4 Roles of Domain Name Monitoring in Making Cybersecurity Decisions

Posted on November 5, 2019

You might be surprised to find out, but there's a lot you can tell about a domain name or a group of them from the cybersecurity standpoint. You may attempt to understand what the intentions of a registrant are, check for the consistency of data provided across touchpoints, get some insights into the scale of online operations, and more.

Overall, gathering and applying domain intelligence allows cybersecurity specialists to decide whether it's in the company's best interests to let information flow with unknown external agents. Or if, on the contrary, the risks outweigh the benefits so much that interactions should be at least heavily scrutinized or blocked altogether.

This post explores a variety of more specific situations where domain intelligence can help in making the right cybersecurity call at different levels of the organization and beyond it.

1. Prevent Social Engineering Scams

With people generally considered the weakest link in cybersecurity, scammers often pretend to be someone the victim trusts to steal a company's confidential data. Particularly worrisome is the rising number of targeted attacks such as business email compromise (BEC) where a fraudster poses as a high-ranking company officer.

The trick here is about using authority to compel victims to transfer funds to their own accounts. But there are ways to deceive the recipients. For example, they may be prompted in downloading attachments containing malware or clicking on links that appear legit but redirect to forged sites.

Domain data can prevent such phishing and spoofing attempts by serving as a means to verify if emails actually originate from where they appear to be. More precisely, internal security teams and outsourced providers can check a suspicious sender's domain with its WHOIS records. Some signs of alerts include private or incoherent registrant details or suspiciously recent registrations.

2. Protect Trademarks from Typosquatters

Your trademarks and other intellectual properties are online assets that identify your brand or company. As such, they are attractive targets for copyright infringers eager to cash in on your popularity or avid competitors looking to tarnish your reputation.

Typosquatters typically register domains that are strikingly similar to yours in the hope that your typos-prone customers land on them instead of your website. A brand monitoring tool can help you spot misspelled variations of your domain name practically in real time. Being aware of new registrations allows you to be more proactive — e.g., warning your customers, opening a domain dispute, etc.

This undertaking is particularly relevant in light of the emergence of countless new gTLDs that give lots of room for the impersonating of brands and misleading of customers. In fact, a recent domain abuse and activity report from the Internet Corporation for Assigned Names and Numbers (ICANN) found that more than half of all security threats emanate from new gTLDs.

3. Prevent Supply Chain Attacks

Confirming the trustworthiness of the people and companies that you do business with is important because dubious characters can infiltrate your company if you don't. With that in mind, domain monitoring can help you screen potential partners, suppliers, resellers, and other stakeholders.

You can work with our Domain Research Suite dashboard to check the history of a domain name. This information lets you know if someone you thought you knew may be trying to fool your employees.

A technique scammers may use, for example, is purchasing the domain name of a company that

ceased to exist or changed its branding and is now operating under a different registration. By getting familiar with domain history, you can find out about any recent new owner with whom you actually never did business before.

4. Enhance Managed Security Services

MSSPs brings in security specialists and technological tools and systems for detecting and responding to threats on behalf of their clients. However, these professionals are heavily reliant on the information made available to them to speed up detection and response as well as to avoid false positives and negatives.

Domain name feeds offer them a rich source of threat intelligence to thwart intrusion attempts and identify the entities behind them accurately. Moreover, these sources can indicate the existence of established criminal networks and nation-state hackers through the identification of malicious connections. Connected domains may, for example, have been registered on the same day, share the same physical address, or are owned by characters or organizations with questionable reputations.

Securing a business operation is no mean feat if you don't have the right tools or have no idea where threats could come from and in what form. Bad actors are becoming really ingenious at disguising themselves, and stopping them requires access to domain intelligence that can contribute to their identification.

Comprehensive domain information contained in our enterprise packages offers a versatile cybersecurity solution to identify, investigate, and respond against bad actors and threat indicators. Contact us for more information.