wiley

NEWSLETTER

Preparing for New Cybersecurity Risks From Cybersquatting

February 2017

Cybersquatting is not just a nuisance or trademark problem; as cyberthreats rapidly evolve, it presents serious risks to companies. In the not-too-distant past, a company's primary concern from misuse of Internet domain names was that someone would register a domain name that appeared similar to the company's trademarks, in order to display a website with annoying pay-per-click advertisements or a "for sale" landing page. However, as consumers have come to expect that companies will use intuitive domain names to make available everything from banking services, to entertainment software, to all manner of consumer goods, Internet scam artists have sought to take advantage of consumer expectations with increasingly sophisticated misuses of domain names.

Today, the most problematic domain name misuses include spam, phishing, distribution of malware and bloatware, and other types of scams and cyberattacks. Given the potentially serious consumer and brand harm from such activities, companies should consider modernizing their anti-cybersquatting practices to adapt to these threats and should consider how to address anti-cybersquatting in overall cybersecurity planning.

The Nature of Cybersquatting Is Evolving

Bad actors use domain names to further illicit schemes in elaborate and evolving ways. According to recent studies by information security firms, in certain new top-level domain extensions, over 95% of the issued domain names are being used for spam, phishing, distribution of malware and bloatware, and other types of scams.[1] As a result of these factors, spam alone now accounts for up to 70% of the domains in certain new domain registries according to one study.[2]

Authors

David E. Weslow
Partner
202.719.7525
dweslow@wiley.law

Practice Areas

Cybersquatting & Internet IP
Privacy, Cyber & Data Governance

Cybersquatted domain names also have been used in a number of recent high-profile cybersecurity breaches. For example, in early 2015, hackers gained access to the names, Social Security numbers, and birth dates of over 78 million Anthem customers. To facilitate this attack, the hackers reportedly registered the domain name we11point.com, which looked like Anthem's former name, and used an e-mail address from that domain to entice an employee to click a link in an e-mail designed to look like an internal message.[3]

A breach at the U.S. government's Office of Personnel Management exposed the Social Security numbers of more than 20 million applicants for federal positions, along with usernames and passwords used to complete background information forms, the findings of some background interviews, and fingerprints.[4] That breach apparently was facilitated through the use of the domain names opm-learning.org and opmsecurity.org, which replicated legitimate government sites like learningconnection.opm.gov.[5]

Distribution of malware through domain name misuse is a particular focus of certain cybersquatters and criminal syndicates. Last year, cybersquatters registered the expired domain names of Internet advertising companies and reportedly used them to serve malicious software through third-party advertisements displayed on the websites for *The New York Times*, *Newsweek*, the BBC, and AOL, among others.[6] Security experts note that the low price of registering domain names (including the availability of free names from certain registries) makes it easy for cyber criminals to register and exploit domain names.[7]

Once systems are infiltrated by malware, the threat to the domain name system is far from over. A recent report by network equipment provider Cisco estimates that 91.3% of malware uses the domain name system to gain command and control, exfiltrate data, or redirect traffic.[8]

Many Anti-Cybersquatting Practices and Protocols Are Dated

Just a few years ago, the conventional wisdom was that companies could effectively protect their trademarks online simply by defensively registering their marks across the most popular top-level domain extensions and engaging in aggressive monitoring and letter campaigns to target copycat domains. With up to 1,400 new domain registries launched or launching, and increased use of country-code domains, third-level domains, and social media platforms, those strategies are no longer practical. Registering a single mark defensively across all new domain registries would run into the tens of thousands of dollars alone, not accounting for typos, which would push the costs into six figures or beyond.

The benefits of overzealous demand letter campaigns likewise no longer can be justified. Pursuing marginally problematic sites with a low likelihood of consumer or brand harm merely increases costs and is not necessary to protect the brand. For example, it may not be necessary to pursue a domain with an extension unrelated to the company's products/services and that is merely being used to display generic pay-per-click content, given the low risk of consumer confusion or brand harm.

Companies Should Modernize Their Anti-Cybersquatting Programs

Rather than rely on outdated tactics that can be ineffective and, in some instances, counterproductive, companies should adjust their online enforcement strategies for the fast-changing online ecosphere.

As an initial step, companies should register their trademarks with the Trademark Clearinghouse (TMCH). The owner of a mark registered with the TMCH has the opportunity to register the mark during the sunrise period for new domain registries—where appropriate. The TMCH also provides a notification service to would-be registrants for a limited time following the launch of new domain registries, and to trademark owners notifying them when a domain has been registered corresponding to the trademark. Trademark owners should be prepared to file complaints under the new Uniform Rapid Suspension (URS) administrative procedure, where appropriate, and a TMCH validated mark can satisfy the trademark owner's burden of establishing the validity of the trademark under the URS.

Companies also should develop a strategy for very limited defensive registrations, focusing on the top-level domains that are most likely to cause consumer confusion or harm to their brand. To complement limited defensive registration efforts, companies should consider the various brand protection and domain name registration monitoring options that can provide early warnings of potentially problematic domain name registrations. These monitoring services can be particularly helpful in early identification of potential cybersecurity issues when paired with IT staff monitoring of company network connections and exfiltrations to identified third-party domain names.

Finally, and most importantly, companies should develop in advance a protocol for prioritization of the inevitable Internet-related incidents that will arise. An effective protocol should include a procedure for identifying which domain name registrations merit action and for dealing with those names in the appropriate forum. Based on the severity of the potential for harm, escalation options may include engagement with the registrar, registry, or other service provider; pursuit of a domain name dispute resolution proceeding or judicial action; and consolidating actions for efficiency. We have had success on behalf of a number of clients in bringing consolidated court cases under the U.S. Anticybersquatting Consumer Protection Act (ACPA) against dozens, or even hundreds, of domain names in a single action.

Developing a protocol to prioritize domain name and Internet issues will provide a clear road map of options in the event of a cybersecurity incident involving a domain name, and will facilitate the avoidance of ad hoc decisions and unnecessary or overly aggressive enforcement actions. Although cybersecurity incidents and associated misuse of domain names are likely to continue, such incidents can be more readily and efficiently addressed by pre-event modernization of online trademark enforcement protocols, and integration of those protocols with existing or evolving cybersecurity policies and practices including incident response plans.

---

[1] *See* Blue Coat Research, *Do Not Enter: Blue Coat Research Maps the Web's Shadiest Neighborhoods* (Sept. 2015), *available at* https://www.bluecoat.com/documents/download/895c5d97-b024-409f-b678-d8faa38646ab.

[2] *See* Spamhaus, *The World's Worst TLDs*, https://www.spamhaus.org/statistics/tlds/.

[3] *See* Kara Scannell and Gina Chon, *Cyber Security: Attack of the Health Hackers*, Financial Times (Dec. 21, 2015), *available at* https://next.ft.com/content/f3cbda3e-a027-11e5-8613-08e211ea5317.

[4] *See* Office of Personnel Management, *Cybersecurity Incidents: What Happened*, https://www.opm.gov/cybersecurity/cybersecurity-incidents/.

[5] *See* ThreatConnect, *OPM Breach Analysis* (June 5, 2015), https://www.threatconnect.com/opm-breach-analysis/.

[6] *See* Reuters, *Cyber Criminals Snap Up Expired Domains to Serve Malicious Ads* (Mar. 16, 2016), *available at* http://www.reuters.com/article/us-website-malware-idUSKCN0WI2DZ.

[7] *See* Paul Vixie, *Domain Name Abuse: How Cheap New Domain Names Fuel the eCrime Economy*, RSAConference2015, *available at* https://www.rsaconference.com/writable/presentations/file_upload/hta-r02-domain-name-abuse-how-cheap-new-domain-names-fuel-the-ecrime-economy_final.pdf.

[8] *See* John Stuppi and Dan Hubbard, *Overcoming the DNS Blind Spot*, Cisco Blog (Jan. 22, 2016), http://blogs.cisco.com/security/overcoming-the-dns-blind-spot.