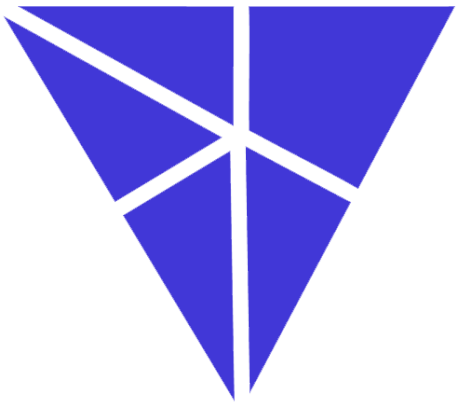

Squarespace Security Advisory

July 12, 2024

samczsun, tayvano, AndrewMohawk

Version 1.1 - July 15, 2024
Version 1.0 - July 12, 2024

Background

On September 7, 2023, Squarespace acquired all domain registration data and customers from Google Domains. Per the agreement, customers would be migrated from Google Domains to Squarespace over an unspecified transition period [1].

On or around July 9, 2024, an unknown threat actor began compromising multiple domain names registered with Squarespace. All affected domains were transferred into Squarespace as part of the migration.

Squarespace has yet to release an official statement or postmortem but at this stage, based on the number of impacted projects, we do not believe that this was caused by user negligence such as reusing weak passwords or not enabling MFA

Methodology

Initial Access

During the migration process from Google Domains to Squarespace, the following emails were granted administrative access over domains [1]:

- The email address associated with the Google Domains account where the domain was managed
- Any contributor email addresses associated with the domain [2]

It appears that Squarespace implemented this by pre-linking all emails to domains, regardless of whether the account already exists, likely because they wanted users to be able to OAuth with Google and immediately have access to all their domains. However, because Squarespace also does not require email validation to create an account using password authentication (i.e. you can create an account for bill@gates.com without owning the email address), the threat actor simply created accounts with all potential emails that might be migrated with a domain but had yet to be registered. Once the threat actor found a valid email, they had full access to the associated domains without having to verify the email address.

Privilege Escalation

Once the threat actor has administrative or management access to the domain in Squarespace, they typically proceed to take over as much control as possible. This typically begins with taking over DNS records, either by changing the nameservers

to ones that they control, or by editing the DNS records in Squarespace directly. When editing DNS records, the threat actor both changes the A records in order to hijack the domain content, as well as the MX records in order to intercept future emails. This also allows the threat actor to perform password resets on accounts with a branded email in order to escalate their access.

Squarespace is a Google Workspace reseller and during migration if your Google workspace was purchased from Google Domains (also a Google Workspace reseller), this is transferred over to Squarespace. This gives Squarespace account managers and administrators the ability to add new Google Workspace administrators, even if they themselves were not a Google Workspace administrator.

The threat actor leverages this to escalate access within the Google Workspace tenant. If no Google Workspace tenant is linked, then the threat actor may additionally create a new Google Workspace tenant associated with the domain.

From Google Workspace administration, threat actors were able to add new accounts, devices and browsers as well as sync data and access previous historical services such as email and view authorized SaaS products. Additionally they added footholds into the Workspace via OAuth Applications and disabling strong authentication across accounts.

Recommendations

Log in and enable 2FA on Squarespace

If you have never logged in to Squarespace, your account will not have 2FA enabled. If you previously had a Squarespace account, your 2FA may have been automatically disabled. Log into Squarespace, create a new password, and enable 2FA for all Squarespace accounts which can administer domains.

Remove excess contributor accounts from Squarespace

Auto-created contributor accounts pose an unnecessary risk to your domain. Log in with the primary domain owner and remove access to your domain from any contributors which no longer need access.

Remove reseller access from Squarespace on Google Workspace

Google Workspace licenses which were purchased from Google Domains were transferred to Squarespace, which is then able to create admin users. To be safe, disable reseller access to your Workspace tenant by following these instructions.

Revert all changes in Google Workspace

Review all of the admin and user logs in Google Workspace to identify any changes made and revert and revoke access where needed. Validate there are no new devices or browsers and where possible remotely wipe these devices

Revert all changes to DNS records

Double check the nameservers that the domain is configured to use and ensure all DNS records are correct. The threat actors have been known to appear to revert all changes to mask a single extra DNS record.

Check additional settings for anything unexpected or unnecessary

It's possible that the threat actor configured additional settings for your domain. Check all the settings and if you aren't using it or don't recognize it, remove it.

Transfer domains to a different registrar

If you use Squarespace as your primary domain registrar, consider transferring your domain to one of the following when you are able to:

- Cloudflare Registrar
- Amazon Route53
- dnsimple
- MarkMonitor
- CSC

Indicators of Compromise

DNS

The threat actor has been known to use the following IP addresses in A records:

- 185[.]196[.]9[.]29

The threat actor has been known to use Zoho to intercept emails for a hijacked domain:

- mx[.]zoho[.]eu
- mx2[.]zoho[.]eu
- mx3[.]zoho[.]eu

Email Addresses

The threat actor used the email address steve@fear.pw as well as other anonymized mail providers

Devices

The threat actor was seen adding the following devices to Google Workspace:

- Asus ROG Phone 5 (Android)
- Asus ROG Pc (Windows)

Emails

If the threat actor was able to create a new Google Workspace for a domain
From: `no-reply@squarespace.com`
Subject: `Welcome to Google Workspace`

If the threat actor unlinked the new Google Workspace from the domain in order to maintain control over it
From: `no-reply@squarespace.com`
Subject: `Your Google Workspace account is canceled`

If the threat actor was unable to create a new Google Workspace for a domain because one already exists
From: `no-reply@squarespace.com`
Subject: `Couldn't connect Google Workspace to your domain`

Google Workspace

Use Investigation Tool to check the following:

- Log Source: `Admin log events`
  Actor: `wksp-svc-resell-prod-001@reseller.squarespaceapps.com`

References

[1] https://support.squarespace.com/hc/en-us/articles/17131164996365-About-the-Google-Domains-migration-to-Squarespace
[2] https://support.google.com/domains/answer/7179397?hl=en

Appendix

pendle.finance domain monitoring script

https://gist.github.com/UncleGrandpa925/a6e682e1a2674054cd58845b7d07dad1

Crypto domains migrated to Squarespace

https://gist.github.com/AndrewMohawk/dc25cab889ec4b874acbe85ddd0f009e

Drainer

Hostname: `compound-finance[.]app`, `v2-pendle[.]finance`
C2: `checker-api[.]su`