Subdomain Finder Tools and Data Sources: Top 4 Cybersecurity Applications

Posted on March 22, 2021

Subdomains are useful as they help domain owners organize their websites. They identify specific pages on a company's site, guiding customers and internal and external users to where they will find the information they need or product they wish to buy.

But while using subdomains indeed has advantages, it has disadvantages as well. Cybercriminals can use them for malicious campaigns that rely on subdomain takeovers, among other cyberattacks. Threat actors can also create subdomains and hide them under what seems to be totally legitimate domains to evade detection.

Subdomain-related threats are addressable, at least to some extent, with the help of a subdomain finder that enumerates the subdomains of a particular domain. This post explains how to go about it.

What Is Subdomain Enumeration?

Subdomain enumeration basically has to do with finding all of the subdomains under a given domain (e.g., subdomain1[.]paypal[.]com, subdomain2[.]paypal[.]com, etc.), though the process can be expanded to find all subdomains that contain a particular string, regardless of the root domain (e.g., paypal1[.]domainABC[.]com, paypal1[.]domainBCD[.]com, etc.).

Subdomain enumeration is a common part of passive reconnaissance, as it can help specify a company's web infrastructure for a variety of cybersecurity purposes, such as security assessment, vulnerability identification, and spotting old and likely forgotten web properties.

What Is a Subdomain Finder?

A subdomain finder can be called a "subdomain enumerator" or "subdomain scanner," as it enumerates and scans for all of the subdomains of a specific domain. It can come in various consumption formats that include:

- **Database:** An example would be Subdomains Database Download, a repository of more than 2.3 billion subdomains (and growing) generated from our passive Domain Name

System (DNS) intelligence. Users can download the database and use it to search for the subdomains of a given domain, including their WHOIS record details.

- **API:** An example is Subdomains Lookup API, a tool users can integrate into existing cybersecurity solutions and systems. Each query for a particular domain lists down its subdomains and when IP resolutions were first and last seen, as established from passive DNS data.

- **Web-based service:** Some examples are Subdomains Lookup and Domains & Subdomains Discovery, which are accessible to subscribers anytime. Subdomains Lookup provides the same details as Subdomains Lookup API but has the added benefit of generating custom URLs for easy sharing with teammates and stakeholders. Domains & Subdomains Discovery, meanwhile, is part of the Domain Research Suite (DRS). Thus, it gives users the ability to access all the DRS tools from the same dashboard.

What Intelligence Sources Can You Use with a Subdomain Scanner?

Subdomain scanners can be used with various intelligence sources to enrich cybersecurity investigations, such as:

- **WHOIS and WHOIS history search tools:** Let users compare the owners of domains that contain a particular search string. If any of the subdomain enumeration results turn out malicious, they can check who the root domains' owners are for further investigation or possible takedown. Those with redacted current records can be subjected to WHOIS history searches for clues.

- **Screenshot service:** Captures a screenshot of the page a subdomain may currently resolve to. The subdomain finder results could be pointing to obviously fake sites that may be part of an ongoing phishing or other malicious campaigns.

- **Passive DNS:** Reveals IP addresses connected to the domain or subdomain in question. The subdomain scanner results can be subjected to reverse IP/DNS searches to find connected IP addresses that may not be included in publicized indicators of compromise

(IoCs) but may need to be blocked on networks.

As the following section will show, the above-mentioned domain intelligence sources can be used alongside subdomain scanners, although indirectly.

4 Cybersecurity Uses of Subdomain Finders

Subdomain finders are especially useful for cybersecurity-related purposes, four of which are listed below with illustrative examples.

Use #1: Attack Surface Management

Any organization, especially large ones or those with a very strong online presence, need to monitor wild domains and subdomains as part of their attack surface management strategy. Wild domains and subdomains are web properties that use a company's brand name even if they are not necessarily under the said enterprise's control.

You can use Domains & Subdomains Discovery to look at the wild domain and subdomain footprints of the most-phished brand of 2020—Microsoft—if you happen to be part of the tech giant's cybersecurity team.

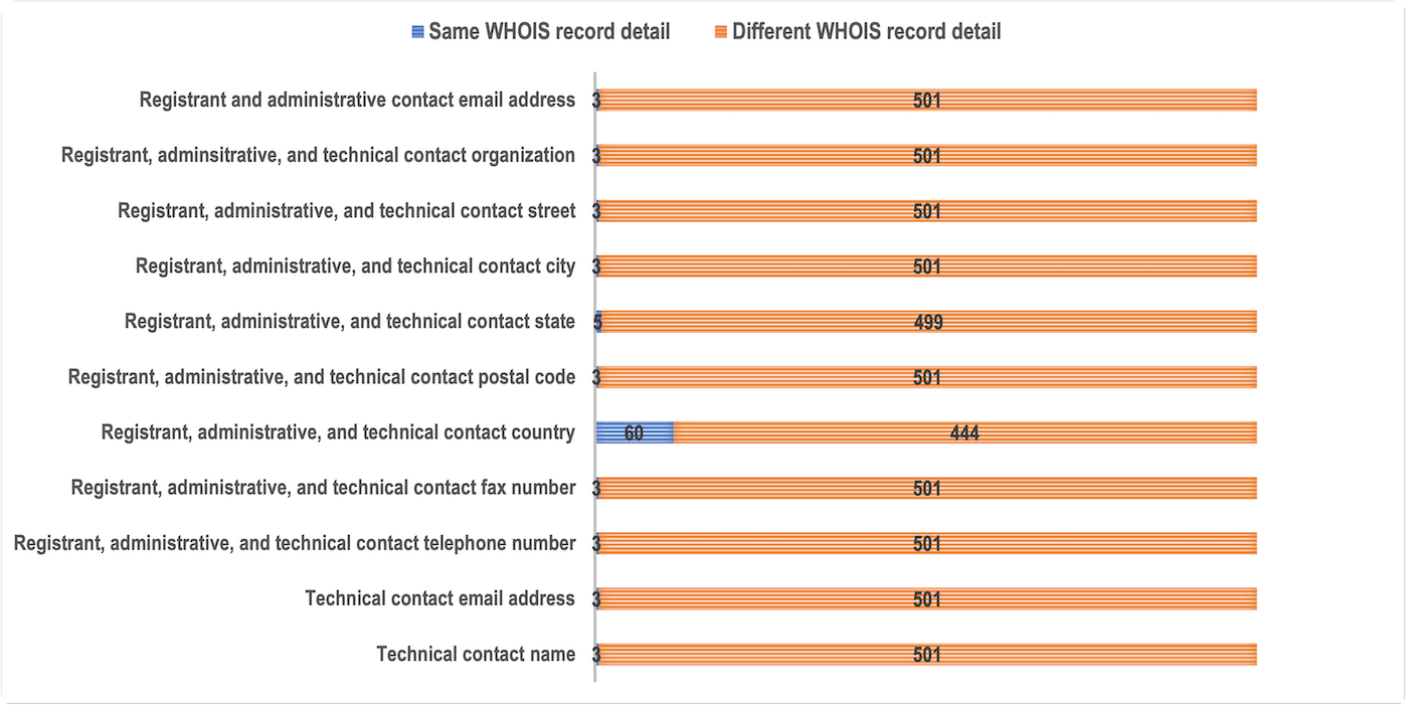
A search for "microsoft," for instance, looking back at a one-month period, would give you a list of 504 domains and 534 subdomains. These numbers go well over 10,000 if you are doing the same queries for the past year or so.

The company's security researchers can make sure that all of the identified domains and subdomains are under their control. If that is not the case, they may want to request for the web properties' takedown, as these could potentially figure in attacks targeting Microsoft's stakeholders.

As a first step, it's possible to check for ownership by comparing the WHOIS records of the identified domains and subdomains' root domains with that of microsoft[.]com.

From a bulk WHOIS lookup, we found that none of the 504 domains' registrant email addresses match those indicated in microsoft[.]com's WHOIS records. Only three of them matched

Microsoft's registrant contact name, organization, street, city, postal code, fax number, and phone number. Five domains matched microsoft[.]com's registrant contact state. Sixty of them matched Microsoft's registrant contact country. Based on the indicated technical details, meanwhile, only three of the domains matched microsoft[.]com's contact email address and name.



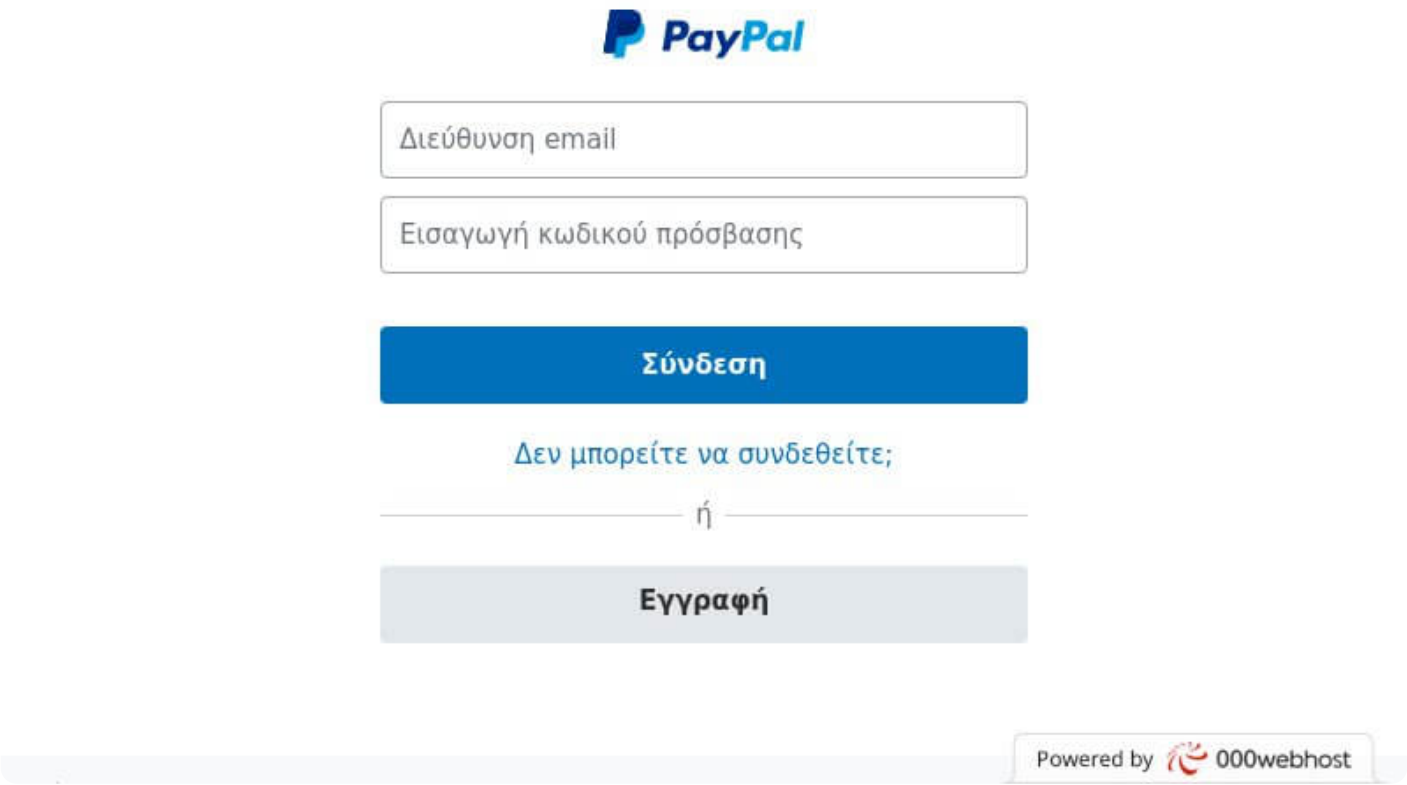
Given the results above, we can say that only three of the 504 domains could be under Microsoft's direct control, as they can be publicly attributed to the company as per the details they share with microsoft[.]com's WHOIS record. The remaining 501 are not and could possibly figure in malicious campaigns.

Use #2: Phishing and Fraud Detection

Phishing has been and still is a big threat to companies and their customers, employees, and stakeholders. But like other threats, it is addressable, at least partially, with the help of various tools and open-source intelligence (OSINT) sources.

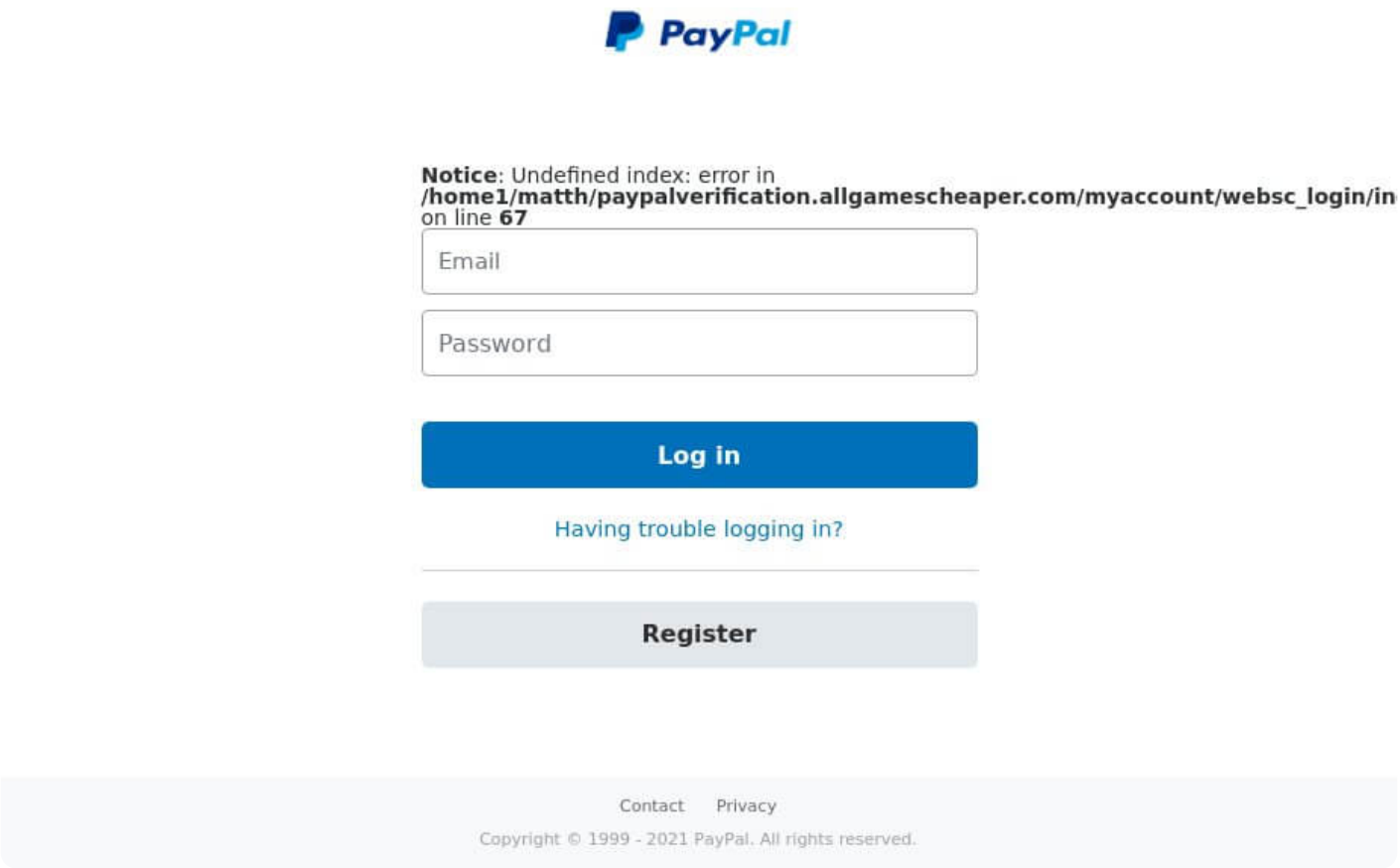
We found two confirmed phishing websites on PhishTank—covid2021onlyout[.]000webhostapp[.]com and www[.]paypalverification[.]allgamescheaper[.]com/myaccount/websc_login.

Using Screenshot Service, we discovered that these sites do not seem to match what their domain names (including their subdomains) convey. Here is a screenshot of covid2021onlyout[.]000webhostapp[.]com:



For what seems to be a COVID-19-related website based on its URL, it is odd that the page thelink leads to is a supposed PayPal login page.

Here is a screenshot of www[.]paypalverification[.]allgamescheaper[.]com/myaccount/websc_login:



For a supposed PayPal account verification page, the site seems amateurish given the error code. Threat actors do not always take time to polish their web pages like an established company would.

Subjecting the root domain of the first URL (000webhostapp[.]com) to a subdomain finder search resulted in a list of more than 10,000 subdomains. Note that 000webhostapp[.]com is a domain provided by a free web hosting company. Users can add subdomains to that domain and host content, sometimes maliciously, as covered in this podcast.

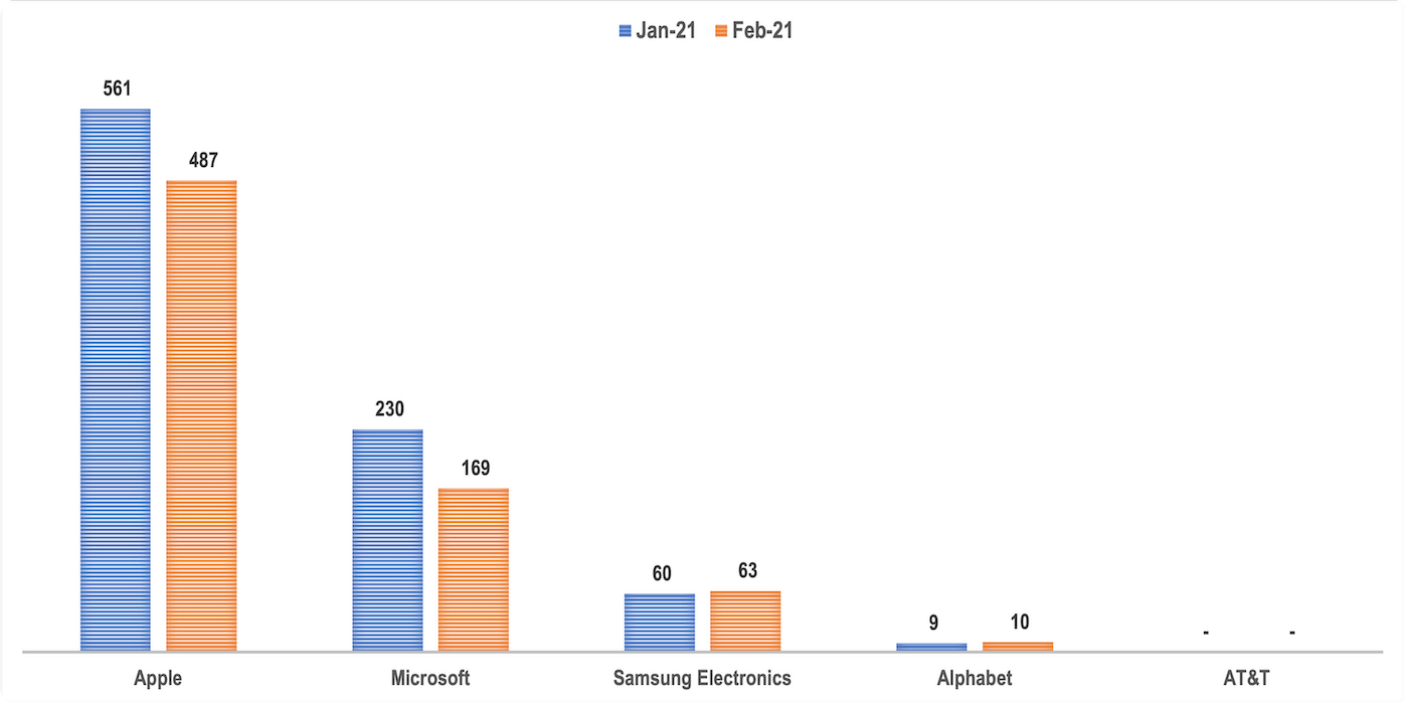
The subdomain scanner lookup for allgamescheaper[.]com, meanwhile, gave us 20 subdomains. Organizations may want to look into all of these for possible inclusion in their blacklists. That way, they can ensure protection against scams perpetrated by the same people behind the phishing attack.

Use #3: Brand Protection

One way to protect your business's reputation is to ensure that no malicious actor uses your brand and trademarks for phishing and other malware- and exploit-enabled attacks. A subdomain scanner can help with this cybersecurity strategy.

You can monitor subdomain data feeds daily, weekly, or monthly, for example, to determine how many subdomains contain your company or brand name and other trademarks to catch infringers.

We looked at how many subdomains contained the brand or company name of the top 5 digital companies (with the greatest digital footprints)—Apple, Microsoft, Samsung Electronics, Alphabet, and AT&T—according to Forbes. From there, we compared the number of subdomains that contained their company name to see brand protection trends aided by a subdomain enumeration tool. Note that the numbers in the chart below do not account for misspelled variations of the company names and all of their brands or products.



As the chart shows, we could say that the larger a company's digital presence is, the greater the number of subdomains may be preying on its popularity for cyberattacks. A downward trend in subdomain volume can be seen from the organization with the biggest presence (Apple) to that with the smallest digital footprint (AT&T).

Use #4: Vulnerability Scanning

As has been established earlier, subdomain scanners can help organizations identify possible attack entry points in the form of forgotten subdomains or those with dangling DNS records.

A DNS record that points to a subdomain that is not available is a dangling record. It should be removed from a company's DNS zone. If not, it can make a subdomain takeover possible.

A subdomain takeover occurs when attackers gain control over one of your subdomains. That is possible when that subdomain has a canonical name (CNAME) in the DNS but does not have a host that provides content for it. That can happen when a virtual host has not yet been published

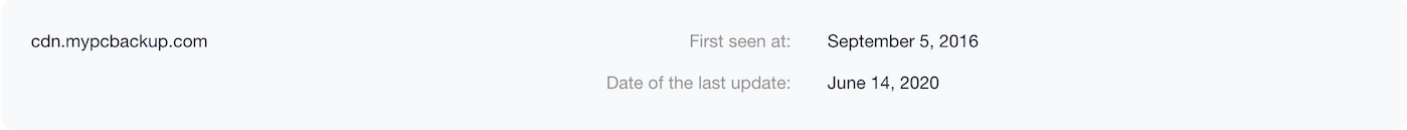
(the subdomain remains unused) or has been abandoned (the subdomain is no longer used but has been forgotten). The attackers can take over that subdomain by providing their own virtual host and hosting their own content for it.

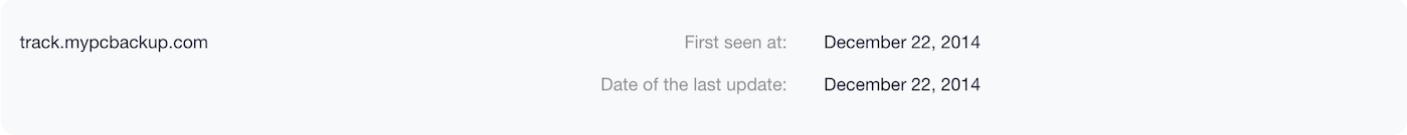
Let us take the domain mypcbackup[.]com as an example. It is non-malicious on its own, according to a VirusTotal report. A look at its website on Screenshot Lookup would tell users that it seems legitimate as well.

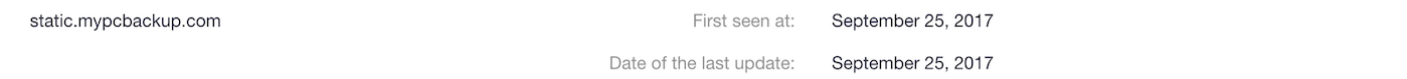
But further scrutiny using a subdomain finder revealed that it has 22 subdomains, three of which

(cdn[.]mypcbackup[.]com, track[.]mypcbackup[.]com, and static[.]mypcbackup[.]com) are dubbed malicious according to VirusTotal at the time of writing.

The subdomain enumeration search results also showed that all three malicious subdomains may have dangling DNS records since an update, which is the addition of a fresh passive DNS record, has not been recorded in months or even years. Cdn[.]mypcbackup[.]com was last updated on 14 June 2020, track[.]mypcbackup[.]com on 22 December 2014, and static[.]mypcbackup[.]com on 25 September 2017. If those subdomains still resolve to the DNS record actively and the company is legitimate, the organization would benefit from deleting them and their respective DNS records since associations with malicious web properties can negatively affect its search engine optimization (SEO) ranking, not to mention land it on a blocklist.







Subjecting the domain mypcbackup[.]com to a DNS lookup gave us the IP address

35[.]227[.]204[.]37, which is dubbed malicious on VirusTotal as well. The organization may also want to look into asking its Internet service provider (ISP) for help in taking its IP address off the blacklist. Purging its entire web infrastructure of the malicious subdomains identified above may help.

An additional reverse IP/DNS search using the IP address the domain resolves to also provided a list of three connected subdomains—37[.]204[.]227[.]35[.]bc[.]googleusercontent[.]com, mypcbackup-cc[.]com, and support[.]mypcbackup[.]com.

As we demonstrated in this post, subdomain scanners can be considered critical threat intelligence sources for a variety of cybersecurity purposes, including attack surface management, phishing and fraud detection, brand protection, and vulnerability scanning.