REN-ISAC

ADVISORY: Subdomain Takeover
Sharing Guideline: PUBLIC (TLP:WHITE)

If you receive a REN-ISAC alert or have other reasons to suspect that your organization may be impacted by a subdomain takeover attack, take the following four steps.

1. Understand

REN-ISAC defines Subdomain Takeover as the following:

> Subdomain takeover involves external hosting and an old DNS entry. It is made possible when an organization sets up a server hosted in a cloud environment (e.g. AWS, Azure, etc.), creates a DNS entry to point to that server's (externally-hosted) DNS name or IP address, and then later decommissions the service but does not remove the DNS entry.
>
> An ill-intentioned third party discovers this stale DNS record and re-establishes a server in that cloud environment answering under the original server's DNS name or IP, the same one to which the hanging DNS entry still points. The solution is to remove any unused DNS entries, severing the relationship with the third-party server.

The threat actor's web server is used to serve spam and may redirect visitors to other websites as well. As you investigate, please heed this advice:

> Sites fronted by subdomain takeover are often used for SEO purposes and may contain sensitive, adult, and/or malicious content; please practice adequate sandboxing, privacy, and anonymity precautions when investigating an attack.

Virtual machines/sandboxes, proxies/VPNs/Tor, plug-ins such as NoScript, curl/wget, etc. are all tools that should be in your incident response toolkit. It is not advisable to browse the suspected site with your device's regular web browser.

2. Record and Verify

Gather DNS information about the hostname and determine that you no longer have control over the target resource.

Use `nslookup`, `host`, `dig`, etc. to note targets of the hostname's DNS resolution. For example, assume you work at *foo.edu* and suspect *host1.foo.edu* and *host2.foo.edu* as targets of subdomain takeover. Their DNS resolutions might look like the following:

```
host1.foo.edu is an alias for heiue-3489sdk-34kcuwz.cloudapp.net.
heiue-3489sdk-34kcuwz.cloudapp.net has address 51.137.71.32

host2.foo.edu is an alias for mig-test-2534.azurewebsites.net.
mig-test-2534.azurewebsites.net is an alias for blue7-testrig-
7873.sip.azurewebsites.windows.net.
blue7-testrig-7873.sip.azurewebsites.windows.net is an alias for blue7-
testrig-7873.cloudapp.net.
blue7-testrig-7873.cloudapp.net has address 40.71.10.23
```

For both hosts, you should record all the hostnames involved and then verify that your organization no longer has control over the referenced resources. In the examples above, that would mean verifying that *heiue-3489sdk-34kcuwz.cloudapp.net* and *im-migration-test-2534.azurewebsites.net* are not defined in (any of) your organization's Azure subscriptions.

If you find that you do still have control over the target resource in question and were alerted to potential subdomain takeover by REN-ISAC, please respond to the alert email and let REN-ISAC know that there is no subdomain takeover even if the site may be hosting webspam pages.

3. Report the Abuse

Report the subdomain takeover to the applicable cloud provider.

For example, use the following forms to report takeovers and other abuse to AWS, Azure, Linode, or Digital Ocean.

Make sure your report includes all the DNS information you recorded in step #2. Feel free to attach or include any alert text from REN-ISAC as well.

4. Mitigation

What action you take next depends on your organization's stance, policies, or guidelines around search engine rankings and search results.

If the speed at which spam URLS are removed from a search engine's cache is unimportant, you only need to delete any dangling DNS entries under your organization's control. In the example above, that would mean deleting the DNS entries of *host1.foo.edu* and *host2.foo.edu.* It may take months for your site's entries to disappear from Google searches and caches, but your work is done.

Otherwise, you will need to take the following actions **instead of** deleting the DNS entries:

A) Set up a controlled web server and target any DNS entries to that new host. Configure it to return for all requests either HTTP 404 (Not Found) or HTTP 410 (Gone) return codes. There is some debate online as to whether 410's result in faster removal from search engines indexes than 404's[i], but either will work. This has the added benefit of allowing you to further monitor the web server logs for visits to the sites by crawlers, malicious actors, and others.

B) For removal from Google search results, first claim ownership of the site in the Google Search Console. This requires either creating additional DNS entries or new files on the web server you set up in the previous set. Once completed, follow these instructions to use GSC's Removals Tool to temporarily remove all the search results from your compromised hostname.

Once Google re-crawls all its entries from your site (now with 404 or 410 responses), the search results from your hostname should be permanently removed from its index.

[i] 410 vs 404 from Google Webmaster, "Google Offers Advice on 404 and 410 Status Codes" from Search Engine Journal

C) If your site has entries in Bing and you wish to expedite their removal, you will need to claim the site in Bing's webmaster tools and then follow the instructions for the content removal tool.

Detecting/Preventing Subdomain Takeovers

If you received an alert from REN-ISAC, the report was generated by a system that searches for websites hosting webspam pages. If you are wondering if you are vulnerable to additional future takeover attacks; or are currently the victim of other subdomain takeover attacks that don't use the end resource to host spam, and your organization lacks strong DNS governance or auditing controls, the following two periodic tasks may prove helpful:

1. Collect and resolve all your organization's hostnames in your domain's DNS servers. Look for CNAME or A records that point to external hostnames or IPs, paying particular attention to those that resolve to domains or IP addresses that belong to cloud providers such as Azure, AWS, Digital Ocean, Linode, etc.

2. Audit those entries to verify that they point to resources that your organization has either direct control over or a relationship with (a SaaS provider, for example). This can be difficult if your organization's IT infrastructure is large and/or decentralized.

3. Consider claiming your top-level domain (TLD) in the Google Search Console which will facilitate Google notifying you directly when Google crawlers find spam on sites within your domain.

Resource List

AWS report address:
https://support.aws.amazon.com/#/contacts/report-abuse

Azure report address:
https://portal.msrc.microsoft.com/en-us/engage/cars

Bing webmaster tools:
https://www.bing.com/toolbox/webmaster/

Bing content removal tool:
https://www.bing.com/webmaster/help/bing-content-removal-tool-cb6c294d

Google Search Console:
https://search.google.com/search-console/about

GSC Removal Tool Instructions:
https://support.google.com/webmasters/answer/9689846

Acknowledgments: Adam Arrowood, Georgia Tech