How Conducting a Domain Reputation Check Can Improve Incident Response

Posted on December 9, 2019

Indicators of compromise (IoCs) are crucial elements of the incident response process. From identification and containment up to eradication and recovery, security teams need to be on the lookout for IoCs to detect the presence of a threat in real time. When so, responses to cybersecurity incidents are quicker, more effective, and less costly.

One key source of IoCs is domain reputation data, which is aggregated by using a wide range of factors. Domain Reputation API, for instance, allows performing a **domain reputation check** from which it derives a score from the following:

- The domain's WHOIS record
- Website content
- Associations with other domains
- Secure Sockets Layer (SSL) certificates, connections, and configuration
- The domain's IP address infrastructure
- Alerts from various malware data feeds
- Domain Name System (DNS) and mail exchange (MX) record configuration
- Nameserver (NS) configuration
- Reverse IP lookup results

Using an algorithm that takes into account all of the abovementioned factors and hundreds of other parameters, Domain Reputation API returns a score for a domain, along with more information on the vulnerabilities detected. The scores range from 0 (highest risk) to 100 (lowest risk).

How Domain Reputation Data Improves Incident Response

Identify and Block Malicious Domains

Around 200,000 newly registered domains (NRDs) are recorded every day, many of which have ties to malvertising, spamming, and other cyber-attack avenues. Malvertising, for one, is used to lead unsuspecting users to pages that host exploit kits that pave the way for ransomware, spyware, and other malware into systems.

With millions of active domains — a good portion of which is malicious — security teams can find it beneficial to include **domain reputation checks** for websites their staff frequently visits.

Considering an example, imagine a scenario where an employee of an advertising agency searches for free video-editing software online and comes across this domain: youtube-self[.com] (warning: do not visit!).

When fed into Domain Reputation API, the domain is tagged malicious (at the time of writing) due to its low score and red flags including recent registration, its recently obtained SSL certificate, and the fact the domain name itself does not match the certificate.

Part of the incident response process is determining whether or not a domain flagged as malicious is a false positive. If the domain indeed represents a threat, the employee's connection should be denied or conditionally resolved. It is also best to block the domain from being accessed by anyone else in the future to avoid compromise.

Determine the Specific Violations of a Domain

Security teams can check the violations or warnings associated with a domain to understand if it is a potential attack vector. With this knowledge, they can improve the rules set in their automated incident response systems, thereby strengthening their cybersecurity posture.

Identifying the specific violations or warnings detected on a domain is easy with Domain Reputation API. The 75 warnings that it returns include the following:

- **Domain status:** The API warns if the domain's status is unknown. It can thus be malicious, and so needs further scrutiny.
- **Registration date:** Security teams can check if a domain has been recently registered or if its registration is about to expire or has expired. Note that cyber attackers often use NRDs to evade detection.
- **Place of registration:** The tool can detect if the domain was registered in a free zone or an unexpected country. Some countries have very lax or even non-existent cybercrime laws, making them safe havens for criminals.
- **A and AAAA records:** Domain Reputation API also checks the A (IPv4) and AAAA (IPv6) records of the domain. It can detect if nameservers have no A and AAAA records and are, therefore, not reachable via IPv4 and IPv6 protocols. If that's the case, they may not be safe to access.
- **Redirects and links:** The tool tells security teams if a domain contains redirects, links to .exe or .apk files, and scripts that open in new windows. The API also detects iframes. The presence of these can be indicative of malware hosting.

These are just a few of the domain reputation data that the API checks, giving security teams rich information that can better shape their incident response strategies. This data can help security operations centers (SOCs) determine if they are detecting ongoing targeted attacks.

Filter Email Senders Based on Domain Reputation Score

A **domain reputation check** performed by Domain Reputation API also includes checking data on MX servers and their status. With the help of other data feeds, the tool can check if an associated MX server is blacklisted by any reputable sites. The API also detects (through a reverse DNS search) if the MX server resolves to an IP address that differs from that indicated in its original A record.

SOCs can then filter out and reject emails sent from MX servers with high-risk scores, saving employees from the temptation of opening a malicious email. They can also use the MX server data to improve their incident response process by implementing additional rules that enhance existing ones.

Forewarned is forearmed. With the domain reputation data gleaned from Domain Reputation API or Domain Reputation Lookup, security teams can enhance incident response for a large variety of threats and better protect users.