Monitoring New Domain Registrations Effectively

Posted on June 16, 2023

An early line of defense for companies that want to protect their staff or customers from bogus websites is to monitor new domain registrations. Threat actors often use variations of well-known domain names to lure unsuspecting users to fake portals to steal their private information or drop malware onto their devices.

There are a few ways users can watch out for new domain names that closely resemble their existing websites or their customers' or suppliers' sites. But before we dive into them, let's review why monitoring new domain registrations is essential.

Why Monitor New Domain Registrations?

There are several reasons for monitoring newly registered domains (NRDs).

Marketing Research

Marketing professionals can use the registration information to conduct research and study market trends. It can also help identify new players in a particular industry. For instance, web development teams can use NRD data to detect newly launched companies offering the same services.

Cybersecurity Applications

Monitoring new domain registrations, either through an NRD database or new domain monitoring alerts, is also particularly useful for security professionals because bad guys register domains, too.

Like all other Internet users, cybercriminals need domains for their online operations. Carrying out web-based attacks using domain names provide threat actors much flexibility. Therefore, a new domain monitoring alert could play a vital role in proactive security.

Brand Protection

Monitoring newly registered domains that include your product or brand name can also be instrumental as a safeguard against cybersquatters, who sometimes aim to extort payment from the rightful brand owner in exchange for acquiring the domain.

How to Find Newly Registered Domains

Option #1: Newly Registered Domain Database

The first option would be to use an NRD database. WhoisXML API, for instance, offers the Newly Registered & Just-Expired Domains Database so clients can access hundreds of thousands of NRDs daily. Gathering insights from this data set enables companies to search for and monitor NRDs to enhance their brand protection and threat intelligence systems.

Here's an example of how this could work. As seen in this database sample, thousands of recently added domain names are registered daily across all top-level domains (TLDs). Analyzing NRD data may help reveal domains potentially typosquatting on popular brands, such as the ones in the table below.

Brand Name	Examples
Google	fmi-google[.]com googleipuclari[.]com googlemap-us[.]info
DHL	dhl-express[.]ltd dhl-pachetulmeu[.]com mydhl-folgen-sie-meineim-paket-de[.]com
Microsoft	reply-to-mailmicrosoftoffice365[.]com microsoftagreement[.]zip microsoft-edge[.]top

Netflix	netflixactualizar[.]com netflix-repay[.]com netflix-payments[.]com
Facebook	facebookminigroup[.]com facebookseller[.]com facebook-groups-766145341653006pl[.]online
Apple	find-appleidevice[.]com appleappleid[.]com lcloud-apple-i[.]com
WhatsApp	gbwhatsappoldversion[.]com whatsapps[.]ltd gbwhatsappproapk[.]com
Amazon	amazon-heip[.]com amazonks[.]store amazonnbrr[.]com
Instagram	instagramcini[.]com instagramvideoindir[.]com instagramcourse[.]com
LinkedIn	linkedinarchetype[.]com zolalinkedin[.]com berkshirehathawaylinkedin[.]com

Further analysis of this data may help reveal the entities behind the domains and check connections between them and the legitimate domains.

You can discover more types of free samples here to analyze and test how our NRD data works in your environment. Note that we also offer diverse NRD database subscription plans with varying features to meet different company needs.

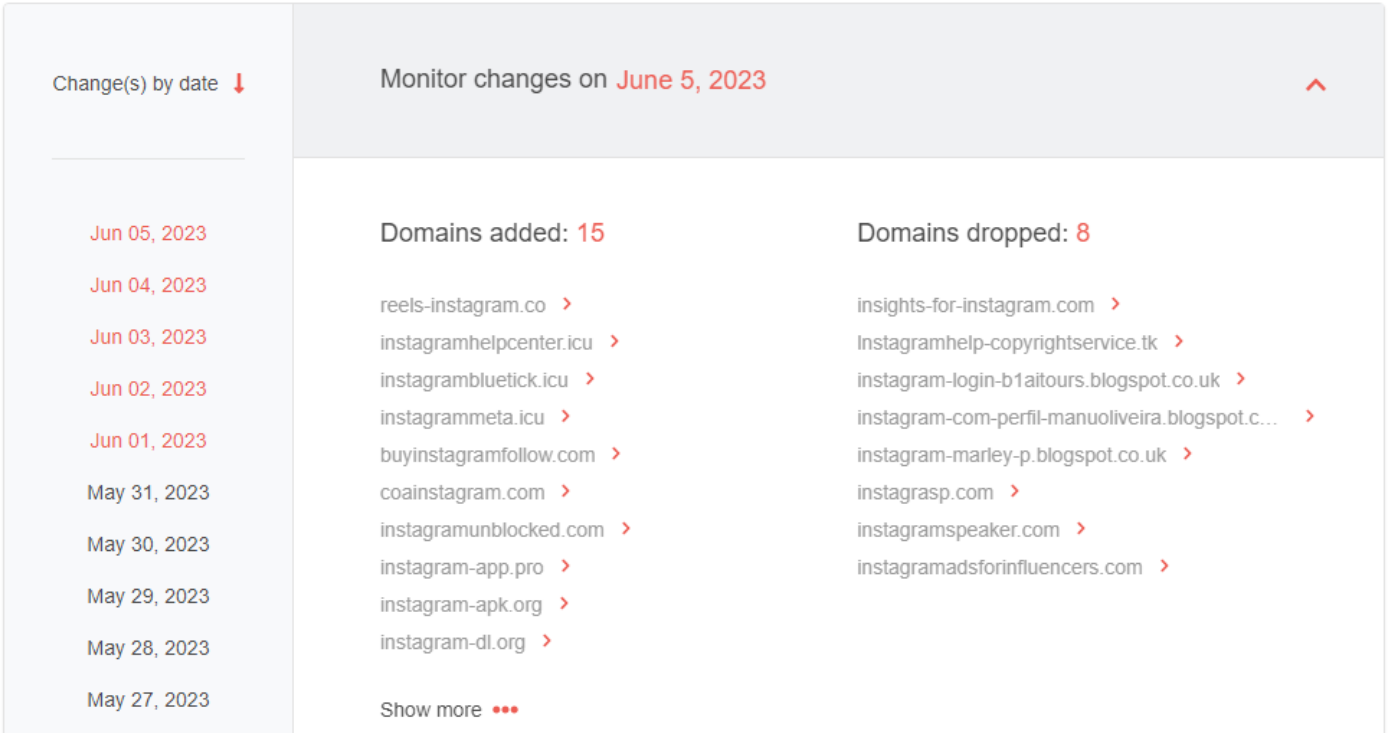
Option #2: Use Web-Based Tools

Another option would be to use a web tool or an application programming interface (API) that automatically sends alerts when new domains containing a specific string get added to the WHOIS database. Complementary tools can also help monitor domains and registrants of interest. WhoisXML API's Domain Research Suite (DRS) offers such capabilities, as detailed below.

Brand Monitor

Typosquatters tend to follow brands and piggyback on the popularity of their products and services. WhoisXML API offers a brand monitoring tool that tracks the new registrations and expirations where domains contain an exact or fuzzy match of brand names.

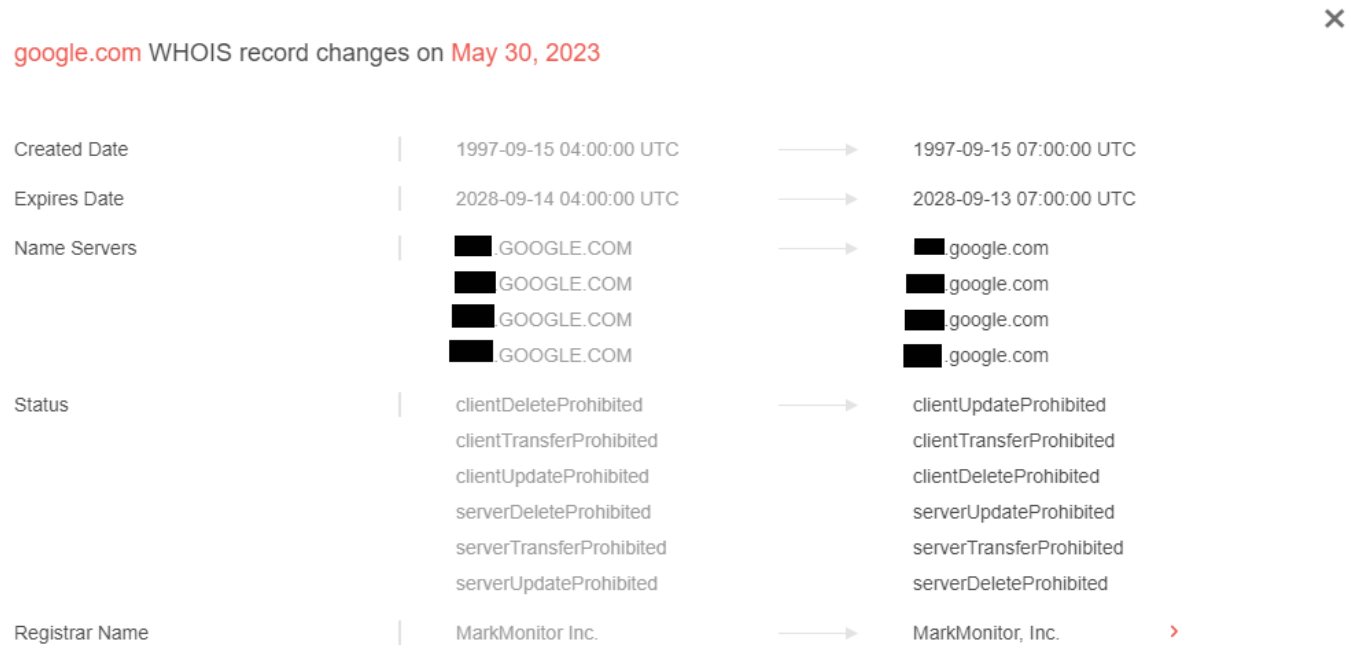
For example, a brand monitor for Instagram yielded 50 look-alike domains that were either added or modified within a five-day period. The screenshot below shows the Instagram-themed domains added on 5 June 2023.



Domain Monitor

Domain Monitor can help you keep track of new or old domains of interest. Whenever a domain's WHOIS record is modified, the tool sends an email alert to users, specifying the change that occurred.

For example, we added google[.]com to Domain Monitor. On 30 May 2023, we received an alert that some of the domain's WHOIS details changed as shown in the screenshot below.

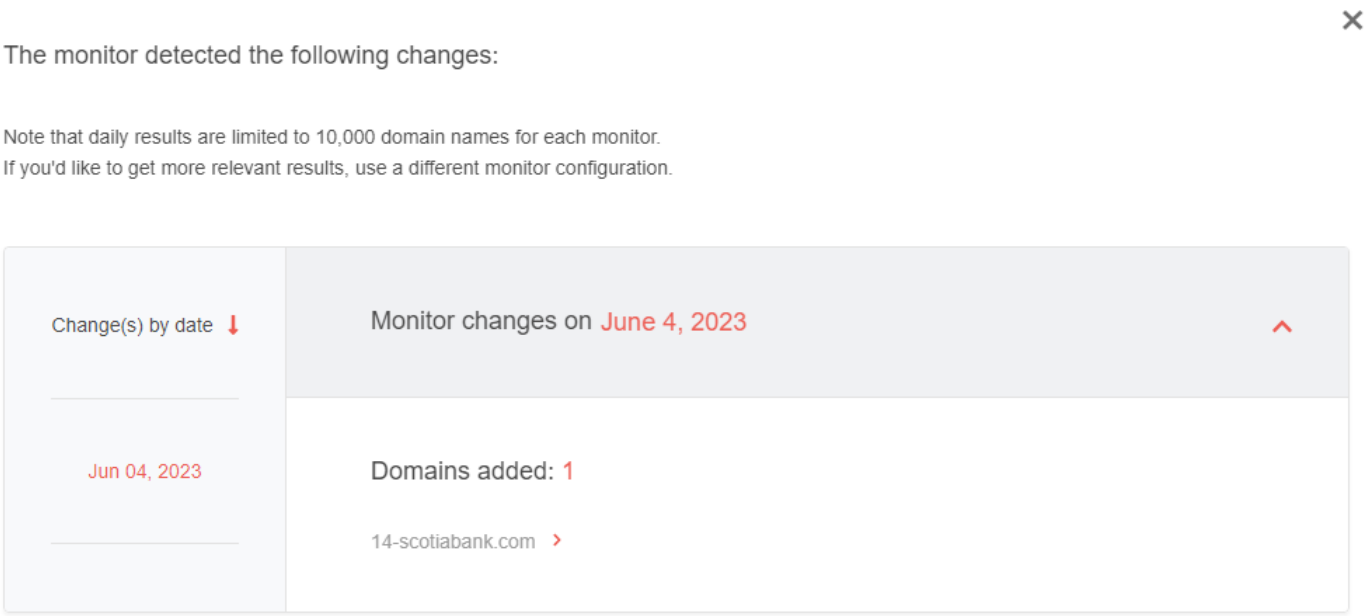


In the same way, cybersecurity professionals can receive email alerts regarding any change that occurred for the criteria they used to configure their monitors, such as update, creation, or expiration dates; registrant information; domain status; and more. For those specifically interested in NRDs, the tool will help by sending an alert once a previously unregistered domain becomes active, as indicated by a change in its Created Date field.

Registrant Monitor

Some cybercriminals may leave public information, such as an email address or a registrant name, behind as part of their malicious domain registration activities. Registrant Monitor allows you to keep tabs on such registrants and issue alerts whenever a specific registrant detail is used for new domain registrations, deletions, or WHOIS record updates.

For instance, an email address involved in registering typosquatting domains targeting banks was recently seen in the WHOIS record of a newly added domain—14-scotiabank[.]com.



—

The Newly Registered & Just-Expired Domains Database and other WhoisXML API tools can provide critical data to organizations and individuals regarding suspicious new domain-related events. Download a sample of our database to see how it can help enhance your threat hunting efforts and strengthen your cybersecurity and marketing strategies.