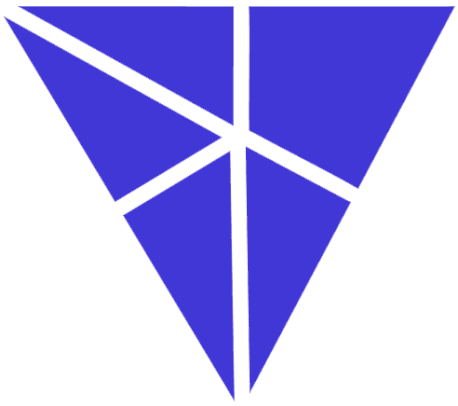
TLP:CLEAR - PUBLIC DISCLOSURE



Squarespace Security Advisory

July 12, 2024

samczsun, tayvano, AndrewMohawk

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 10, 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.

Methodology

Initial Access

It is currently unclear how threat actors are accessing Squarespace accounts, although we suspect the following potential explanations.

During the migration process from Google Domains to Squarespace, the following accounts were automatically created for each domain [1]:

- The email address associated with the Google Domains account where you managed the domain
- Any contributor email addresses associated with the domain
- The email addresses listed as the Admin, Tech, and Billing contacts on the domain

If any of these emails owned a Squarespace account prior to the migration, attackers may be able to access them via leaked passwords, re-used passwords or other means.

There may also be some other vulnerability which allows the threat actor to take over Squarespace accounts, although if such a vulnerability exists, it may be limited to only accounts which were automatically created during the migration process.

Finally, the threat actor may have social engineered a support employee, or otherwise gained insider access to Squarespace systems.

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 likely to have transferred over to squarespace. This gives Squarespace account administrators the ability to add new Google Workspace administrators, even if the same email address is not itself a Google Workspace administrator via the reseller service account. 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 create a new Google Workspace tenant associated with the domain.

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 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.

Remove all unnecessary owners/admins from the account

Anyone not actively managing the domain should be removed from the Squarespace account, especially those with email addresses that are not being used / monitored regularly.

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
- 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

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 GoogleWorkspace 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

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`