Optimizing Threat Hunting with Bulk Domain Search

Posted on January 14, 2020

Threat hunting involves proactively looking for signs of attack within your network, by means of a set of indicators of compromise (IoCs). These IoCs are compared with network access logs to pinpoint if any of the users are unauthorized. More specifically, threat hunters can use Domain Name System (DNS) and firewall logs to list all IP addresses and domains connected or trying to gain access to the network.

This is relevant because many attackers typically hide malicious traffic within legitimate traffic to successfully infiltrate a target network. Once that is done, they can easily carry out the rest of the steps in their carefully orchestrated attack. Attackers will generally wish to gain command and control (C&C) of a system to gain entry into connected systems and devices. When that's done, they can move laterally throughout the network and exfiltrate data to their own remote servers. Since they are using compromised systems, the C&C traffic typically goes undetected.

However, anomalies such as when a system that is not designed to upload data to servers but does so anyway can be indicative of an ongoing attack that threat hunters should look into.

How to Spot Unusual Domain Name System Requests for Enhanced Threat Hunting

Know What Is Normal from What Is Not

It is crucial for cybersecurity staff to know which of their internal systems typically communicate with external servers or systems, how much traffic goes out of their network within a given period, or where the systems and servers their network communicates with are located. That said, when they know that their organization does not do business with offshore companies from a said country, for instance, but a system is sending data to a server based there, they should dig deeper into the issue. Doing so is especially critical if large packets of information are being transmitted.

Stay in the Know

For their schemes, attackers register or compromise multitudes of domains each day. It is therefore an excellent practice to continuously update company blacklists and blocklists to ward off threats. Bookmarking publicly accessible spam, malicious URLs, and malware databases and adding identified IoCs to your blacklists and blocklists is a great proactive approach toward cybersecurity. Keeping up with security news from reputable news sites and security vendor blogs can also help.

Watch Out for Signs of Domain Generation Algorithm

Threat actors can hide spyware that sends out stolen data to their C&C servers using a domain generation algorithm (DGA). This evasion tactic allows malware to generate new domains for their C&C communications based on a given period, for example, and so avoid detection and blocking. If a system accesses various URLs within a day, that could be a sign that it is infected with a DGA-enabled malware, and so needs attention and remediation.

Heed NXDOMAIN Responses

DNS servers that cannot resolve to a particular domain issue NXDOMAIN responses. Such responses occur when you misspell the website URL, or when the servers have misconfigurations, or the servers are infected with a DGA-enabled malware that turned them into bots. Make it a point to run regular checks on your domain infrastructure to make sure none of your DNS servers are returning NXDOMAIN responses, which can indicate malicious activity.

How Can Bulk Domain Search Tools Aid Threat Hunters?

Attackers do not usually use a single domain to compromise targets. That would lessen their chances of effectively compromising their victims' networks. They are, in fact, known for registering domains in bulk. And so like threat actors, threat hunters must also be capable of identifying several malicious domains at one time. That can be made possible with the use of Bulk WHOIS Lookup.

Let us say that you obtained 100 domains that may be linked to an ongoing attack. You can only tell which are malicious if they used a given email address (i.e., one that belongs to an identified threat actor). You can use Bulk WHOIS API to get detailed WHOIS records for each domain and only block those that have the same proven malicious email address, for example. That way, you prevent anyone in your company from visiting related malicious sites and pages while still allowing them to access those that have been deemed safe to access. You never know, because some of the users connected to the harmless domains can be potential customers or clients, and blocking them would be therefore detrimental to your business.

Apart from shared email addresses, threat hunters can also use shared or common name servers, registrants, organizations, street addresses, and phone numbers to filter good domains from bad ones.

Bulk WHOIS Lookup is a useful **bulk domain search** tool for threat hunters who need to sift through tons of IoCs and logs amid a landscape where attacks occur left and right. It can help security teams streamline their search and investigation efforts, giving them more time to spend on incident response and future attack prevention.