Threat Prediction Based on Domain Registration History

Posted on December 26, 2019

There is a tendency to look at the past to anticipate what the future may hold. The historical performance of financial investment products, for example, is always showcased, although with a disclaimer that they don't guarantee any future results. Athletes watch past performance of their would-be opponents, so they know what strategies to formulate for the future encounters.

This train of thought is also applicable, at least to some extent, to the field of cybersecurity. Knowing more about past attacks can help security teams strategize and improve their current and future cybersecurity posture.

To illustrate this point, let’s take a look at how investigating domain registration history through the use of WHOIS History API can help managed detection and response (MDR) teams to anticipate further threats.

Domains as Threat Vectors

Domains should be generally considered as potential threat vectors. They can, after all, be used to launch attacks such as phishing and other malware-instigated campaigns. Phishing, which requires attackers to use domains similar to those of trusted entities, is behind 90% of data breaches. This success rate is just too high, and thus it calls for automatic identification and blocking of malicious domains. But how?

Researchers found that out of the 200,000 newly registered domains (NRDs) per day, 70% are used maliciously or aren’t safe. Yet another study found that of all the registered-level domains (RLDs), 57.6% are reused while the rest are new registrations.

These statistics tell us that while attackers invest in NRDs, many also reuse previously registered domains. These findings highlight the importance of examining a domain's registration history.

What Information Does WHOIS History API Reveal?

A WHOIS API or lookup tool allows anyone to access our comprehensive WHOIS database and see any website's domain records. Basic WHOIS records show the following:

- Registrant details including his/her name and contact details
- Registrar information such as name and contact information
- Registration details including the creation and expiration dates as well as the date when the record was last updated
- Technical, administrative, and billing contact names and details
- Nameservers

WHOIS History API returns all this information - and more. It also exposes the domain's registration history records, giving users an idea of the changes in its ownership over the years. WHOIS history data can also be gathered from WHOIS History Search, a component of the Domain Research Suite that gives access to an exhaustive and well-structured database that houses more than 6.7 billion historical WHOIS records. It crawls over 582 million domains and about 3,000 top-level domains (TLD).

How Domain Registration History Helps in Predicting Threat Vectors

Track a Domain's Historical Footprint

Having access to websites' historical records allows users to get a glimpse of domains' historical footprint — valuable information that can reveal past and current owners' activities. More and more attackers hide behind seemingly innocent domains, either newly registered (misspelled variations) or expired (typically abandoned), to trick victims into believing that those belong to trusted contacts.

A 2017 independent research on abandoned law firm domains (when hacked) could provide attackers with personally identifiable information (PII) from bank notices, corporate debit card statements, business travel reservation documents, invoices, and others.

With historical domain data, security teams can find out if an email sender's domain is genuinely associated with the entity. Some can reveal past connections to suspicious activities. That way helps to identify possible sources of threats that should be blocked.

WHOIS History API findings can be fed to a company's security solutions or systems to enable automatic identification and blocking. Then, no employee will receive emails from spotted malicious domains or access the corresponding unsafe websites in the future.

Determine If a Domain Poses Threats

In-depth investigations can be done when an alert is triggered by a domain's registration history either manually or by using security tools. Organizations can, for instance, use Domain Reputation API to quickly determine a domain's reputation score.

The reputation score is calculated based on hundreds of parameters, including the domain's association with malicious domains and mail exchange (MX) server reputation. The tool also checks the domain for links to .apk or .exe files. Domains with low reputation scores can be automatically blocked if the API is configured to do so and integrated into existing security solutions and systems.

Better still, organizations can integrate any of WhoisXML API's various APIs into MDR solutions or systems so they can gather as much threat intelligence as possible.

Threat prediction is key to prevention and protection. While the word "prediction" implies the mystic ability to see the future, there is such a thing as an intelligent prediction to anticipate where cyber attacks may come from next. MDR and other security teams shouldn't rely on visceral foresight, but instead examine multiple sources of data, including **domain registration history** and domain reputation information.