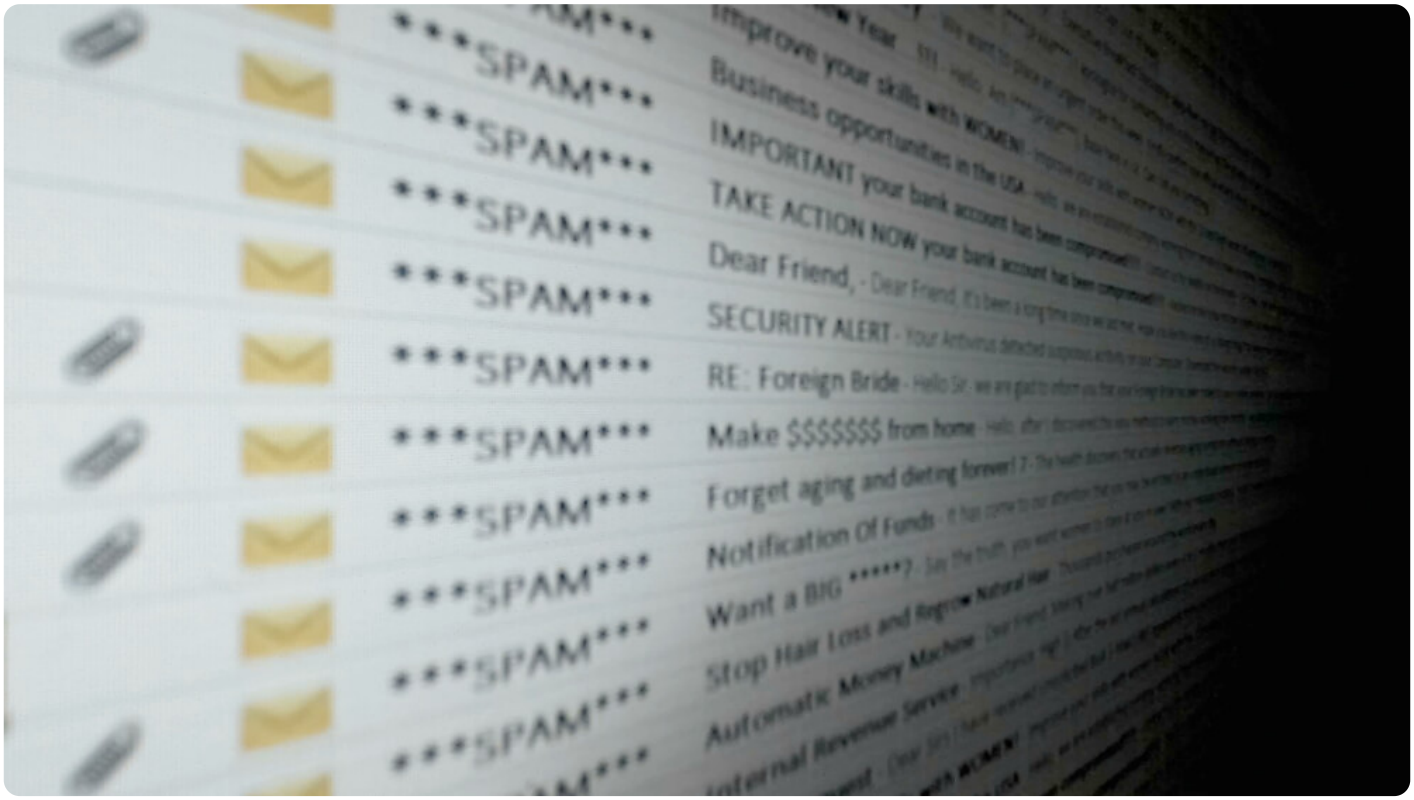
Warding Off Threats Spawned by the Abuse of Newly Registered Domains

Posted on December 27, 2019



When the Internet Corporation for Assigned Names and Numbers (ICANN) agreed to the addition of new generic top-level domains (gTLDs) in 2012 through the New gTLD Program, the number of spam emails coming from these domains started to rise significantly.

In fact, studies revealed that a new malicious site is hosted on a domain with a new gTLD extension every 15-20 seconds. What's more, seven out of 10 newly registered domains are classified as either suspicious or downright malicious and thus should not be accessed.

A possible reason for said criminal activities is that domains sporting the new gTLDs are relatively cheap in comparison to the more popular .com and .net domains. Another reason is that most credible name entries using traditional TLDs have already been taken. Either way, there seems to be a substantial amount of abusive domains registered using a new gTLD after its sunrise period (the 30 days during which trademark holders are the only ones entitled to register their domains), and, similarly, across registries.

As we know, spammers and phishers need tons of domains to pull off numerous scams at once. Going with cheaper, more available domains lets them cut down on costs, which makes sense from the perspective of threat actors since malicious hosts are often quickly taken down once detected as dangerous.

In this post, we further discuss the threats that come from **newly registered domains** and illustrate how Domain Reputation API and Newly Registered & Just-Expired Domains Database can help identify and assess potentially dangerous online properties.

Table of Contents

Age-Old Threats Get a New Lease on Life with New TLDs

Newly registered domains and new TLDs didn't lead to new cybercrime techniques. On the contrary, they have mostly revamped the packaging of the same old threats.

Spam Emails from Newly Registered Domains

Spam emails that regularly flood inboxes are not only a nuisance but they also pose security risks as these can come laced with malware or contain links to phishing and other malicious sites. And we all know that those threats can lead to information and identity theft or a network breach.

To date, the most abused TLDs worldwide by spammers are new gTLDs. These include (from the most to the least abused) .ooo, .desi, .gdn, .bar, .?? (xn--tckwe), .life, .world, .live, .ryukyu, and .work. These had badness index ratings ranging from 3.42 to 6.19 — translating to between 32.9-96.8% of the domains sporting these extensions to be categorized as malicious.

Interestingly, .ooo domains may have been topped one of the most favored new gTLDs for spamming because it has been dubbed "search engine optimization (SEO)-friendly." This wouldn't be surprising since, like legitimate registrants, spammers also do their best to end up on the first page of search engine results. That is, after all, an effective means of luring in as many victims as possible.

Debates regarding how to combat spam coming from **newly registered domains** thus surfaced.

Some opine blocking all such domains from accessing their virtual properties. Others think that this could be an extreme measure as companies may inadvertently block non-malicious visitors. It may be wiser to strike a balance between these two approaches.

Phishing Sites Find New Homes in the New gTLD Space

Phishers are always on the lookout for victims who will readily click the links they get from supposedly known contacts. The problem is that even if most people know about phishing, they still fall for scams. In fact, despite the threat's ubiquity, the number of phishing victims continues to soar over time with increasingly debilitating effects:

- Almost a third of the data breaches reported in 2018 involved some kind of phishing activity.
- More than 80% of organizations worldwide suffered from phishing attacks in 2018.
- The number of phishing URLs (including those used in business email compromise [BEC] attacks) rose by 269% from 2017 to 2018.

But what do these numbers have to do with **newly registered domains**? Well, reports say the share of phishing attacks stemming from domains using new gTLD extensions, especially .app, .ooo, .xyz, .online, .site, .club, .top, .info, .icu, and .website, has risen by 24% between the first and fourth quarters of 2018.

That's why, along with traditional anti-spam & anti-phishing solutions, organizations may find it useful to add domain research and monitoring tools to their arsenals. When a database of newly registered/just-expired domains and a domain reputation checker are used in tandem, they can help users to identify which domains are actually malicious based on counterchecks with several threat databases and, therefore, should be denied access to their networks. Said databases would help them determine all connected domains that should be blocked as well.

Malware Hosts in New (gTLD) Clothes

One of the most notorious malware types these days would probably still be ransomware. While the threat is now better understood, it is still causing tremendous losses. Victims, for instance, lost a total of US$3.6 million to ransomware operators in 2018 alone.

What's more, a 2018 research predicted that as many as 2,126 newly registered domains would play host to Cerber ransomware. GandCrab, a more recent ransomware variant, reportedly used a ".bit" domain for its command-and-control (C&C) server.

Typosquatters' New Safe Haven: The New gTLD Space

Humans are commonly dubbed "the weakest link in cybersecurity." A lot of corporate breaches result from human errors that include mistyping a link and causing employees to land on phishing pages. And more often than not, they end up giving their login credentials away to the bad guys.

Indeed, a simple typo could land any company in hot water. How? One plausible scenario would be when an employee uploads a file containing confidential customer data onto the wrong portal.

Let's say, for example, that a fictional company named "emendario" typically stores customer data on its online database emendario.com. Typosquatters could find this out and create a fake version of that portal, such as emendario.ooo.

They would, most likely, plant a keylogger into this fake portal in case an emendario employee lands on it and inputs his/her username and password. Even if the said employee isn't able to log in to the fake portal, the simple act of typing in his/her login credentials would already give the criminals what they want. The bad guys can then use the victim's credentials on the real portal to gain access to all the data stored in it.

You may think that .com and .ooo can't possibly be mistaken for the other, but what if the user just typed emendario and emendario.ooo ended up as the top result? If the user inattentively clicks that, the hypothetical scenario could turn real very fast.

Combatting New gTLD-Hosted Threats with WhoisXML API Solutions

Indeed, none of the threats discussed above are new. However, the emergence of new gTLDs has opened a lot of possibilities for spammers, phishers, malware distributors/operators, and typosquatters to register new domains that are seemingly looking like those of known brands and entities.

Organizations that rely on the Internet to keep their business going can mitigate the risks these threats pose with the help of at least two of WhoisXML API's vast array of domain research and monitoring tools — Domain Reputation API and the Newly Registered & Just-Expired Domains Database. Here is how these tools can help spot potentially malicious online properties.

Domain Reputation API at Work

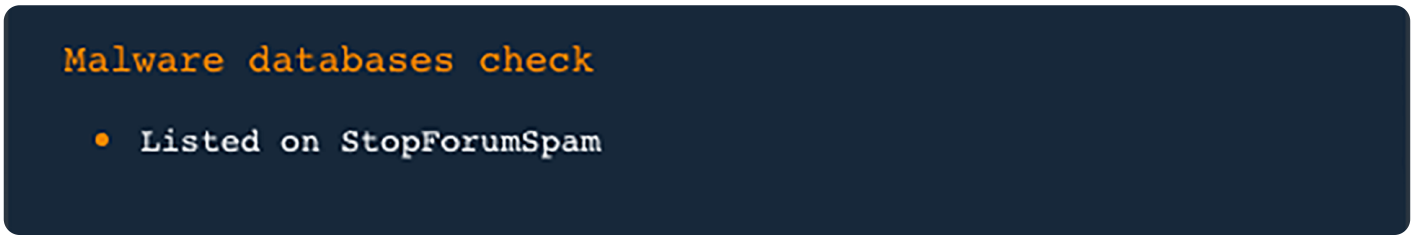
Domain Reputation API can be integrated into organizations' existing solutions, systems, and portals so that these can automatically determine if a URL is safe to access or not. The tool analyzes each domain or IP address according to several parameters that include:

- Website content and relation to other domains and host configuration
- A cross-check against numerous malware data feeds
- Secure Sockets Layer (SSL) certificate presence and validity, connections, and configuration

- Domain Name System (DNS) mail exchange (MX) record and server configuration
- WHOIS record details
- Nameserver configuration
- IP address connections

To illustrate how the tool works, let's look at a few examples following these steps:

- 1. Go to the Domain Reputation API page (https://domain-reputation.whoisxmlapi.com/api).
- 2. Type the suspect domain into the input field and click on the search icon. For this demonstration, we used a randomly chosen domain (i.e., googmail.gdn) with a new gTLD extension. Let's pretend it was used in a spam message that uses an enticing job offer as a social engineering bait. You should see this result:

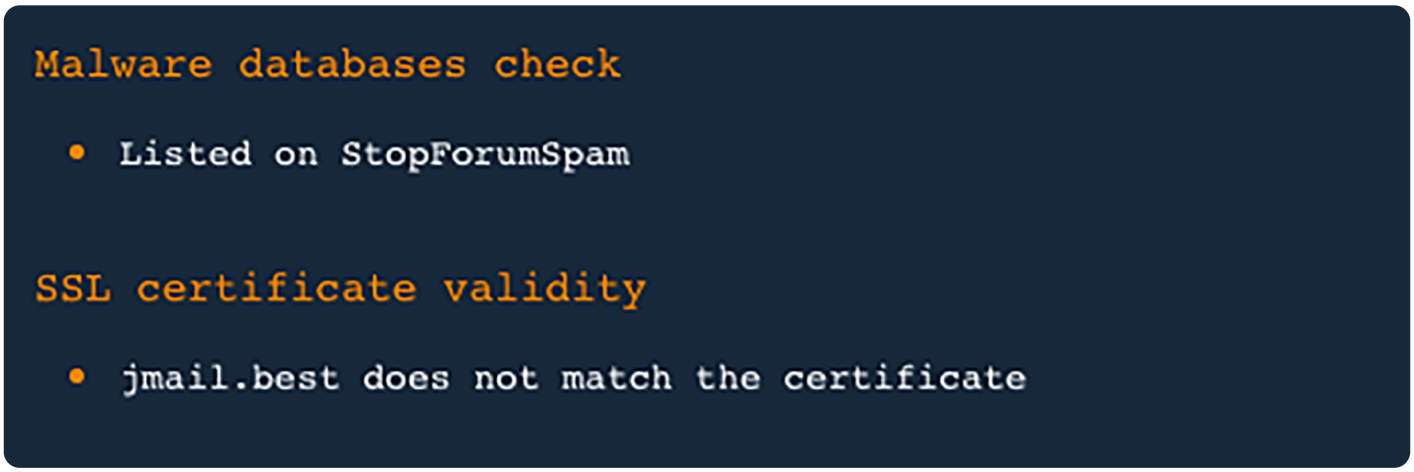


- Due to the domain's listing in the StopForumSpam blacklist, users would do well to consider including the domain in their blacklists too. Doing so would prevent any email using that domain from landing in their inboxes.
- 3. Deepening the analysis, the use of Domain Reputation API for assessing new gTLDs doesn't limit itself to a malware database check. Other results that may raise cybersecurity concerns include the following, analyzing a different domain name with another extension:

- The inconsistency between the domain and the site's SSL certificate and the presence of SSL vulnerabilities indicates that discretion and possibly blocking might be required in this case.

- 4. Now, let's say an employee wishes to purchase office equipment from a long-time supplier but accidentally mistypes the domain name. He/She thus lands on a spoofed site. Thinking the supplier just changed domains, he/she just proceeds like everything is normal and falls into the trap.A Domain Reputation API-enhanced firewall solution could have prevented that

employee from landing on the fake site in the first place, because of several warnings that include being listed on the StopForumSpam database and a mismatched SSL certificate:



Newly Registered & Just-Expired Domains Database in Action

Another way to stay on top of the threats posed by newly registered domains pose is by getting access to an extensive database that details all recent domain registration activity in nearly real-time.

With Newly Registered & Just-Expired Domains Database, users can quickly identify domains with new gTLD extensions that should be treated as potential indicators of compromise (IoCs). In order to do so, they can establish connections based on a shared:

- Domain registrant
- Contact email address
- Organization
- Street address

- Contact number (fax, phone, or both)
- Administrative, billing, and/or technical contact name and details

Let’s take a look at an example.

Say, for instance, that the domain avttw20146.info was cited as malicious in the news and is tied to an ongoing BEC campaign. (Note that the domain is not necessarily dangerous and was randomly picked from our sample database for demonstration purposes only.)

Digging further, you found that the email address used to register it was 2512483930@qq[.]com. Consulting the Newly Registered & Just-Expired Domains Database, you then realized that its registrant owns other domains (i.e., avttwbt.info, avttw20156.info, and avttw2018.info). Knowing that 2512483930@qq[.]com is a suspected BEC campaign domain, it would serve your organization to include all of the other domains sharing the email address in your blacklist.

That way, your company would be safe from any email coming from the suspicious email address. In turn, none of your employees would land on sites hosted on the potentially harmful domains because you’ve already blocked them up front.

7	anannaya-princessa.info	NameCheap,	25118bc9aa2f422389940
8	avttw20146.info	GoDaddy.cor	2512483930@qq.com
9	avttwbt.info	GoDaddy.cor	2512483930@qq.com
0	avttw20156.info	GoDaddy.cor	2512483930@qq.com
1	avttw2018.info	GoDaddy.cor	2512483930@qq.com
2	astrologerprediction.info	NameCheap.	25935fb47555403784f21

Concluding Thoughts: Threat Protection and Newly Registered Domains

Threat tactics, tools, and procedures (TTPs) have kept evolving over the years through the expansion of the Web and online properties. To help combat new forms of attacks as they emerge, it's important not to trivialize what some may consider as "old" threats, including spamming, phishing, and malware. Cybercriminals will use this lack of awareness to conduct fraudulent undertakings that new gTLDs and newly-registered and recently-expired domains can allow.

This post doesn't imply that all newly registered domains are malicious and should be avoided. After all, traditional TLDs are still widely used as well to conduct lots of cyber attacks. What matters, however, is the ability to discern between perfectly legitimate domain names and those acquired to cause harm.

Domain Reputation API and Newly Registered & Just-Expired Domains Database can help in that regard as they provide data points that are relevant for threat identification, assessment, and protection. Would you like to learn more about how our tools can help? Feel free to drop us a line at support@whoisxmlapi.com.