Criminals Manipulate Trusted Brand Names

Organizations allocate substantial resources to draw partners, customers and employees to product information, services and commerce on their websites. Customers quickly navigate to these websites trusting that it is owned and operated by the branded organization. However, despite the best safeguards, an organization’s brand can suddenly become compromised by fraudulent lookalike domains. A stealthy type of cyber crime called brand typo squatting is attacking organizations, infiltrating them through the fraudulent manipulation of the Domain Name System (DNS) naming conventions. Brand typo squatting creates a niche in an otherwise secure domain to launch one of the following attacks:

- **Brand Infringement** - Unauthorized use of a trademark.
- **Brand Dilution** - Malicious use of a brand, diminishing its perceived quality.
- **Brandjacking** - Assuming the online identity of another entity to use that organization’s brand equity.
- **Brand Typo Camping** - Registration of a “typo domain” that is lexically similar to a brand with the intention of launching one of the three attacks listed above.

Actionable Intelligence to Stop Brand Erosion

Brand Sentry enables an organization to monitor its brands for unauthorized or uncharacteristic usage in real time. The actionable intelligence empowers an organization to quickly identify illegal, infringing or threatening incidents against their brands in order to stop and prevent future breaches. The Brand Sentry solution monitors the global Internet and triggers an alert when an organization’s brands or lookalikes are first detected in the DNS.

Many of these newly-created, fully qualified domain names (FQDNs) are used in phishing attacks against users, customers and partners. They are also used for brand counterfeiting, brand abuse, identity theft and intellectual property abuse.

Subscribing to Brand Sentry dramatically reduces an brand vulnerability by providing:

- **Early detection** of lexically similar, FQDNs that are close (or exact) matches to a brand name. These FQDNs, rapidly used after creation, often indicate criminal intent.
- **Notification** either through JSON blobs or NMSGs, any time a new domain is observed that seems suspiciously similar to an organization’s brand. (https://farsightsecurity.com/Blog/20150128-nmsg-intro/)
- **Advance warning** that enables a security team to integrate data into Splunk/SIEM solutions to analyze phishing attacks against partners, customers and employees, as well as brand counterfeiting.
About Farsight Security

Farsight Security provides the world’s largest real-time actionable threat intelligence information on how the Internet is changing, with more than 200,000 observations per second. Farsight Security provides security solutions to leaders in the health care, consumer brands, banking, travel, and securities industries, as well as government law enforcement agencies.

How Brand Sentry works

Brand Sentry begins with subscribers defining brands as text strings as well as good hosts or subdomains to be whitelisted. Next, subscribers specify one or more ‘match engine modules’ - each offering a different class of matching (literal, homoglyph or phonetic) and a different type of matching method (substring, regular expression, etc.). Finally the brands, whitelist and match engine modules are loaded into the Match Engine and then Brand Sentry monitors matches that may be indicative of abuse. The goal is to determine how similar an FQDN is to a specified set of brands.

Brand Sentry monitors Farsight Security’s Newly Observed Hostnames in real-time and compares each FQDN (known as a Candidate) against the brands and parameters of the Match Engine. If a match is found, a real-time alert with data surrounding the specific event is sent to an organization. The organization can then use this information to take action against the threat.

The Muscle Behind Brand Sentry

Farsight observes millions of domains each day. Using the historical DNSDB database as a delta, Farsight detects that more than 100,000 of these are newly-configured domains daily. Leveraging more than 5 TB of daily real-time Passive DNS data, Farsight discovers when these domains are first used.

Other discovery methods, such as TLD Zone File Access and WHOIS, can’t identify newly-configured domains until 17 hours after registration.

How to Subscribe

For more information, contact sales@farsightsecurity.com or call +1-650-489-7919.