FARSIGHT SECURITY

DOMAINTOOLS

Luxury Brands, Cheap Domains:

Why Retailers Are Losing The Fight Against Online Counterfeiting

Research Report

INTRODUCTION

What do premier watches, designer handbags and prescription pharmaceuticals all have in common? These are just a few items being sold on the Internet, as counterfeits of actual brand names, for enormous profits. In fact, according to the International Trademark Association, $460 billion worth of counterfeit goods were bought and sold last year, mostly online.

Retailers, specifically luxury brands, appear to be popular targets of cybercriminals. Online fraud represents millions of dollars in lost revenue and tarnishes their premium brand status. Gucci America, Inc., recently won judgements worth more than $9 million against a group of nearly 100 web sites selling knock-off merchandise. Sites that used "Gucci" in their domain names were ordered to pay additional damages totaling $110,000.

To lure unsuspecting consumers to fake websites to purchase counterfeit goods, cybercriminals abuse the Domain Name System (DNS) – every day, every hour, every minute. In this report, "Luxury Brands, Cheap Domains: Why Retailers Are Losing The Fight Against Online Counterfeiting," cybersecurity firms Farsight Security and DomainTools, the leaders in DNS intelligence, took a close look at four international luxury brand domains and learned that the potential abuse of their brand, by counterfeiting and other malicious activities, is significant.

DNS: THE MAP OF THE INTERNET

The Domain Name System (DNS) is a critical part of the underlying infrastructure of the Internet. It enables Internet users to conduct billions of online transactions every day, connecting fully qualified domain names (e.g. www.ralphlauren.com) to the numeric IP addresses that site lives on. Each time you visit your favorite website, you use the DNS.

A domain name can include a brand trademark such as "Ford" in http://shop.ford.com/showroom. A typical Fortune 500 corporation may have a thousand or more domain names. Yet not every corporate domain includes an organization's trademark. For example, an organization's marketing departments may create domain names to support an event or other activity.

Trademarks are established at substantial cost, but the associated consumer confidence can be undercut or destroyed in no time if poor quality knockoff goods become conflated with the real thing. Domain names are considered trusted online brand ambassadors by both corporations and their customers. As a result, they are increasingly being targeted by cybercriminal fraudsters.

When criminals misuse the DNS to create fraudulent online infrastructure, they leave a trail of evidence—sometimes obvious, sometimes subtle—of their doings. In particular, the DNS domain-to-IP mappings, and the registration records for fraudulent domains, exist openly on the Internet.

WHOIS RECORDS

Domain registration information is recorded and made available via the Whois protocol. While the specific format of the Whois record will vary from one domain registry to another, in general the records show the following information about a domain:

- Creation and expiration dates
- Registrant contact information such as email addresses, physical addresses, and phone numbers
- Registrar (the organization that processed the domain registration)
- Name servers for the domain (which enable DNS to map the domain to an IP address)

The Whois records for some top-level domains (TLDs) show more fields than above, while some show fewer —there is not a unified global standard for the information provided in the Whois record.

Whois privacy

For various reasons, registrants of domains often wish to remain anonymous. In some cases, the motive may be to protect an individual or family from unwanted attention; in other cases, it may be in an effort to inhibit attribution of illicit activity. Most domain registrars offer Whois privacy or proxy services, typically for an additional fee. When such a service is used, the Whois record for a domain shows the contact information of the privacy or proxy service, not the name and address of the individual who actually registered the domain.

"Do-It-Yourself" Anonymity

Registrants are required to use accurate information when they register a domain. However, it is worth noting that few, if any, domain registrars consider policing registrant information accuracy to be a top priority. In general, the most routinely enforced requirements are a working email address and successful payment of registration fees. As a result, it is not uncommon to see Whois records with obviously fictional character names for the registrant, nonsensical phone numbers (e.g. 111111111111), invalid physical addresses, etc. Registrants can and often do avoid paying Whois privacy fees by simply using a stolen credit card and bogus information when registering a domain name.

DNS ABUSE: HOW BAD GUYS ABUSE DNS TO COMMIT FRAUD

DNS plays a pivotal role in most cybercriminal's infrastructures. Due to the easy availability of free (or cheap) domains, the criminals will often register, use and abandon new domains within a window of just minutes. Cybercriminals will often register a domain name that is close to a targeted brand, but slightly changed, confident that a brand owner who is only watching for a perfect match will overlook their intentionally misspelled or otherwise slightly modified variation, while consumers will still see that site, courtesy of search engines and affiliate links.

How many domains are created daily?

Passive DNS sees 2½ new second-level domains per second and 50-60 new Fully Qualified New Domains (FQND) per second.

Among the types of DNS abuse:

- **Phishing:** Lookalike malicious domains used to create websites or emails to lure unsuspecting users for fraud and other cybercrimes
- **Brand Infringement:** Unauthorized use of a brand or trademark as part of a domain name
- **Brand Dilution:** Brands, if not protected and reserved for use by the brand-holder, are at risk of becoming generic references to a class of goods rather than a specific reference to a particular company's product. This has happened to some photocopier brands, for example, or to some over-the-counter drug brands.
- **Brand Diminishment**: Brands, used without permission to mislabel inferior knock-off products, diminish the prestige and perception of quality that the brand owner has worked hard to establish for their authentic goods.
- **Brandjacking:** A common example is using brand names in a web page's keywords, even if the keywords have nothing to do with what is actually on that page
- **Brand Typosquatting:** Registration of a "typo domain" that is lexically similar to an entity's brand with the intention of launching an attack listed above

NEW RESEARCH

In order to get a sense of the scope and nature of illicit activity currently taking place online, we examined domain names related to four international luxury brands. There were several key questions we were interested in:

- Where abuse is apparent, what is the nature of it?
- What's the magnitude of brand infringement and related problems?
- Where is the abuse concentrated (either geographically or in terms of TLDs)?
- What characteristics, if any, do the abusive domains share?
- Is there a typical profile for the operator(s) of questionable domains?
- Is there incidental/innocent infringement of well-known brand names, as well as intentional infringement?

Variations on Brand Names

While every major brand owns its "flagship" domains (e.g. cartier.com, prada.com, burberry.com, gucci.com), there are many other top-level domains and many brand variations that non-brand owners can and do use to register domains. These domains fall into a few basic categories:

- TLD variation (e.g. prada.**tk**, gucci.**science**)
- Affixes (e.g. **cheap**cartier.com, prada-**handbags**.cn)
- Combinations of affix and TLD
- Typos (not part of this study)

These were not the only types of matches. The first-pass data also included innocent domains, which needed to be screened out. Such domains may happen to coincidentally contain a brand name but not in an intentional way, e.g. gapradar.com. We used samplings or subsets of the discovered domain lists to estimate the distributions of incidental versus intentional inclusions of the brands.

METHODOLOGY

We looked in-depth at four international luxury brands, Burberry, Cartier, Gucci and Prada. The analysis began by searching Farsight DNSDB Export, the world's largest historical database of passive DNS observations, for the month of April 2017. We looked for records containing the brands as part of domain names. For each term (e.g. "burberry," "prada," etc), we found many hits in DNSDB—literally thousands of matches.

Our initial returns were then narrowed down using DNSDB through a multi-step process:

- Duplicate occurrences of domain names were removed, and unneeded record fields were deleted
- Farsight then reduced the FQDN's to effective-2nd-level domains, again eliminating any duplicates
- We then double checked that all the remaining names still contained the magic string of interest (e.g., burberry.sample.com ==> sample.com would get excluded at this point)
- Finally, we mapped each name to its associated nameserver in an effort to identify name servers that may be known to be used by legitimate brand owners, or any name servers that may be disproportionately popular with brand infringing domians. As part of that work, we looked up the nameservers for each brand, and produced a sorted list of nameservers in descending order by frequency.

We then refined that data using the DomainTools database of Whois records and domain profile information. This step allowed us to identify additional domains in the set that were owned by the legitimate brand owner, and, to see patterns of ownership among the illicit or questionable domains. This process also allowed us to do sampling of the data to estimate the rates of incidental or irrelevant occurrences of the brand name in the domain names. Included in the DomainTools database are risk scores calculated by the DomainTools Reputation Engine. These scores pertain specifically to cybersecurity risks such as phishing, malware, and spam; they do not consider other types of fraud such as counterfeiting.

FINDINGS

Each of the brands had its name included in many thousands of effective second-level domain names. Some of the names had more "incidental" occurrences than others—for example, "prada" is a string of letters that sometimes can occur as part of entirely unrelated words. But, even controlling for domains owned by the brand-holder and domains that are incidental "by-catch," there are thousands of domains containing each brand that do not have any connection to that company.

Some specific patterns held true across the brands we examined:

- **Brand-holders don't use Whois privacy, but imitators do**. None of the brands we specifically examined for this report uses Whois privacy for their domain registrations. This holds true more generally for commercial companies and high-profile organizations. Most either use their own corporate information, or that of a third-party brand protection and promotion agency.
- **Brand keywords see wide distributions across TLDs, but .com is dominate**. Whether it's because of name recognition, old habits, or because .com is "too big too block" (unlike some other TLDs), the .com TLD generally represents half or more of the brand-infringing domain names.
- **Relatively low rates of malware, phishing, and spam**: According to the DomainTools risk scores for the brands we examined, fewer than 10% of potentially infringing domains were classified as high risk. That said, websites using brand-infringing domains should always be considered a risk and be avoided since there's no way to tell what domains are and aren't going to be infected. Likewise, while it is true that many spamvertised domains may not be spamvertised, even a single spamvertised domain, if broadly spamvertised, can be as bad or worse than a hundred domains each lightly spamvertised.
- **Strong hints of counterfeiting**: We found hundreds of domains with terms such as "cheap" and "fake," as well as domains purporting to be retail outlets, but whose registration records showed no connection to the brand or any related operation. While these "tells" may not prove counterfeiting by themselves, the identified domains are certainly something that should concern the relevant brand-owners, and something that deserves closer attention from them

FOUR LUXURY BRANDS EXAMINED

CARTIER

After reviewing any occurrences of "cartier" in a month-long extract of data from the Farsight passive DNS database, we eliminated domains that were associated with the name servers used by Cartier itself. This yielded 3,139 remaining domains. We then took other measures to exclude domains owned or reclaimed by Cartier, as well as domains that appeared to be innocent or incidental use of the name.

Specifically, we excluded the following:

- Richemont and Cartier Group AG, which are legitimately part of or associated with Cartier.
- Domains that have been in existence for more than five years. We excluded the older domains because among them were a lot of incidental or coincidental occurrences of the name, and no large-scale evidence of abuse.
- If we exclude all remaining domains that contain the name Cartier in the registrant org, we were left with **1,811 domains**.

The below statistics are some highlights from the domain registrations of the 1,811 non-Cartier-owned domains:

- For around 20 domains, the listed registrant was not an individual or company, but a court case.
- We counted some 275 domains using actual privacy services such as WhoisGuard, Perfect Privacy, etc. 12 of the 275 were registered to "Private Person," which is the generic privacy marker for the .ru (Russia) TLD. 17 of the domains were registered to "Ano Nymous."

Risk scores (malware, phishing, spam)
22 of the domains have been blacklisted, while 48 overall were in the high-risk category (risk scores over 70). Looking at domains 5 years old or less, the numbers change to 37 high-risk domains, and for domains a year or less old, just 15. Many of the high-scoring domains used their names as part of what may well have been phishing lures: fakecartier[.]top, copycartierwatches[.]cn, and replicacartierwatches[.]cn are typical examples.

Age
In Internet terms, 10 years is a long time. While the bulk of our attention was paid to younger (<5 year old) domains, we did take a quick look at Cartier-themed domains over 10 years old and found that, in general, there was not strong evidence of abuse. Among the 408 domains in this category, we saw:

- Lots of coincidental occurrences of the brand name as a substring, also things like "cartierwatches.com" which is not owned by the company but which represents a dealer of used Cartier watches, with no obvious indication of fraud.
- In a case of potentially misdirection but not necessarily outright fraud, cartierpearls[.]com redirects to asianpearls[.]net.
- Among the 408 older domains, we found 11 domains that seem potentially abusive (cartiertime[.]com, cartierplatinum[.]com, and others similarly constructed) but which don't now resolve to IP addresses and which may never have. Keep in mind, however, that even if those domains don't resolve to IPs, they may have MX records (allowing receipt of email), and hence should still be considered "operational" or potentially live.

BURBERRY

After our broad-brush name-server-based refinement of the list of Burberry-themed domains, we were left with 2,216 domains whose ownership wasn't clear. We cut this almost exactly in half, to 1,109 domains, by making the following exclusions:

- Burberry Limited or a burberry.com email address as the registrant information
- Email addresses connected to a major brand protection company
- Whois records related to litigation on behalf of Burberry
- Registrations where the surname Burberry indicated innocent usage of the name

Age
With the above constraints applied, we observed the following:

- 886 of the domains are domains that have been in existence for more than five years. Of these, 72 are in the high-risk category.
- 537 of the domains are one year or younger, with 34 of these flagged as high-risk.
- 148 of the domains had been registered in calendar 2017 up to the research date (2Q2017), with 15 flagged as high-risk.

PRADA

The name-server-based trimming left us with a pool of 4,366 domains. We then made similar exclusions as with the other brands. Specifically, we excluded any domains where the name server or the registrant emails contained the domain barbero.co.uk, which is an online management/hosting company that appears to be used by Prada (as well as many other well-known brands). However, this trimmed fewer than 5% of the domains from the list, and no other large-scale ownership patterns gave us simple heuristics to trim the list.

Estimating Infringement vs. Incidental Use

Because we were manually reviewing records, we decided to use a sample of 500 domains to more closely examine the proportion of apparent infringement versus innocent or accidental incorporation of the string "prada" in the domain name. Our findings were that approximately **50% of these domains are actively leveraging the brand**, and 50% seem to accidentally include that string. The string "prada" appears in various person names, and often is seen in conjunction with the word "radar," any time the prior word ends in p (e.g. "ga**pradar**.com").

Risk scores
As with the other brands, the incidence of domains flagged as high risk for malware, phishing, and spam is relatively low. For the domains registered within the last 5 years we saw 110 high-risk domains, and of the domains one year or less in age, there are 78 flagged as high-risk.

Zoom in on .com

- Of the domains not owned by Prada, 2258 are in .com.
- Of the 557 Prada-themed .coms of the last year, **6 of the top 10 registrants are privacy services**. 400 of the 557 domains belong to singletons—registrants with only one Prada-themed domain to their name.

All Prada-themed domains of the last year

- Of 972 total Prada-themed domains not owned by Prada, and registered within the last year, 694 are owned by singletons
- The largest individual registrant is "Private Person" with 19 domains. (Since this is the .ru privacy service, there's no way to know how many actual persons are represented in that pool.) Nexperian Holding, a Chinese company, is second with 18 domains.

GUCCI

After our initial screening, we had 5188 Gucci-themed domains. As we did with the other brands, we identified several markers in the DomainTools data that helped us trim out domains that appeared to be owned by Gucci or to have legitimate business connections (for example, Fiat offered a Gucci edition of the model 500). This round of trimming involved removing records registered with @gucci.it or @gucci-anticounterfeiting.com email addresses, name servers belonging to Mark Monitor or Com Laude, as well as those with Com Laude as the domain registrar, or Gucco Gucci s.p.a. as the registering organization. These layers of trimming brought the number to slightly under 3,100 domains.

Within this group of domains, some interesting patterns emerged:

- The top four registrant organizations, and seven of the top 10 in terms of numbers of domains, were privacy providers
- The seven privacy providers comprising the top 10 list accounted for only 483 of the domains, meaning that ownership is not especially concentrated in this set.
- Two of the other top 10 registrants related to legal settlements.

Other tidbits from this set of domains:

- 86 were identified by DTRE as high risk for malware/spam/phishing
- 1,615 of the domains, or just over half, were in .com
- 84 of the domain names begin with "cheap"

As with the Prada-themed domains, we did a random sampling of 500 domains from the set. 127 of these domains, based on domain name and Whois data, appeared to be incidental rather than infringing. This is a markedly lower percentage than we observed with Prada; this may be attributable in part to the fact that "gucci" does not tend to appear as part of a larger generic word.

DETECTION AND PREVENTION: HOW RETAILERS CAN MINIMIZE RISK

A common reaction to the amount of abuse of well-known brand names is that the brand owners should simply register the domains themselves to keep them out of the hands of miscreants. While this is a logical suggestion, a bit of analysis of the problem space illustrates the impracticality of this recommendation.

There are several factors at play:

- Beyond the bare brand string itself (e.g. "gucci"), there are a huge number of possible word combinations that could include the brand. For luxury accessories, for example, words such as "shoes," "footwear," "bags," "handbags," and countless others, can be included with the brand name, and each of these may occur in multiple languages. There are other categories of relevant words, as well, such as those related to the process of commerce (e.g. "store," "online," "outlet," "sales"). For any given brand there may be dozens of plausible combinations, and this is to say nothing of sub-brands.
- Numbers are often added before or after the bare brand string, as well as the multi-word variants described above (e.g. "123pradashoes.com"), further raising the numbers of possible names.
- The total number of plausible variations must now be multiplied by the number of TLDs, since any given string could occur in multiple TLDs (e.g. gucci.com, gucci.us, gucci.co.uk, etc). There are currently over 1,500 top-level domains.

Thus, it is not farfetched to reason that a given brand could easily have 100,000 or more possible reasonable domain names for each of its brands—and many brands have multiple properties. Add that there is no centralized method for bulk domain registration across TLDs, and it becomes easy to appreciate the non-trivial scope of the problem.

A WORD ABOUT TAKEDOWNS: A SOLUTION OF LAST RESORT

When a retailer has identified a potential website that has co-opted its brand to sell counterfeit goods, the initial reaction is often to strive to have the website taken down/go offline. Takedowns normally are a solution of last resort. Potential collateral damage increases if the takedown is done to a shared domain name, of if a shared IP address is blocked, or if you attempt to block name servers used by diverse domains. Collateral damage to third parties even has the potential to dwarf the direct harm that's being targeted for remediation.

THE VALUE OF FARSIGHT PASSIVE DNS + DOMAINTOOLS

Using Farsight Passive DNS and DomainTools solutions, we were able to show that brand name infringement is an enormous and significant challenge to today's retailers. Yet, the report also showed that identifying potential malicious domains is more than a game of whack-a-mole. Not every domain that contains a brand name is malicious. Farsight DNSDB and DomainTools solutions enable retailers to not only identify potential brand infringement site using DNSDB's historical passive DNS, collected since 2010, but also confirm possible intent using Whois and domain profile data.

To understand the entire brand infringement threat to your company, you need a comprehensive approach that goes beyond just monitoring, Earlier this year, Farsight Security and DomainTools announced a new partnership that integrates their flagship solution into the DomainTools Iris investigation platform to enable users to more quickly identify and mitigate potential threats.

REFERENCE:
For more information on this partnership and the value it can provide your organization, please visit:

https://www.farsightsecurity.com/solutions/dnsdb/

https://www.domaintools.com/company/press/domaintools-and-farsight-security-join-forces-to-power-threat-hunting

ABOUT FARSIGHT SECURITY

Farsight Security is the world's largest provider of historic and real-time passive DNS data. We enable security teams to qualify, enrich and correlate all sources of threat data and ultimately save time when it is most critical - during an attack or investigation. Our solutions empower enterprise, government and security industry personnel and platforms with unmatched global visibility, context and response. Farsight Security is headquartered in San Mateo, California, USA. Learn more about empowering your threat platform and security team with Farsight Security passive DNS solutions at www.farsightsecurity.com or follow us on Twitter: @farsightsecinc.

ABOUT DOMAINTOOLS

DomainTools helps security analysts turn threat data into threat intelligence. We take indicators from your network, including domains and IPs, and connect them with nearly every active domain on the Internet. Those connections inform risk assessments, help profile attackers, guide online fraud investigations, and map cyber activity to attacker infrastructure. Fortune 1000 companies, global government agencies, and leading security solution vendors use the DomainTools platform as a critical ingredient in their threat investigation and mitigation work. Learn more about how to connect the dots on malicious activity at www.domaintools.com or follow us on Twitter: @domaintools.