Attack Scenario

* Your company starts using a new service, eg an external Support Ticketing-service.
* Your company points a subdomain to the Support Ticketing-service, eg support.your-domain.com
* Your company stops using this service but does not remove the subdomain redirection pointing to the ticketing system.
* Attacker signs up for the Service and claims the domain as theirs. No verification is done by the Service Provider, and the DNS-setup is already correctly setup.
* Attacker can now build a complete clone of the real site, add a login form, redirect the user, steal credentials (e.g. admin accounts), cookies and/or completely destroy business credibility for your company.

**Three things that make this scenario dangerous**

* It’s SUPER easy. Sign up for a new account and claim the domain. Done.
* It’s completely hidden. The Domain Owner won’t notice. The attacker won’t leave any traces for the Domain Owner. Good luck monitoring this in an IDS!
* The Service Provider is unlikely to be able to fix this in a feasible way.

INSTALLATION:

Go to <https://github.com/nahamsec/HostileSubBruteforcer>

Download HostileSubBruteforcer

Unzip HostileSubBruteforcer

Now, run it and give the domain which you want