How MSSPs Can Enhance Network Resilience with the Help of Domain Name History Records

Posted on February 6, 2020

Threat management has grown increasingly complex for most organizations — with more endpoints to secure, new compliance pressures to face, and advanced persistent threats (APTs) to monitor. As a result, several organizations have opted to modify their approach to network security by enlisting the help of managed security service providers (MSSPs).

MSSPs combine different approaches to enhance network reliability, ranging from unified threat management (UTM) to threat intelligence analysis. The majority also implement business continuity (BC) solutions, which are especially crucial in the wake of recent global cyberattacks. To facilitate their programs, they incorporate various tools into their security systems, including traditional firewalls, traffic logs, cyber forensic solutions, and threat data feeds.

The tools that MSSPs use to improve clients' security posture, however, won't work without reliable sources of threat intelligence. And that's where domain information comes in. MSSPs can obtain more insights and data to correlate with internal logs from solutions such as WHOIS History API.

Domain Name History Lookups Boost Network Integrity

A massive chunk of MSSPs' responsibilities focuses on correlating events with intelligence to improve network uptime. As such, security researchers may rely on **domain name history** records to generate attack forecasts and corresponding reports.

WHOIS History API extracts a domain's ownership history from our vast WHOIS database. Each entry details changes made to domains over the past decade, before privacy restrictions were implemented. The output is then normalized and well-parsed for easy analysis.

Below are some of the areas where MSSPs can employ the API.

- **Improving network configuration:** As endpoints become more distributed, it is critical to ensure that an organization's network is configured correctly for seamless telemetry. Security

analysts can evaluate their domain infrastructure with additional data from historical WHOIS records. By knowing the past and present nameservers attached to their domains, engineers can perform more in-depth analyses of their systems.

- **Regulating network traffic behavior:** Network engineers can perform better deep packet inspection (DPI) by cross-referencing WHOIS data as well. WHOIS records can be used as a basis for establishing relationships between domains attached to the same IP address. The records provide users with the target's nameservers, which can then be scanned for anomalies with a reverse NS API. Results from this can reveal malicious hosts sending requests.

- **Enhancing email security:** Cybersecurity professionals can use WHOIS records as a starting point to conduct other lookups to verify the validity of email senders and the reputation of their hosts. Users can scan the sender's domains with an email verification API to learn more about their owners and namespaces. The API can be integrated into email security solutions to automate validation as well.

- **Monitoring network access:** WHOIS records provide actionable intelligence that enables engineers to simplify their network segmentation. For instance, they can verify if a nameserver is configured correctly based on historical WHOIS data. MSSPs can also secure their clients' workloads and edge by efficiently using the information. In short, domain data helps pinpoint attackers attempting to gain unauthorized access to their network.

- **Blocking known threat sources:** WHOIS records allow incident responders to identify domains related to nefarious activity. In fact, a Domain Name System (DNS) database provides them with information on connected domains. These can be compared with various threat feeds to determine attack trends.

Other Useful Applications of Historical Domain Data

Domain records also provide enterprises with detailed customer insights that they can use to improve existing business campaigns. Domain data also helps them protect their brands from

entities that aim to use their marks in bad faith. Here are some initiatives where historical WHOIS records can help:

- **Big data analytics and marketing:** Business professionals can build robust marketing strategies by studying domain histories. The API results can be used to analyze market trends, build demographic reports, and monitor competitors' digital properties.

- **Protecting trademarks and digital assets:** WHOIS records provide enterprises with contact information of potential cybersquatters. With Whois History API, they can also identify registrants with a history of domain squatting and keep tabs on their next moves.

- **Avoiding the potential purchase of bad domains:** It is common practice for entrepreneurs to purchase and use old domains for their websites. However, not all old domains that are up for sale have a good reputation. Their previous owners may have abandoned some due to search engine results page (SERP) violations. Others may have been left behind due to blacklisting. WHOIS History API can serve as a starting point for doing thorough background checks on old domains that users may be eyeing for their use.

Time is money. To prevent costly damages brought on by network downtime, organizations should deploy security appliances that allow them to respond to incidents and prevent threats with real-time precision. In addition to internal network data, contextual information coming from external sources could come in handy. **Domain name history** records reveal exhaustive information on an adversary's background, making them a great addition to any infosec professional's toolset.