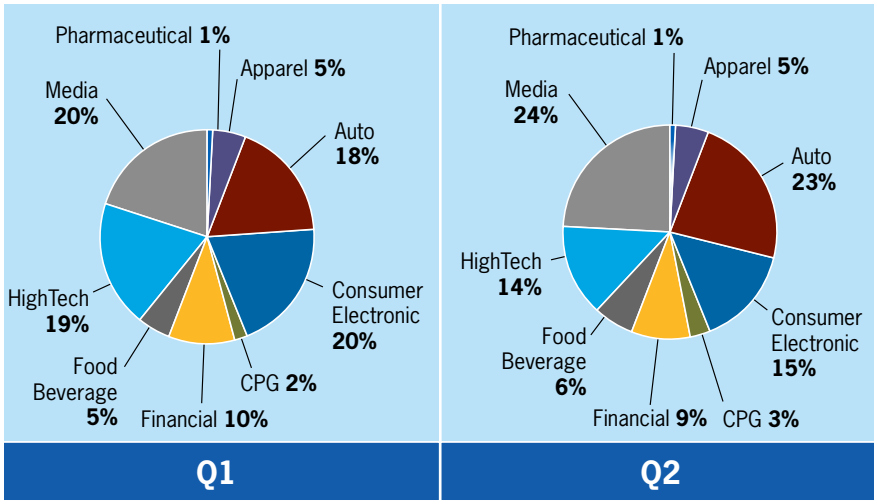
Summary

Threat Type	1Q-07 Results	2Q-07 Results	%Change
E-Commerce Sites	21,093	22,639	7%
Cybersquatting	286,801	311,050	8%
False Association	75,167	107,316	43%
Pay-Per-Click	50,743	73,774	45%
Offensive Content	1,395	2,138	53%
Domain Kiting	11,015	37,634	242%

* Threat types are not exclusive of other threats. Data is based on weekly samples averaged over one quarter.

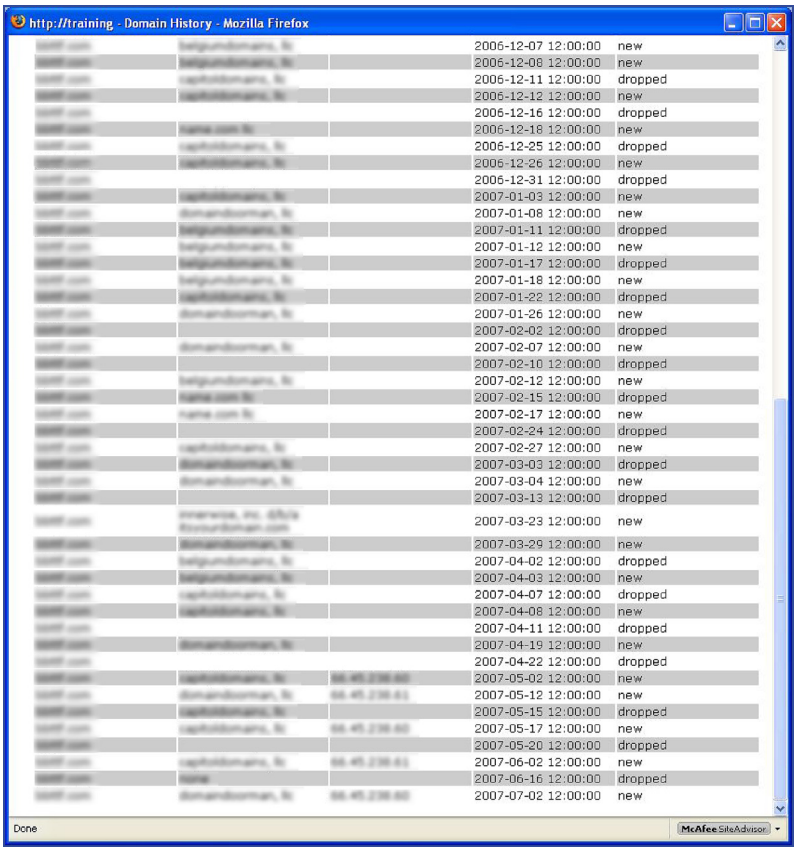
By Industry Segment 2007

- Media still leads all segments with 24% of abuse
- Automotive is the fastest growing segment (18% in Q1-07 to 23% in Q2-07)



Kiting Growth

- Substantial rise in kiting incidents
- Kiters are adaptive, avoiding enforcement techniques
- Rotating registrars (round robin registrations)
- Registration fallow periods
- Certain registrars are ignorant, cooperating, or turning a blind eye to abuse
- Kiting registrars make it difficult to identify abusers



Round Robin Registration Example

Summary

- Drug Brands & Channel Abuse
  - Problem of scale
  - Online pharmacies have questionable business practices and poor Internet security
  - Trade and exchange sites are outside established distribution channels
- Phishing
  - Rock phish techniques are on the rise
  - Rock Phish Gang targeting commercial bank accounts
  - Continued growth in number of organizations phished
- Brand Abuse
  - Consumers face an increasing risk of accidentally doing business with someone other then their trusted brand
  - Kiting has increased, using adaptive and evasive practices

Glossary

Brandjacking – To hijack a brand to deceive or divert attention; often used in abusive or fraudulent activities devised for gain at the expense of the goodwill, brand equity, and customer trust of actual brand owners.

Cybersquatting – The registration of domain names containing a brand, slogan or trademark to which the registrant has no right.

Domain Kiting - The process whereby domains are registered and dropped within the 5 day ICANN grace period, and then registered again for another 5 days. Kiting a domain lets the registrant gain the benefit of ownership without ever paying for the domain.

E-commerce Content – Web sites containing a specified brand that appears in visible text, hidden text, meta tags or title in conjunction with other site content that indicates online sales are being transacted on the site.

Offensive Content – Web sites containing a specified brand that appears in visible text, hidden text, meta tags or title in conjunction with pornographic, online gaming or hate content.

Phishing – Criminal use of email to divert traffic to Web sites in order to fraudulently acquire usernames, passwords, credit card details, and other personal information. The email and Web sites used in these operations employ "social engineering" techniques to trick users into believing they are interacting with a business or organization that they trust.

PPC (Pay-Per-Click) – Paid placement advertising appearing on Web pages. Operators of Web sites hosting PPC advertising derive revenue from ads that are clicked, hence the name PPC.

Traffic Diversion – The use of brands, slogans or trademarks located in visible text, hidden text, meta tags and title in order to manipulate search engine rankings so that the brandjacker's site can gain a more favorable search engine placement.

MarkMonitor®
MAKING THE INTERNET SAFE FOR BUSINESS

PRESS CONTACTS:

Te Smith, MarkMonitor
(831)-818-1267 (mobile)
(415) 278-8400 (office)
te.smith@markmonitor.com

Jonathan Jordan,
A&R Edelman for MarkMonitor
(240)-483-6986 (mobile)
(202)-370-6187 (office)
jjordan@ar-edelman.com

About MarkMonitor

MarkMonitor, the global leader in enterprise brand protection, offers comprehensive solutions and services that safeguard brands, reputation and revenue from online risks. With end-to-end solutions that address the growing threats of online fraud, brand abuse and unauthorized channels, MarkMonitor enables a secure Internet for businesses and their customers. The company's exclusive access to data combined with its real-time prevention, detection and response capabilities provide wide-ranging protection to the ever-changing online risks faced by brands today. For more information, please visit www.markmonitor.com.