Orbitera Subdomain Takeover

ADVISORY SUMMARY

Title: Subdomain Takeover of '***blog.orbitera.com***'

Impact: Subdomain Takeover

Vendor: Orbitera

Researcher: Mayank Kapoor (HoF)

Identifiers: https://issuetracker.google.com/issues/74041516

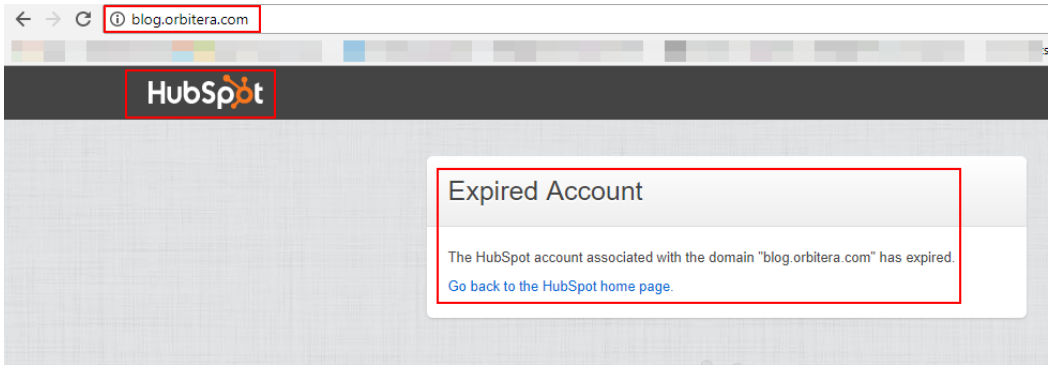
Timeline: March 1st, 2018: Issue disclosed to Google
March 7th, 2018: Issue and reproduction confirmed by Google
May 24th, 2018: Issue Marked as Fixed

TECHNICAL DETAIL

DESCRIPTION

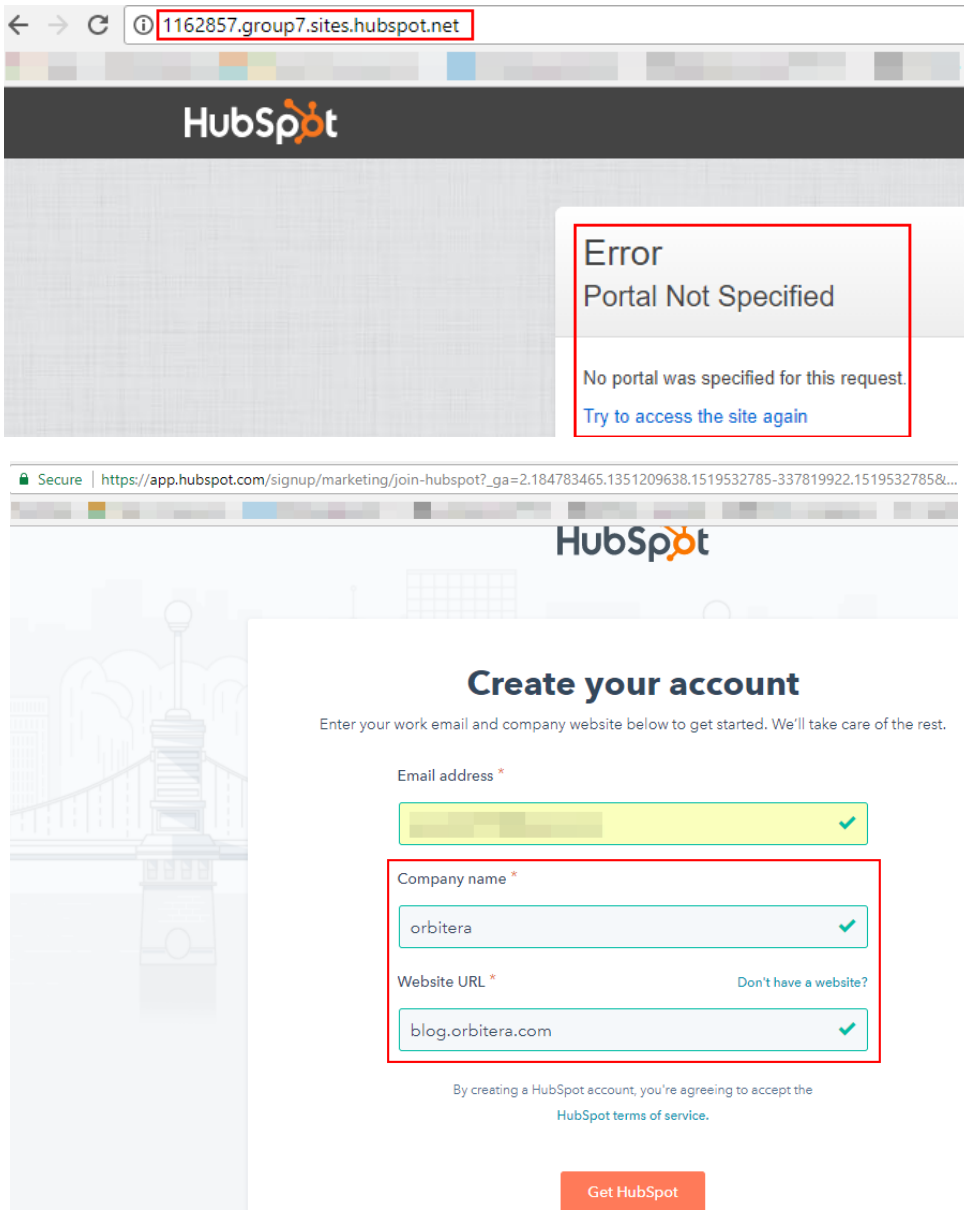
Subdomain takeover occurs when a subdomain points to a deleted or expired third party service allowing the attacker to register using the expired subdomain and claim the ownership. This vulnerability generally occurs when someone forgets to remove the CNAME entry point of the website.

The CNAME of '*blog.orbitera.com*' was pointing to an external service i.e. HubSpot. Adding to the above, the webpage discloses that the account has been expired, indicating that "blog.orbitera.com" can be claimed by registering on hubspot.com using the expired domain.




```
# host blog.orbitera.com
blog.orbitera.com is an alias for 1162857.group7.sites.hubspot.net
1162857.group7.sites.hubspot.net is an alias for group7.sites.hscoscdn00.net
group7.sites.hscoscdn00.net has address 104.17.136.180
```

```
;; ANSWER SECTION:
blog.orbitera.com.      5       IN      CNAME   1162857.group7.sites.hubspot.net
```



IMPACT

Once claimed, attackers can serve malicious content on the acquired subdomain, which can cause an impact on the business. It also helps in generating foolproof phishing attacks.

RECOMMENDATIONS

It is recommended to remove the DNS-entry for expired subdomains pointing to external services.