



Page 1

Tuesday, July 24, 2007

10:00 a.m.

Washington, D.C.

PREPARED STATEMENT – Josh Bourne

Thank you for joining this call. My name is Josh Bourne, and I am President of the Coalition Against Domain Name Abuse. I have a prepared statement, which will be followed by brief comments from a few of our members. I am very excited this morning because I am here to advocate that CADNA's goals are both pro-business and pro-consumer. I ask that you please hold questions until we have completed the presentation. For all those dialing-in, if you would mute your lines now, we can be sure to have a clear transmission.

Today, we are happy to announce the official launch of the Coalition Against Domain Name Abuse, or CADNA, and the start of our campaign to combat cybersquatting.

CADNA was formed to raise awareness about Internet fraud and to advocate policy changes that will promote a safer Internet. Our membership includes the following corporations: AIG, Dell, Eli Lilly, Hilton, HSBC, Marriott, Richemont, Verizon, Wyndham, and Yahoo!.

Over the past few years, the Internet has changed dramatically. Today, nearly 75% of Internet users access Web sites through direct navigation - the practice by which the user enters a domain name into the address bar of a web browser, rather than through a search engine. In response to this widespread practice, a cottage industry of fraud and intellectual property infringement has sprung up turning Internet browsing into a costly and dangerous game of Russian roulette. Web bandits and criminal profiteers have devised new ways to use domain names to rob consumers of their identities, brands of their hard earned trusted names, and the public of its safety.

Although the Anti-Cybersquatting Consumer Protection Act (or ACPA) was passed in 1999 to address some forms of domain name abuse, cybersquatting remains an underestimated and largely unmitigated threat. Many consumers, brand owners and policymakers have yet to understand the full scope and impact that cybersquatting has on us all.

Cybersquatting is defined as the bad-faith registration of a domain name that includes or is confusingly similar to someone else's trademark. When ACPA was passed, the most common scheme associated with cybersquatting was the use of registered domain names to extort exorbitant sums from trademark holders in exchange for the names. Since then, the definition of cybersquatting has not changed, but the methodology, scale, and fraudulent applications of the practice have.

By using familiar brands to bridge the trust gap, the cybersquatter is able to harm consumers through spam, spyware and other crimewares, phishing, and counterfeit goods such as automobile brakes, circuit breakers, and prescription medicines. False registration information (or "WHOIS" data) provides a level of anonymity that is as dangerous as it is frustrating. With no checks for legitimacy and WHOIS privacy services acting as roadblocks to accountability, the Internet provides criminals not only with lucrative opportunities for exploitation, but also with a place to hide. In any other setting outside of cyberspace, this sort of free reign is unheard of.

CADNA | The Coalition Against Domain Name Abuse
2122 P Street, NW | Suite 300
Washington, D.C. 20037
+1 202.223.5232

The magnitude of this issue is extremely large. The number of domain names has more than doubled since 2003, and the growth of cybersquatting has exceeded that pace. According to a recent independent report prepared by MarkMonitor, cybersquatting increased by 248% in the past year alone. In addition, the World Intellectual Property Organization (or WIPO) reports steadily rising UDRP complaints filed with its Geneva-based arbitration center. CADNA member Dell sees 500 new infringements of its brand name each month. The unhindered growth of cybersquatting is so substantial that it demands that we examine the legitimacy of the system, and efficacy of the current countermeasures. Unfortunately, they aren't working.

One reason that cybersquatting has been able to grow so quickly is that the sophisticated cybersquatters have been exploiting a loophole in the domain name registration process to register and subsequently drop domain names, risk free, within an accepted 5-day grace period known as the Add Grace Period or AGP. By abusing this grace period, cybersquatters "taste" and "kite" domain names in order to test their profitability. Tasting is the act of systematically dropping domain names prior to the 5-day deadline, and kiting is the perpetual act of registering, dropping, and re-registering the same names.

These practices not only enable cybersquatters to efficiently optimize their domain name holdings to capture the greatest number of visitors, but they also stymie the efforts of brand security and law enforcement agencies. The 5-day turnaround time on domain names (thanks to the AGP) coupled with routinely falsified registration information essentially outfit scam artists with an easy-bake cybercrime kit - electronic ski mask and getaway car included - just add victim.

Jay Westerdahl of Name Intelligence recently asserted that 2 million domains are tasted or kited daily. It's no surprise tasting targets brand-derived domains that are more likely to get traffic.

One brand owner told us that when they filtered out the domains that were less than 5 days old from their infringement monitoring report, the list was reduced by 80%.

Cybersquatting is present in nearly every successful phishing attack since it is easier to lure victims by tapping into existing brand-consumer trust. The Internet Crime Complaint Center, a partnership of the National White Collar Crime Center and the FBI, found that consumers in the United States reported personal losses of greater than \$198 million to phishing in 2006. This figure is undoubtedly an understatement of the actual losses caused by phishing, as many losses due to phishing attacks often go unreported out of personal chagrin.

Domain tasting and kiting are also used to facilitate phishing. A phishing attack often lasts less than a day. With tasting, a domain can be temporarily registered, used in an attack, and then put back in the available names pool, while the perpetrator disappears. For the law enforcement agencies and brand owners trying to protect the public, phishing prevention is akin finding a needle in haystack. With more than 1,000 new phishing sites erected daily (according to the Anti-Phishing Working Group) combined with the "tasting" practice that adds 2 million new domains each day, that haystack has grown to proportions so large that finding the needle is nearly impossible.

CADNA member HSBC, a global financial services company, notes that phishing is just one way in which domain name abuse can have an impact on its customers. Martin Sutton, HSBC's manager of Fraud Risk & Intelligence, will be addressing this in further detail.

Brand name recognition aids phishers and other cybercriminals who depend on traffic – the more visitors they get, the bigger the target audience and the bigger the payoff – it’s a volume game.

One example of this can be seen in the weeks surrounding Apple’s launch of iPhone, when it was reported that Apple’s new trademark was heavily cybersquatted.

Currently, there are at least 21,822 registered domain names that incorporate the word iPhone (such as 360iphone.com) and 476 registered domain names that are a single character away from “iPhone” (such as ipho0ne.com with a “zero” after the “o”). CitizenHawk, a digital brand management company that focuses on stopping the use of typographical errors in domain name infringement, identified those potential infringements and pointed out that many of the names are being kited, a permitted tactic used to avoid payment while getting the full benefit of domain ownership.

You might wonder, how much traffic does an infringing domain name attract – or – how destructive could any given name be?

FairWinds Partners, the Internet Strategy Consulting firm where I am a managing partner, routinely checks for domain names that infringe on the intellectual property rights of our clients. Just last week, we discovered a domain that includes a typographical error so common that it receives over 600,000 visitors a year. Unfortunately, this was not a unique discovery or even the most alarming example. Typosquatting, the use of domain names containing common typographical errors of popular sites, is the perfect tactic for cybercriminals to siphon errant traffic, deposit spyware, or dupe consumers into surrendering sensitive information. For example, the top 5 misspellings of myspace.com each receive over 3 million visitors per year. If only 1% of those 15 million fall victim to one of these Internet crimes, 150,000 people are directly harmed.

Even more disturbing, typosquatting preys on Internet users who are most prone to making typographical errors: children and seniors. Children are targeted using names that closely resemble familiar fictional characters and toys. Children who misspell one of these names can be exposed to pornographic material, spyware, or even sexual predators.

Seniors on fixed incomes are also targeted by typosquatters. Hunting for bargains on prescription drugs, seniors commonly visit sites whose domain names convey association with or sponsorship by legitimate pharmaceutical or pharmacological corporations. Peddling inert or even toxic drugs, these sites and the counterfeiters who run them endanger public safety to turn a profit.

These examples of cybersquatting-enabled abuses highlight the growing need for new action.

Given the global community’s increasing reliance on the Internet as a platform for convenient commerce and the open exchange of information, policymakers must act to shore-up accountability and transparency on the Internet. If we fail to modernize our policies, if cybersquatting continues to grow unchecked, then we risk squandering the Internet’s potential to our own detriment and the detriment of future generations. The members of CADNA believe that we must act, and that the time to act is now.

To effectively combat cybersquatting and reduce spyware deposit, phishing, and other Internet based fraud, CADNA will work at the national and international levels to make these practices both difficult to establish and unprofitable to maintain.

In the coming months, we will begin to pursue **federal legislation** to increase the statutory damages in the Anti-Cybersquatting Consumer Protection Act in order to deter the cybersquatting that breeds Internet fraud.

On the **international level**, we hope to work with WIPO, to introduce an international anti-cybersquatting treaty - setting a global standard that will prevent U.S.-based cybersquatters from moving their operations off-shore and will better protect the international community in general.

Finally, CADNA will urge **ICANN** to take decisive action on abuses by domain name registrars and registrants, and close the AGP loophole that affords criminals the opportunity to “kite” and “taste” domain names.

CADNA aims to be the catalyst for making the Internet a less confusing and safer place for consumers and businesses alike. We hope that lawmakers will see that by reducing cybersquatting through increased deterrence, and taking tools that serve no legitimate purpose away from cybercriminals, they will be taking giant steps toward eliminating the spam, phishing, spyware and malware, and counterfeit-peddling that pollute the Internet, weaken its viability as a platform for commerce, and irreparably harm consumers.

Thank you. That is the conclusion of my statement.

We thought it would be helpful for you to hear the voices of some of our members and why they think this is a worthwhile endeavor. First you'll hear from Elisabeth Escobar, Vice President & Senior Counsel of Intellectual Property at Marriott International, then Martin Sutton Manager of Fraud Risk & Intelligence at HSBC, and finally Susan Crane, Group Vice President of Intellectual Property at Wyndham Worldwide.

STATEMENTS FROM DESIGNATED MEMBER SPEAKERS

1. MARRIOTT - Elisabeth Escobar

The five-day grace period for new domain registrations, inaccurate and incomplete WHOIS data, and the lax regulation of registrars have all contributed to an explosion of Web sites filled with nothing but “pay per click” links to other sites. Many of these click-through sites use domain names that contain well-known brands to sidetrack consumers and divert them away from their intended destinations. Domain tasting and kiting has resulted in the proliferation of so many sites that it is impossible to attack the problem effectively through traditional methods. Instead, we need to address the abuses of the system that make cybersquatting an attractive business model.

2. HSBC - Martin Sutton

The issue of Cybersquatting is a serious one, one that threatens the viability of businesses, the rights of consumers and the trust between brands and the people they serve.

Josh already mentioned that phishing is an example of when domain name abuse is used to harm consumers. In addition to phishing, there are many more ways that cybersquatting can be employed to inflict damage—Section 419 scams, also known as “Nigerian” or “Advance-Fee” scams, bogus investment scams and taster domain names, to name a few, are all real problems.

HSBC, like many other brand owners, constantly detects and responds to the online threats that target our consumers around the globe but there is no complete solution to prevent or combat these problems. The options currently available to brand owners are often too slow and ineffective to stop these “Web bandits”.

CADNA will work for more effective ways to prevent fraud and combat criminal activity.

3. WYNDHAM – Sue Crane

Cyberquatters are siphoning away Internet user traffic meant for brand Web sites and deceiving online consumers. Customers can be duped into believing that they are getting the hospitality and service that they have come to expect from the Wyndham family of hotel brands, only to be left with rooms at unaffiliated properties, with no reservations at all or with their personal information compromised. It's a horrible experience for the customer and it is a company's responsibility to help protect against such an experience—but the burden of navigating through and policing the ever-changing landscape of Internet fraud is too much for a single brand or corporation to bear. CADNA will provide an opportunity for brand owners to work together to bolster fraud protection for both customers and businesses.

CONCLUSION – Josh Bourne

At this point if there are any questions, I welcome them. But because of the call-in format, please state your name and your organization prior to your question. We'll have a few minutes for questions, but feel free to contact Andrew Friedman, CADNA's Communications Director, after the call concludes to arrange a time for any additional questions. Also, please expect to see a fact sheet, which will be sent by email, that includes a few additional member points of view.

Contact: Andrew Friedman
Communications Director
(202) 341-3722
andrew@cadna.org