Tracking Domains for Cyber Self-Defense

Posted on August 10, 2018

In 2008, hackers hijacked CheckFree.com, which provided online bill payment services and redirected traffic to a website in Ukraine. The fake CheckFree website downloaded malware on CheckFree customers' computers. The malware stole usernames and passwords. Even worse, it infected the computers of customers of minor banks that had partnered with CheckFree. The banks' websites had been directing their users to CheckFree.

Neither CheckFree nor the banks had been monitoring changes in the WHOIS registries of their websites. If they had, they would have seen the redirection hackers had placed in domain records.

Cybersecurity product makers like WhoisXML API offer tools to monitor any changes in domain registries that may indicate hackers are tampering with pointers. Professionals can use the tools to monitor their own company domain entries or the domains of websites suspected of malicious activity.

The Man-in-the-Middle Is Not Your Friend

Some hackers, though, are even more subtle than the CheckFree criminals. One company had its domain hijacked for almost five months without their knowledge. The cybercriminals had chosen not to redirect visitors to another website, as is the case of the CheckFree heist. Instead, they would send users to the intended domain and then monitored all the company's digital traffic. The black hats routed all the company's website traffic and emails through a set of servers that the hackers were controlling.

Domain hijacking puts sensitive corporate information at risk. And in these days of heightened awareness of data breaches, a well-publicized intrusion may mean the end of a company's reputation -- or of the company itself.

This Is How They Do It

Every day, hackers around the world are trying to gain control over the accounts of services that host the domains of websites. Once an intruder has infiltrated the account they can modify or add records in your zone data to alter responses to user queries to the website. Instead of forwarding

requests to genuine web pages, the altered registry sends users to malicious websites that promote phish bait or drop malware onto computers.

Attackers also hijack domain name registration accounts to change the configuration of the website entries so that the name server addresses in the domain configuration point to a system, name server software, or malicious zone data the attacker manages.

The WHOIS XML API Advantage

WhoisXML API offers a host of tools with which infosec professionals can analyze data on the WHOIS database. The most effective products the company offers to monitor changes in domain registries and domains suspected of malicious activity include:

- Domain Reputation Scoring
- Connected Domains API
- Domain Malware check
- Registrant Monitor
- Brand Monitoring

Domain Reputation Scoring enables cybersecurity analysts, researchers, and threat investigators to determine whether a domain has a history of malicious activity. If domain registrars have cited that the domain has been responsible for dropping malware onto computers, for instance, the Domain Reputation Scoring API will report the site is in disrepute.

Bots controlled by hackers will often set up malicious domains under the same IP address. The Connected Domains API reports on whether a domain with a black history is part of a cluster of domains created with the same ill intent. The tool informs infosec researchers if network firewalls should be configured to block any traffic from the cluster of black sites.

Domain Malware Check API delivers users a composite safety score for targeted domains.

Algorithms gauge the level of a domain's mal-intent based on numerous security data sources. Within the range of 0 (dangerous) to 100 (safe) the API reports whether a domain is a potential threat. The API report also offers comments regarding dangerous domains, indicating which malware trackers blacklist it and why.

Registrant Monitor tracks all newly registered, updated & deleted domain names registered by specific individuals and company names. System administrators and threat investigators use the tool to monitor specific domain registrants. The API alerts users whenever their domain information appears in a newly-registered domain name.

Brand Monitoring helps infosec professionals and marketing departments to track any changes to domain names that will impact the reputation of organizations. Track all the newly registered and recently expired domains specifically for relevant keyword terms to protect brands online.

Without the proper toolkits, infosec professionals will grope in the dark trying to determine the domains that are safe to connect to. Cybersecurity engineers must also determine if hackers have compromised the domains for protection of which they are responsible. Whois XML API's provide a suite of proven solutions to some of the most vexing security issues on the internet.