What Is Subdomain Takeover and How Does It Happen?

Posted on August 9, 2021

As an extension of a domain name, subdomains play an essential role in the Domain Name System (DNS). Some websites like Wikipedia offer content in different languages using them—en[.]wikipedia[.]org, es[.]wikipedia[.]org, and de[.]wikipedia[.]org, among many others.

Websites can also be segmented by category through subdomains, and sometimes point to third-party-hosted services. For instance, blog[.]example[.]com could contain content hosted by blogging platforms like WordPress, while shop[.]example[.]com could point to e-commerce platforms like Shopify.

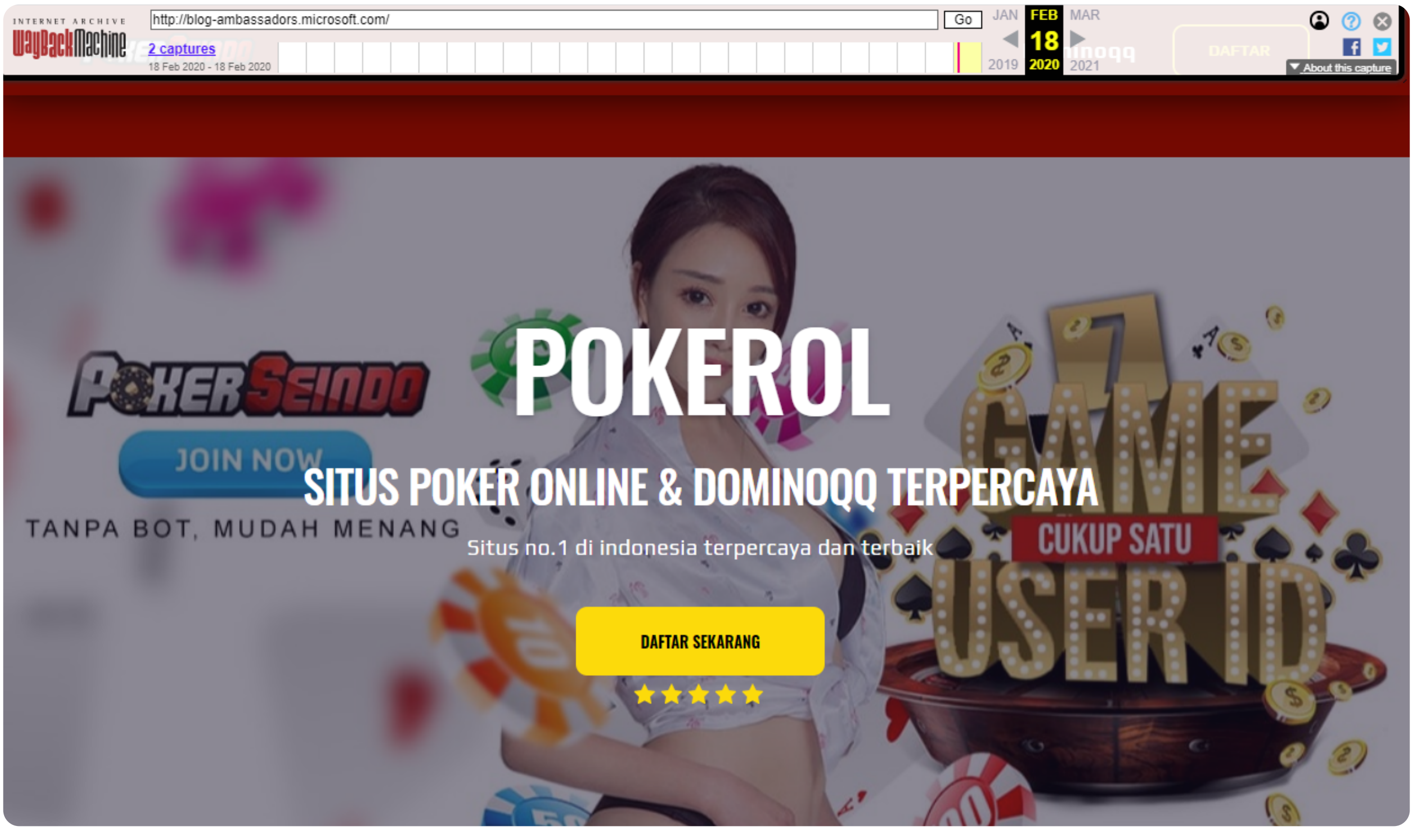
While these use cases are helpful and demonstrate the value of subdomains, threat actors can sometimes take control of them and pose threats to website owners and visitors alike. This post explains how, and tackles a specific threat called a “subdomain takeover.”

What Is a Subdomain Takeover?

A subdomain takeover is a form of cyber attack where threat actors take control of a target organization’s subdomain/s. Doing so notably allows the attackers to:

- Host malicious content on the subdomain/s
- Pretend to be part of the target organization
- Ask website visitors for sensitive information
- Collect and forge the target’s security certificate details

Subdomain takeover can happen in multiple contexts and sometimes involves big brands. For instance, the cybersecurity community saw takeovers happen for some of Microsoft’s subdomains. One of the hijacked subdomains (blog-ambassadors[.]microsoft[.]com) was seen hosting spam content, which a screen capture from Wayback Machine shows:

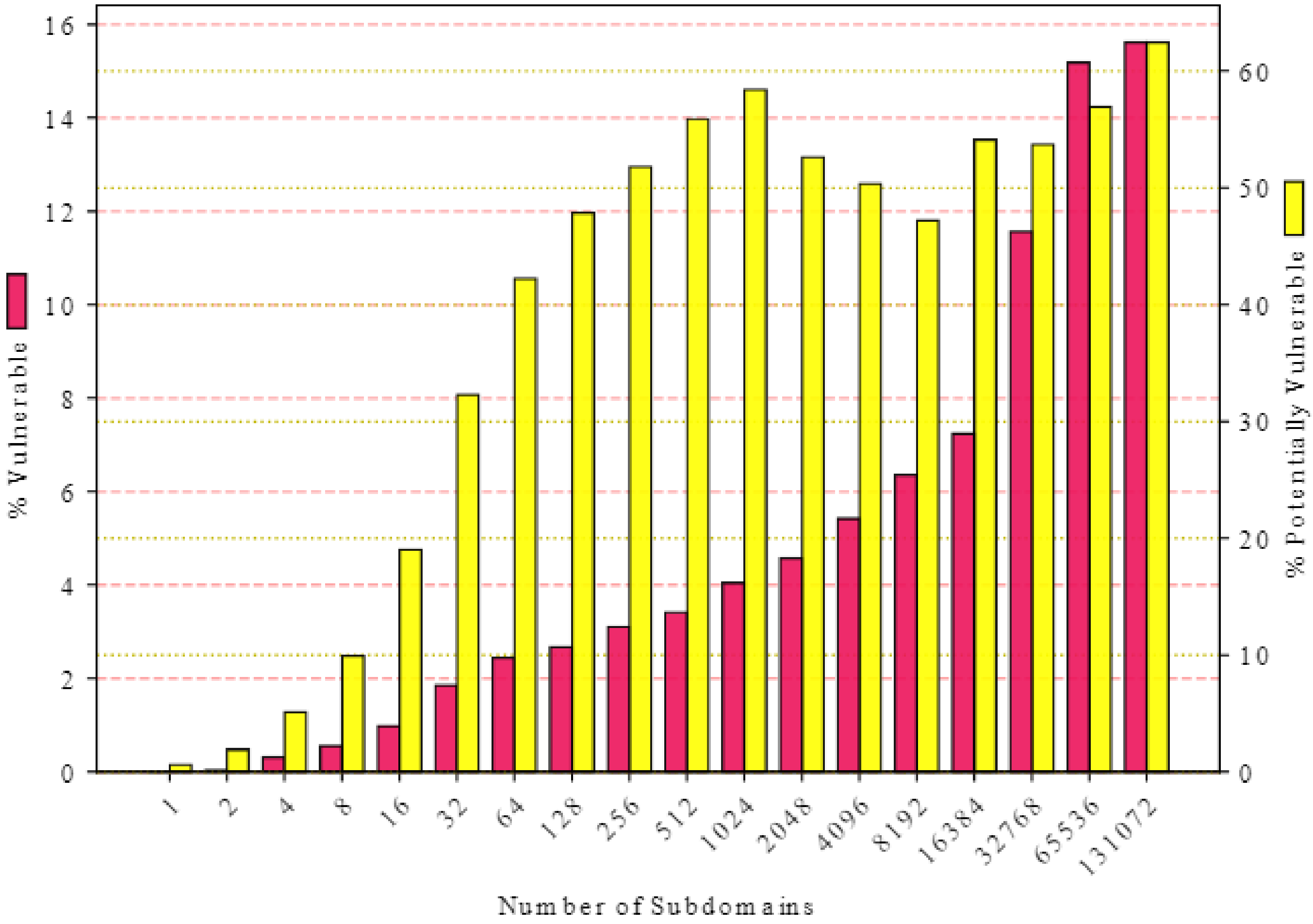


But with large organizations’ domains often having more than 10,000 subdomains, many other entities could have become the target of subdomain takeovers without their knowledge.

The study “Can I Take Your Subdomain? Exploring Same-Site Attacks in the Modern Web,” performed by Squarcina et al., and published here, found possible cases of subdomain takeovers. Among the issues that the researchers saw were site impersonation, session hijacking, and personally identifiable information (PII) leakage.

Subdomain Takeover Vulnerability: How Vulnerable Are You?

The study mentioned above involved a large-scale vulnerability assessment of the top 50,000 sites. The researchers found 1,520 vulnerable subdomains under 887 domain names. The study uncovered a correlation between a website’s susceptibility to subdomain takeovers and the size of its attack surface.



Screenshot of a chart as published on "Can I Take Your Subdomain?"

Simply put, the larger the attack surface, the more vulnerable an organization could be to subdomain takeover. Furthermore, the study found that high-ranking websites have more exploitable subdomains than those in lower positions.

Domains using the .edu top-level domain (TLD) have a higher percentage of vulnerable subdomains compared to other TLDs.

How Do Subdomain Takeovers Happen?

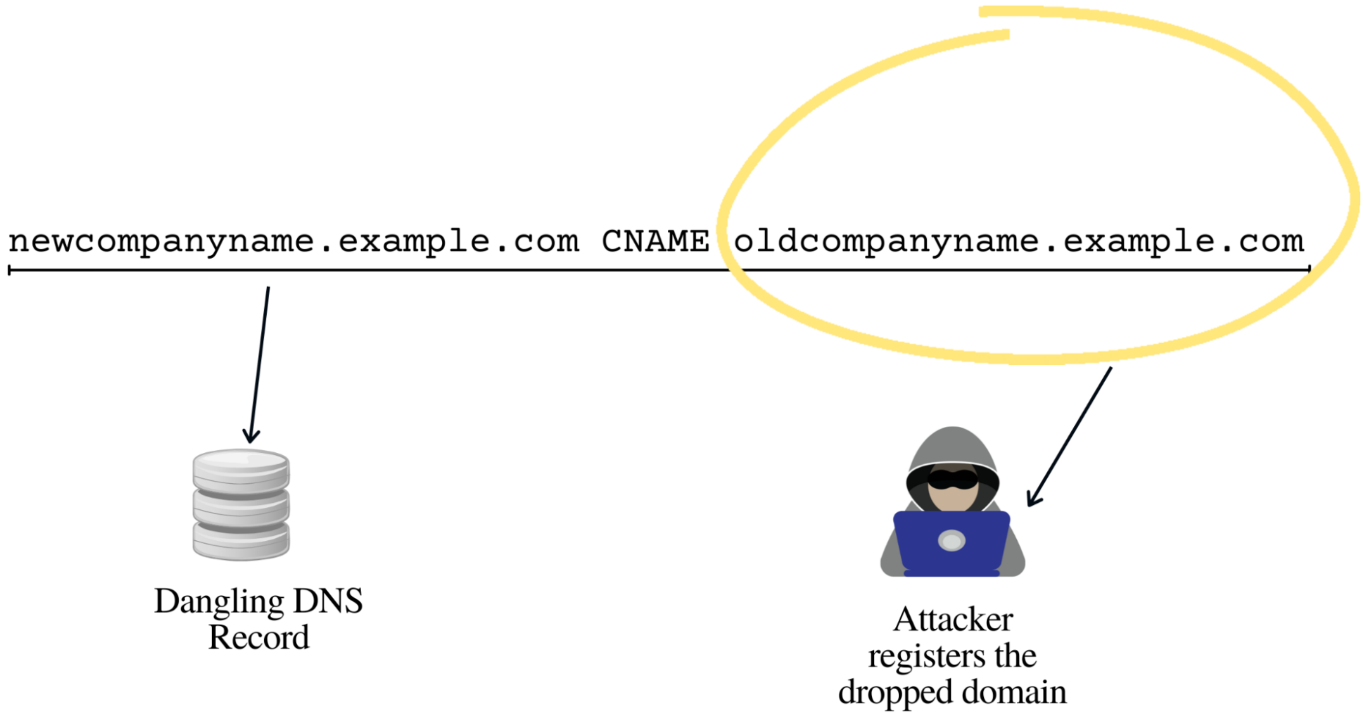
Subdomain takeovers become possible when DNS entries are left online, even when the subdomains they are for are no longer in use. In most cases, dangling DNS records are the most vulnerable to this type of attack.

Dangling DNS Records

Dangling DNS records point to unavailable but undeleted resources. Attackers may obtain access to these resources and control the subdomains they point to. To illustrate, consider this DNS record:

newcompanyname.example.com CNAME oldcompanyname.example.com

This canonical name (CNAME) record allows users to use newcompanyname[.]example[.]com to access the organization's original website. When the website administrator fails or decides not to renew oldcompanyname[.]example[.]com for some reason, its CNAME record should also be updated.


newcompanyname.example.com CNAME oldcompanyname.example.com
Dangling DNS Record
Attacker registers the dropped domain

Failure to do so would make the CNAME record a dangling DNS record since it points to a nonexistent DNS resource. Attackers can register oldcompanyname[.]example[.]com and essentially control what visitors see when visiting newcompanyname[.]example[.]com.

Dangling DNS records can be seen due to several reasons, including the deprovisioning of cloud instances and discontinuation of some services. Squarcina et al., cited that 83% of the vulnerabilities they found during a study are caused by discontinued third-party services, and 17% of them are due to expired domains.

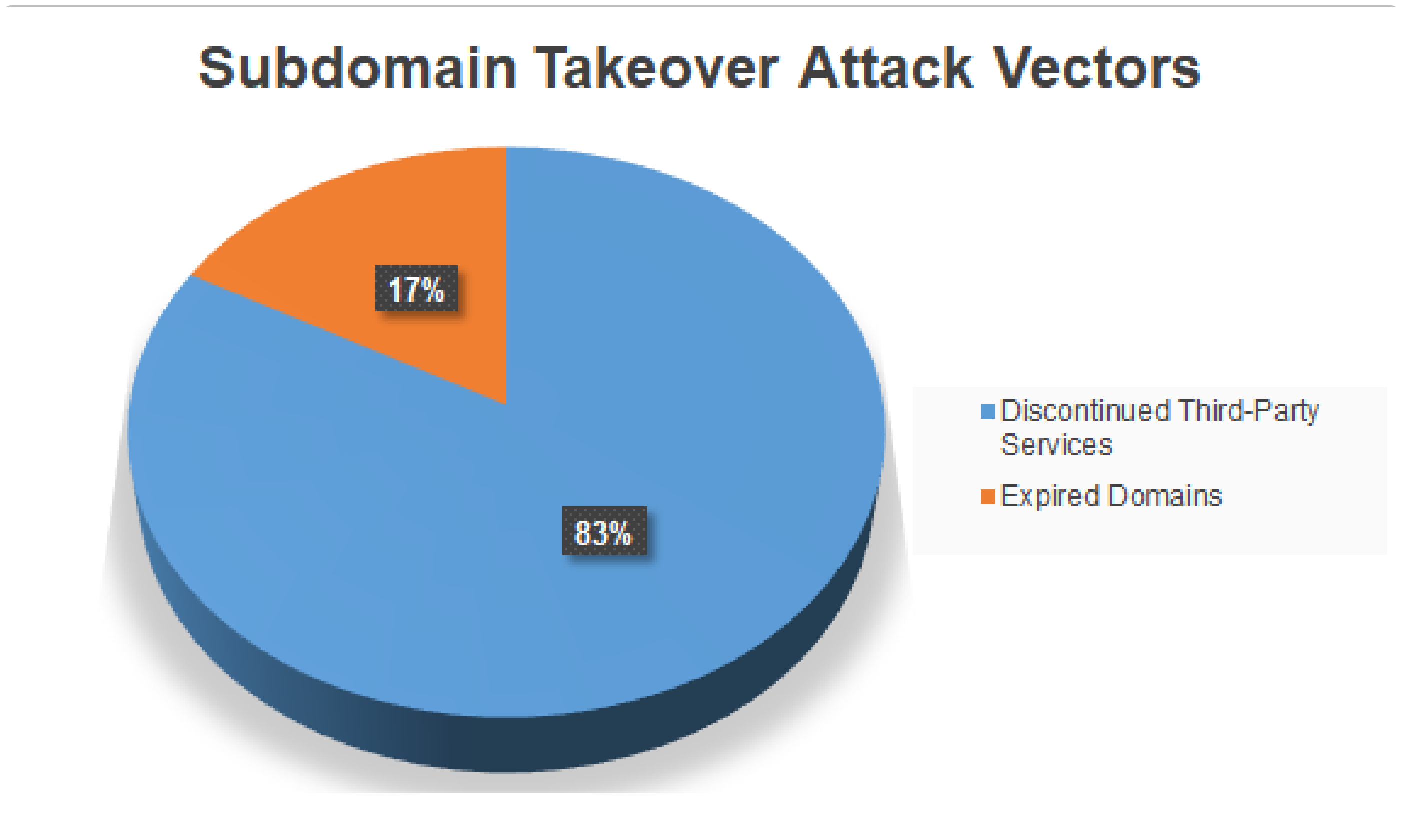


Image based on the findings of "Can I Take Your Subdomain?"

Deprovisioning Cloud Instances

The ballooning number of dangling DNS records could be attributed to how cloud services are provided. When an organization moves from one cloud service provider to another, subdomains pointing to cloud instances could get left behind. For example, a subdomain could point to an IP address in this DNS record:

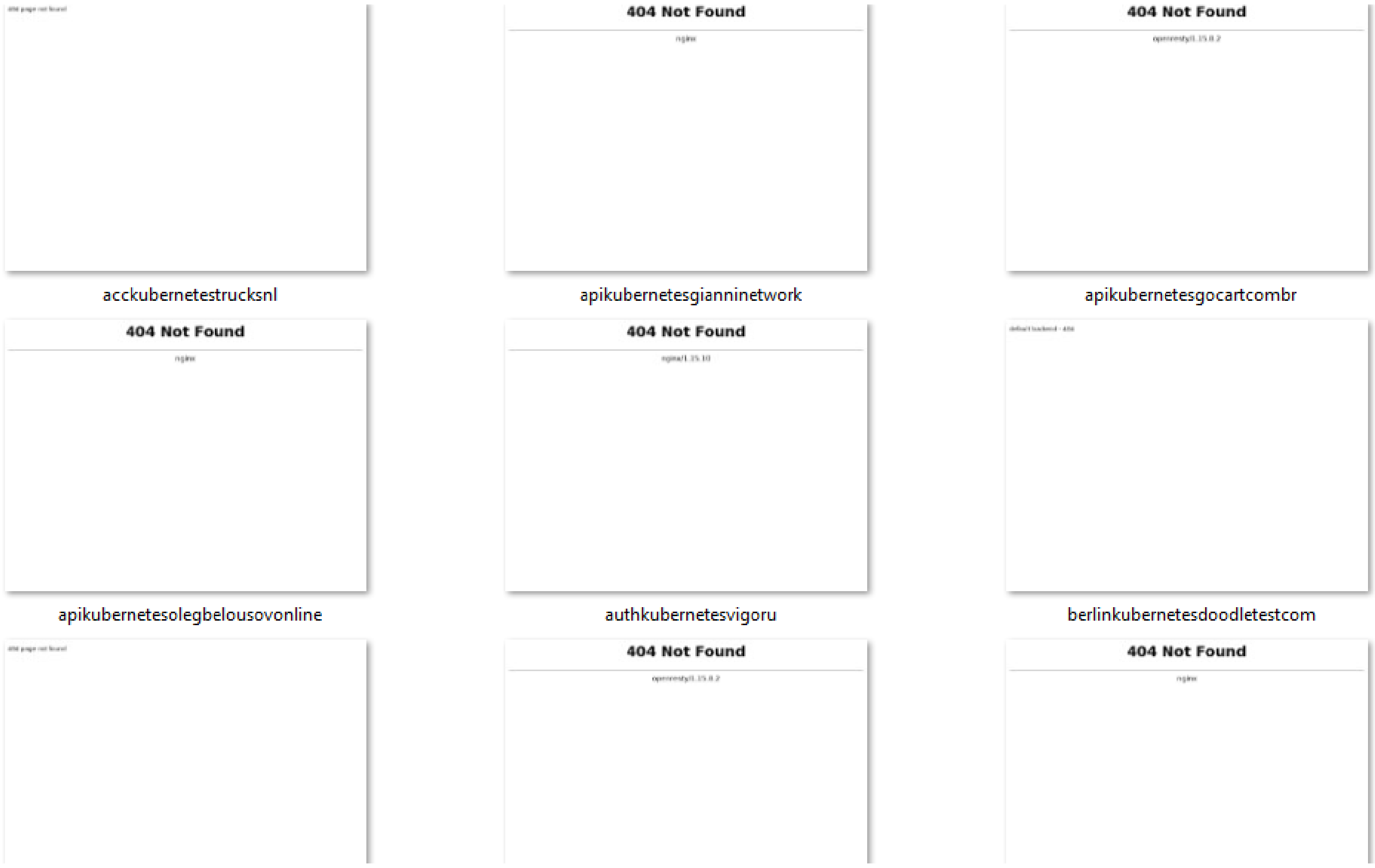
cloud.yourcompany.com A 1.1.1.1

When an organization decides to switch providers, it could deprovision the first cloud instance and create a new subdomain pointing to an IP address given by the new cloud provider:

newcloud.yourcompany.com A 2.2.2.2

While the first provider's IP address is returned to the IP pool, the A record that points to it could remain in the zone file. With this setup, threat actors can attempt to take control of the subdomain.

In many cases, the first thing that threat actors need to do is look for subdomains that point to 404 pages. A study that focused on descriptive subdomains, for one, revealed several Kubernetes subdomains that point to 404 pages.



404 page not found

acckubernetestrucksnl

404 Not Found

nginx

apikubernetesgianninetwork

404 Not Found

openresty/1.15.8.2

apikubernetesgocartcombr

404 Not Found

nginx

apikubernetesolegbelousovonline

404 Not Found

nginx/1.15.10

authkubernetesvigoru

default backend - 404

berlinkubernetesdoodletestcom

404 page not found

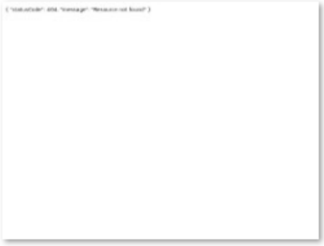
404 Not Found

openresty/1.15.8.2

404 Not Found

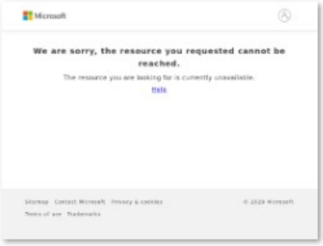
nginx

404 page occurrences can also exist among big brands. For instance, a look at a 1,000 Microsoft subdomains sample using Screenshot API showed that only about 4.6% of the sample were active, several of which resolved to 404 pages or unavailable resources.



{ "statusCode": 404, "message": "Resource not found" }

[redacted]microsoftcom



Microsoft

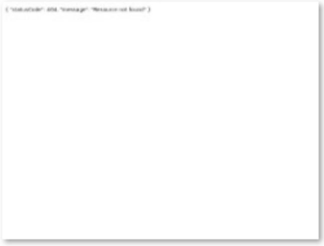
We are sorry, the resource you requested cannot be reached.

The resource you are looking for is currently unavailable.

Help

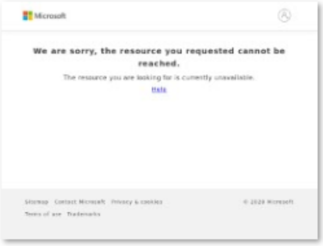
Sitemap Contact Microsoft Privacy & cookies Terms of use Trademarks © 2020 Microsoft

[redacted]microsoftcom



{ "statusCode": 404, "message": "Resource not found" }

[redacted]microsoftcom



Microsoft

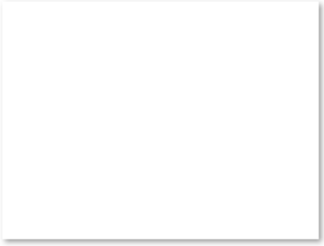
We are sorry, the resource you requested cannot be reached.

The resource you are looking for is currently unavailable.

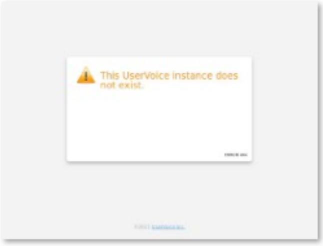
Help

Sitemap Contact Microsoft Privacy & cookies Terms of use Trademarks © 2020 Microsoft

[redacted]microsoftcom

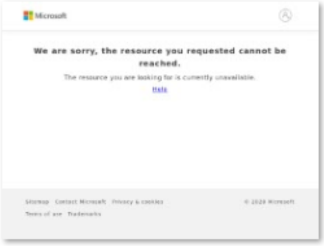


[redacted]microsoftcom



This UserVoice instance does not exist.

[redacted]microsoftcom



Microsoft

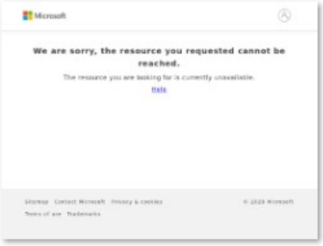
We are sorry, the resource you requested cannot be reached.

The resource you are looking for is currently unavailable.

Help

Sitemap Contact Microsoft Privacy & cookies Terms of use Trademarks © 2020 Microsoft

[redacted]microsoftcom



Microsoft

We are sorry, the resource you requested cannot be reached.

The resource you are looking for is currently unavailable.

Help

Sitemap Contact Microsoft Privacy & cookies Terms of use Trademarks © 2020 Microsoft

[redacted]microsoftcom

Discontinuation of Third-Party Services

Changing third-party providers could also result in dangling DNS records. As previously mentioned, subdomains can be used to point users to certain services. When these services are no longer used, some subdomains remain in the organization’s zone files. Attackers can try to sign up with the third-party provider using the subdomain.

Take, for example, the CNAME record that points a subdomain for your blog to your WordPress account. The record can look like this:

blog.yourwebsite.com CNAME yourwebsite.wordpress.com

Later on, you may decide to use subfolders instead and stop using WordPress as a blogging platform. Website visitors can then access your blog page through yourwebsite[.]com/blog instead of the blog subdomain. The CNAME record above, if not removed from your zone file, becomes a dangling DNS record.

Visitors that type blog[.]yourwebsite[.]com would be greeted by a nonexistent page. The same thing could send a signal to attackers that the subdomain is vulnerable. If you deleted your WordPress account, threat actors can sign up using your username and control what people see on blog[.]yourwebsite[.]com.

The “Can I Take Your Subdomain?” study cited discontinued services as a prevalent subdomain takeover vector. WordPress topped the list, followed by Shopify, Tumblr, and GitHub, among others.

Subdomain takeover is a real and present threat, as attackers can redirect victims to pages that host malicious content. In turn, it could result in session hijacking and site impersonation, among other things. Worse, threat actors can use subdomain takeover as a means to steal PII by enticing users to key in their sensitive data.

The research mentioned in this blog post showed that discontinued third-party services can make subdomains more vulnerable to takeover. Deprovisioned cloud instances can further increase the possibility of such attacks. Organizations can help prevent subdomain takeovers by ensuring that DNS records are updated, especially when switching from one third-party provider to another.

More importantly, we can establish that the larger the attack surface, the more vulnerable an organization is to subdomain takeovers. From a brand protection and cybersecurity perspective, one of the crucial steps toward subdomain takeover protection is domain attack surface discovery—which can be done using Domains & Subdomains Discovery.