MarkMonitor®

February 1, 2008

Susanne R. Sene
Office of International Affairs
National Telecommunications and Information Administration
1401 Constitution Avenue, NW 4701
Washington, D.C., 20230

Re: **Midterm Review of the Joint Project Agreement with ICANN**

Dear Ms. Sene:

MarkMonitor is pleased to submit this response to the National Telecommunications and Information (NTIA)'s inquiry in connection with its midterm review of ICANN under the Joint Project Agreement with ICANN.

First and foremost, MarkMonitor recognizes the significant progress that ICANN has achieved since its creation, and under the JPA. As an ICANN accredited registrar since 2000 serving over 50 of the Fortune 100 through its corporate domain management, anti-phishing and online brand protection solutions, MarkMonitor has a unique vantage point to observe ICANN's performance on issues that protect consumers against online identity theft, as well as issues that impact registrars, multi-national corporations and other Internet users. It is from this perspective that these comments are respectfully submitted.

ICANN's progress includes enabling the explosive growth and competition in the domain name system, providing opportunities for billions of global businesses and consumers to engage in online commerce, and to freely express their political, religious and social opinions without burdensome government intervention. This is a remarkable accomplishment, given the international structure of ICANN.

However, along with this tremendous growth came an exponential growth in illegal and criminal online conduct, such as cybersquatting, domain tasting, phishing, malware, and other forms of online fraud. Much of this abuse originates from the domain name system. The MarkMonitor Brandjacking Indexes published last year (copies attached) highlight this abuse targeting the world's largest brands. The results are breathtaking, indicating a pervasive and systematic abuse of the domain name system.

303 Second Street
Suite 800N
San Francisco, CA 94107

415 278 8400 tel
415-278-8445 fax
www.markmonitor.com

For example, phishing attacks are on the rise, with over 38,000 unique incidents in September, 2007, targeting over 150 brands in the financial, retail and ISP industries. The recent rise of domain name enabled fast-flux networks spurred the notorious rock-phish attacks that have left the financial industry reeling, and exposed the personal information of numerous consumers worldwide. Yet despite this significant threat to the integrity of the Internet for online commerce, ICANN has not provided leadership or policy recommendations to counter this threat. We believe that the international reach of the phishing epidemic makes ICANN the ideal venue to tackle cyber-security risks involving the domain name system.

In 2007, a new form of domain related abuse emerged as a major threat to the integrity of the Internet. Domain tasting, made possible through abuse of ICANN policy, targeted the world's largest brands, causing significant damage to major corporations and confusion to consumers. In the second quarter of 2007, the top 25 brands experienced an average of 38,634 instances of domain tasting diverting Internet traffic and pay-per-click revenues to the registrant. In the study period, these top brands experienced an average of 311,050 unique instances of cybersquatting. The breadth and scale of this abuse leaves brand owners powerless to protect their brand. Traditional remedies such as lawsuits under the Anti-cybersquatting Consumer Protection Act or ICANN's Uniform Dispute Resolution Policy are no longer effective to combat abuse of this scale. The highly publicized lawsuits against domainers and ICANN accredited registrars commenced by companies such as Dell, Verizon and Microsoft highlight the damage caused by these activities. Although the recent fee recommendation by ICANN is a positive step in response to domain tasting, the scale of the problem calls for a more immediate and comprehensive response to domain tasting and the other types of abuses highlighted above.

ICANN's core values include "(p)reserving and enhancing the operational stability, reliability, security, and global interoperability of the Internet." The examples highlighted above cause consumers and businesses throughout the world to question the safety, security and integrity of the Internet. While ICANN tends to interpret this core value from a technical perspective, we maintain that it should encompass much more, such as the security and integrity of the Internet for online transactions. Indeed, when faced with issues that highlight this concern (such as WHOIS), ICANN often overlooks the concerns of businesses combating cyber-security issues for their customers.

The U.S. government is committed to ensuring the stability and integrity of the Internet, and the accountability of abusers of the Internet who harm online commerce and consumers worldwide. Continuing the JPA with ICANN is essential to focus ICANN's energies to address cyber-security issues in a prompt and meaningful manner such as through (i) the creation of policies to combat domain based phishing, (ii) the preservation of freely accessible WHOIS information to hold accountable registrants engaged in illegal online activities, and (iii) the engagement of dialogue with businesses who protect consumers from online fraudulent and criminal activities on a daily basis.

303 Second Street
Suite 800N
San Francisco, CA 94107

415 278 8400 tel
415-278-8445 fax
www.markmonitor.com

MarkMonitor®

In summary, we believe that ICANN has made significant progress in achieving many of the benchmarks identified in the JPA, but that U.S. government oversight is still appropriate. Should you require any additional information related to these comments, please do not hesitate to contact the undersigned.

Respectfully submitted,

MarkMonitor, Inc.

By 
Margie Milam
General Counsel

303 Second Street
Suite 800N
San Francisco, CA 94107

415 278 8400 tel
415-278-8445 fax
www.markmonitor.com

MarkMonitor

MAKING THE INTERNET SAFE FOR BUSINESS

MarkMonitor
Brandjacking Index

April 2007

The Brandjacking Index – Executive Summary

Brands open enormous new prospects yet face new and evolving risks as they move online. Criminals, profiteers and opportunists take advantage of the global reach of the Internet and the anonymity it affords in order to highjack strong brands for their own profit. These 'brandjackers' have learned the rules of online marketing and are exploiting those rules to their advantage and at the expense of true brand owners. As a result, brand owners face threats to their reputations, customer relationships, and, ultimately, their revenues.

In order to shed light on the brandjacking phenomenon, MarkMonitor® created the Brandjacking Index™, a quarterly report that measures the effect of online threats to brands. In this first Brandjacking Index, we examined 25 of the world's strongest brands as ranked by the 2006 Top 100 Interbrand study plus additional Interbrand ranked companies for business segment analysis. Our study included data collected over a four-week period from March 9, 2007 through April 6, 2007 as well as over two years of phishing data. The study quantifies a variety of online threats to brands. Study findings approached 300K results weekly; insights are based on an average of weekly samples of incidents.

These online threats are defined in detail in the Definitions section at the end of this report. The types of brand abuse and fraud that we examined are:

- Cybersquatting
- False association
- Pay-per-click
- Kiting/tasting
- Objectionable content
- Phishing statistics and trends

Summary Findings

The MarkMonitor findings suggest that brandjackers employ elaborate, multi-pronged assaults on the most recognized companies and their associated brands. All threats increased over the four-week report period. Media companies were the most attractive targets for brand abuse while cybersquatting was the greatest threat in terms of scale.

The threat from Phishing continues to increase for several reasons. From a business perspective, phishers use direct marketing techniques to pinpoint their attacks while from the technology perspective, phishers employ 'phish kits' and more sophisticated technologies to cast a wider net. The study found that phishers are now targeting more Financial Services companies than any other type of company.

- Media, both traditional and Internet-based, is an especially attractive target, drawing 31% of brand abuse. Since these brands' Web properties are some of the most heavily trafficked Internet sites, they draw the most abuse in the form of cybersquatting and false associations, resulting in lost revenue and wasted advertising costs.
- Cybersquatting is the greatest threat in terms of scale. Our sample recorded 286,000 instances of Cybersquatting. Cybersquatting causes traffic diversion and false association as well as related abuse.
- Kiters target Financial Services. Our study discovered more than 980 Kited sites focused at Financial Brands. Conservatively, kited pay-per-click sites account for over $125 million each year in revenue for Brandjackers[1].
- Offensive content represents a small volume with a big impact because of the traffic these offensive sites generate. Media was the most frequent target for offensive sites, with most offending sites misdirecting users to pornography.
- The phishing threat continues to increase with a 104% jump in annual attacks in Q1-07. Phishers actively avoid browser-based consumer protection technology evidenced by the more than 300,000 unique URLs used in phishing attacks.
- Phishers cast a wider net; in March '07, 229 companies were targeted. Of that number, 158 companies were phished for the first time.
- Phishers target more Financial Services companies. Financial Services companies made up 41% of all attacks in Q1-07. This represents a jump from 29% in Q1-06. Evidence suggests phishers prey on customer confusion during mergers and security system upgrades.

Overall, our findings suggest that Financial Services and Media companies are at greatest risk. Media companies draw the greatest Web site traffic and the Financial Services category draws the highest premiums for pay-per-click keywords, making these companies attractive targets for brand abuse.

The greatest threats are in the form of Cybersquatting, pay per click (PPC) -related Kiting, and Phishing. These threats present a variety of issues including the cost of support calls and wasted advertising dollars lost to traffic diversion. Ultimately, these threats contribute to a loss of control for brand owners in how their brands are perceived in the marketplace. This loss of control threatens customer trust and loyalty, the greatest brand assets of all.

[1] There are over 1MM kited sites re-registered daily exploiting the ICANN grace period. The grace-period granted by ICANN is five days. Therefore, the number of active kited sites is between 4-5MM every day, the vast majority of which host pay-per-click (PPC). The lowest revenue estimate for a PPC site is $25 annually; therefore, annual revenues for these kited sites is $100-125MM.

Business Implications

- Brandjackers find that the economic incentives to target large companies are substantial.
- Technology that aids large companies to market more effectively to their customers is also being employed by Brandjackers to increase the return on their efforts.
- Brand owners have to rely on themselves for enforcement because regulation by government and non-governmental organizations is insufficient to protect companies and their customers.
- Large companies have trouble keeping up with the problem of enforcing their intellectual property rights because of the scale of abuse.

MarkMonitor

Background and Methodology

The Brandjacking Index is produced quarterly and explores:

1) Numerical trends and statistics about brand abuse in order to quantify the scale and scope of the problems faced by large companies and their customers.
2) Anecdotal information about the business and technical methods used by Brandjackers
3) 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 daily for brand abuse in domain data and U.S. and international Patent and Trademark Office data.

The phishing data that MarkMonitor analyzes is based on feeds and fraud broadcasting from leading international Internet Service Providers (ISPs), email providers and other alliance partners. MarkMonitor has scanned billions of Web pages since November 2004 and processes 16 million unique phishing e-mails daily.

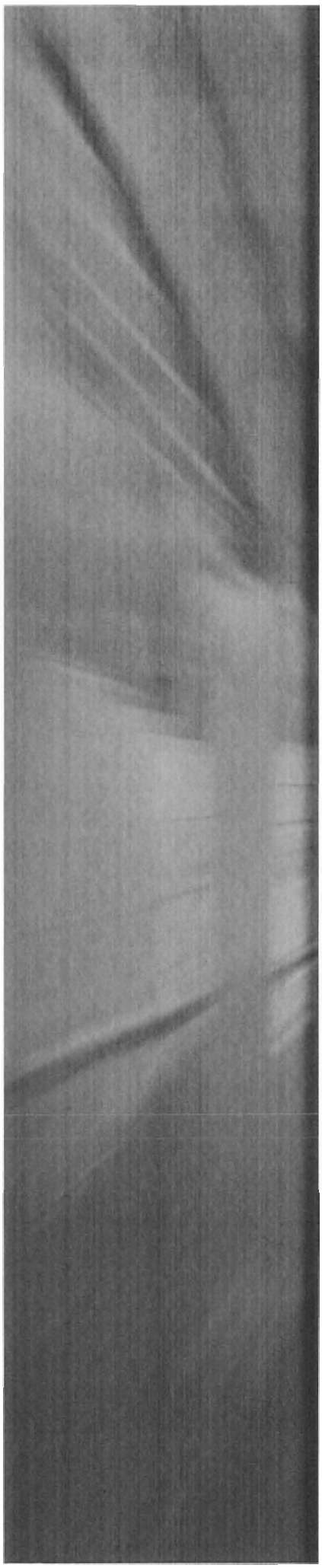
The April 2007 report is based on the following information and analysis:

- Data
  - Tracking top 25 brands from the 2006 Top 100 Interbrand study
  - Weekly sampling conducted March 9 through April 6, 2007
  - 8 vertical segments (Automotive, Apparel, Media, CPG, Consumer Electronics, Pharma, Food & Beverage, High Tech)
  - Approaching 300K abuse results weekly
  - Insights based on an average of weekly samples of incidents
  - NO customer data used in study

Summary Statistics

Threat Type	Number of Results*
Offensive Content	1,395
eCommerce Sites	21,093
False Association	75,167
Cybersquatting	286,801
Pay-Per-Click	50,743
Kiting	11,015

* Weekly Sample Compound threats – Non-mutually exclusive threat categories



Brandjacking Index™

Summer 2007

MarkMonitor®

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. Second, 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. 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 and subsequently reregistering it. 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
Domain Kiting	11,015	37,634	242%
Offensive Content	1,395	2,138	53%
Pay-Per-Click	50,743	73,774	45%
False Association	75,167	107,316	43%
Cybersquatting	286,801	311,050	8%
E-Commerce Sites	21,093	22,639	7%

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:

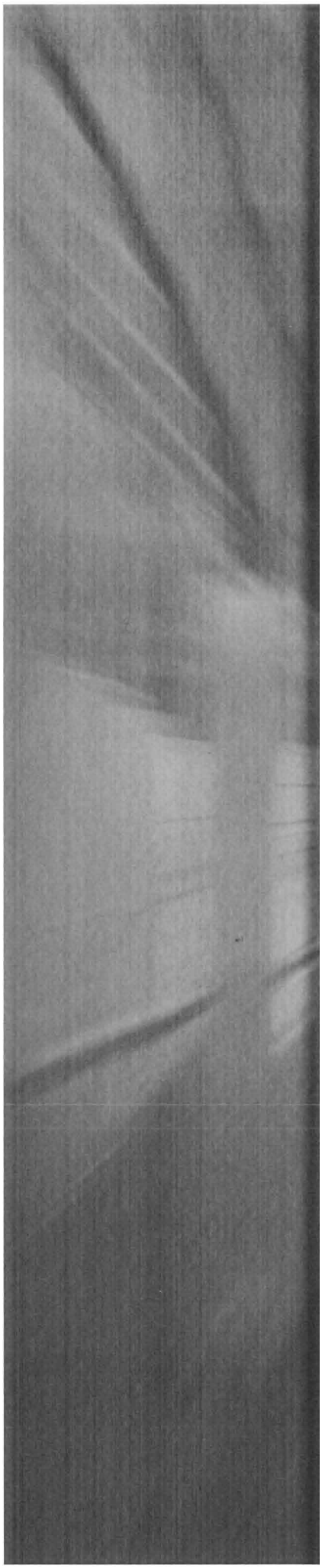
- Tracking 30 brands as ranked by Interbrand
- Weekly sampling conducted April through June 2007 for the overall brand analysis, and samples conducted during June 2007 for the pharmaceutical analysis
- Nine vertical segments (Automotive, Apparel, Media, CPG, Consumer Electronics, Pharma, Food & Beverage, 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[3] 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.

3 See Drugs.com 'Top 200 Drugs for 2006 by U.S. Sales' at http://www.drugs.com/top200.html



Brandjacking Index™

Autumn 2007

MarkMonitor®

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 earlier reports in April and July, this Autumn 2007 edition of the Brandjacking Index tracked millions of emails and billions of web pages. We found some seasonal variation: while overall cases of abuse continue to increase since our first report, we found some quarter-over-quarter declines in domain kiting and pay-per-click abuses. Perhaps the worst offenders were like many of us and busy with their own summer vacations.

This third edition of the Brandjacking Index includes a research focus on the consumer toy market and shows how recalled toy models are readily available at many online sites. Consumers who aren't aware of the recalls may endanger their children by accidentally purchasing items containing lead paint or loose magnets. In addition, we found suspicious and recalled toys for sale in bulk by B2B exchanges of toy wholesalers, which is even more of a threat as large quantities of these dangerous toys could enter the retail stream.

We conducted three different types of analysis for this Autumn 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 in detail the risks that consumers may face in the holiday shopping season, including phony gift card offers and specific brand abuse of leading toy brands and online retailers.

Summary Findings

Consumer Toy Brand Abuse

This has not been a good year for toy manufacturers and retailers. A number of high profile toy recalls combined with a slower economy doesn't bode well as the holiday shopping season begins. And shoppers will find an increasing number of online sites continuing to sell recalled toys.

We found 1,157 different auction listings for nine toy brands and searched for four specific recalled toys that contain lead paint: Dora the Explorer, Thomas the Train, Elmo, and a Barbie and Tanner play set that has loose magnets. We found 349 auction listings after these four toys had been recalled, with the vast majority of these auctions from U.S.-based sellers.

Many of these auctions show steep discounts from the retail toy price, making them even more of a target for unsuspecting consumers. For example, a $30 toy would typically sell for less than $10 on these sites, and some included huge shipping costs too. None of the auctions mention that the toys were recalled and no longer available in the traditional retail market.

Even more troubling than these auctions are wholesalers who continue to sell recalled toys on B2B exchanges. On a representative day in September, we found 1,150 listings for the nine toy brands offering a total of a million toys. From this collection, we found eight percent of the listings were for recalled toys. One site, made-in-china.com, accounts for 79% of toys in this channel.

In addition to these issues, there is plenty of evidence of retail brand abuse in the e-commerce arena from phony sites, cybersquatters, and unauthorized retailers. We examined paid search listings for 393 placements targeting the four leading online retailers (Amazon.com, WalMart, ToysRUs, and Target) – a third of these were phony yet contained some variation of one of the brand names in the site link or pages. A disturbing trend is that in all cases, the fraudsters and cybercriminals are using legitimate merchant back-end operators such as Amazon.com and eBay to mask their deeds and further confound consumers.

We found dozens of counterfeit gift card scams that trap consumers into a maze of misleading links, pay-per-click and phony affiliate sites – all of which could be used to extract a credit card number or other useful identity information.

Phishing

The news on phishing for the past quarter is mixed. We found a greater breadth of targets with this report, along with evidence of more automated phishing site deployment and management. The phishing sites created are becoming more resilient by using fast flux networks, and there is more in the way of hired botnet vendors and easily available development tools for download than in our previous reports.

The U.S. continues to be the source of a quarter of all phishing sites. The number of attacks against the retailing and service sector rose by more than ten times, from 914 in the second quarter to 10,694 in the third quarter. Financial sites continue to account for nearly half of all phishing attacks.

Still, there are some promising trends. There is a small six percent decrease in the overall number of registrars enabling phishing. The times to shut down the phishing sites vary tremendously (from minutes to weeks), but the average lifetime of a phished site is 41 hours. One of the top performers in takedowns is Network Solutions, with an encouraging average of 33 minutes per phony site. There were 65 organizations that were phished for the first time in the third quarter – which is down 26% from last quarter and 13% when measured annually, showing that the phishers are getting more focused on their targets.

Brandjacking Trends

The biggest change this quarter is that brand abuse seems to be seasonal. While the total number of observations continues to increase, the rate of increase is slowing and in some cases we saw a decrease in particular threats, particularly with pay-per-click. There is also a decrease in the number of new brands that are targeted. However, these decreases were offset by a 10% increase in cybersquatting abuses from last quarter.

Overall brand abuse distribution changed little in terms of industry segments from last quarter, with automotive and media segments accounting for more than a third of all observed abuses.

Summary Statistics

Threat Type*	Q1-07*	Q2-07*	Q3-07*	Q2-Q3 Change	YTD% Change
Domain Kiting	11,015	37,634	19,579	-48%	78%
Offensive Content	1,395	2,138	1,311	-39%	-6%
Pay-Per-Click	50,743	73,774	31,818	-57%	-37%
False Association	75,167	107,316	72,206	-33%	-4%
Cybersquatting	286,801	311,050	342,512	10%	19%
E-Commerce Sites	21,093	22,639	16,825	-26%	-20%

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

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 July through September 2007 for the overall brand analysis, and samples conducted during September 2007 for the consumer toy and e-commerce analysis
- Nine vertical segments (Automotive, Apparel, Media, CPG, Consumer Electronics, Pharma, Food & Beverage, High Tech and Financial)
- Nine popular toy brands and four of the most popular online retailers
- 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

Conclusions and Recommendations

Overall, brand abuse is increasing, especially when it comes to cybersquatting and misdirected URLs. Phishers continue to become more sophisticated, building more resilient phish sites and offering increased phishing development tools and botnet network rentals.

There is also a great deal of toy brand abuse and, despite all the publicity regarding recalled toys, unsuspecting consumers continue to be at risk of buying recalled toys online.

We recommend that all toy shoppers first check the Consumer Product Safety Commission Web site (www.cspc.gov) for specific toy recalls – there is even an RSS feed that can deliver the latest information on recalls. In the UK, visit the Trading Standards Central (http://www.tradingstandards.gov.uk) site for information while Canadian consumers can check an informational web site at Healthy Canadians (http://healthycanadians.gc.ca/pr-rp/index_e.php). Remember to navigate directly to the right retailing site and only buy from trusted sources. Finally, never give your personal information in exchange for money or goods.

We also recommend that brandholders be especially vigilant in monitoring their brands for abuse during the holiday season to protect their good names and reputations.