Domain(s) strategy

Targets

What we want our phishing domains to look like:

- 1 ad hock organizations: to look like the company we are providing the service for (attacking) or a parner/provider of said company. Soft requirement: email signature/footer/pictures
- 2 general email provider: to look like a personal email, e.g. X asks Y to give him access
- 3 tool lookalike (github, sendgrid, etc.): to look like tools used internally by the target. Hard requirement: knowing the tools used by the target

Any domain which we expect to use as an email inbox (meaning: to receive emails, be it from phishing replies or other means) will lead to more overhead given that we'll need a real email provider backing the email, or to set up our own email server (costly). A

cheap alternative but likely caveat-y in the long run is a sengrid inbound parse webhook, i.e. a webhook that gets triggered when an email is received

Scalability

Categories 2-3 scale across multiple customers. Category 1 needs to be ad hoc for a customer, subdomains (<target>.molesec.com) can make this more viable but automatizing the setup gets increasingly costly and/or async:

- for example, if we add a new DNS record programmatically (assuming it's possible), we'd still have to wait for DNS propagation
- setting up a given subdomain as a sender identity or as an email inbox might only be partially automatable or might need to wait for DNS propagation

Categories 2-3 can be setup through simple (but reusable) scripts or manually. Category 1 might need automation from the start

TODO: verify to what extent the two aforementioned points are automatable

High-level implementations:

- domain lookalike for links: point the domain to the attack service, so that github.com/phishing-token/<token> gets sent to the attack service
- email outbox: through sendgrid
- email inbox: short term: sengrid inbound parse webhook, long term we might need a real email provider

Domain (and email) health

Over time our domains might suffer "reputation" degradation due to emails not being opened, being marked as spam or phishing, and so on. This might:

- affect the real molesec account (in a provider like sengrid) or email deliverability → use a separate account?
- lead to the necessity of periodically cycling our fake domains or trying to improve their reputation

google postmaster and microsoft sdns can help in checking the reputation status of an email

Would be super nice to be able to automate the check to get a message in case some domain reputation is getting bad

Axes of variations

These are (some of) the ways that we can use to make our domains look like target ones. Mix and match.

- top level domain: io/org/com etc.
- misspellings: github -> gethub
- acronyms: github -> ghub
- departments: github-marketing.com
- industry-related term: github-actions.com
- subdomains:
  target company subdomain: company.com -> company.mlsec.com
  department: company.com -> company.marketing.molesec.com
  location: company.com -> company.eu.molesec.com
  etc.

Legal risks

Legal implications of purchasing domains similar to popular tools?

[link] “If your choice of domain name is so similar to another company’s domain name, or other trademark or service mark, that it is likely to cause confusion among consumers and your company may be subject to allegations of trademark infringement.”

[link] “However, there are some potential legal issues that can arise when buying a domain name that is similar to an existing company's name or trademark. For example, if the domain name is being used to mislead consumers into thinking they are visiting the company's official website”

Where to buy the domain

route53? I’m sure it allows a decent degree of automation. We can then use cloudflare to point things around (?)

Other notes

- labels must follow the rules for ARPANET host names. They must start with a letter, end with a letter or digit, and have as interior characters only letters, digits, and hyphen. There are also some restrictions on the length. Labels must be 63 characters or less. https://www.rfc-editor.org/rfc/rfc1035#section-2.3.4
- sendgrid identities (verify and setup sender identities)
- SPF, DKIM, DMARC (email auth/signing/security)SPF, DKIM, DMARC (email auth/signing/security)
- google postmaster and microsoft sdns can help in checking the reputation status of an email

Open questions

To which extent can we automate:

- domain registration
- DNS changes
- email sender identity
- email domain verification

Proposal

Actionables

Do not go with any ad hoc company names (category 1)

Do not test automating domain registration or DNS changes (only needed for category 1)

Do the domain reputation check but *later*

Test using different email sender identities with domain verification through a single sendgrid account

Test receiving emails as a webhook through sengrid inbound parse webhooks

Register a separate sengrid account to keep the orchest/molesec one separate from the phishing one (will require some work in the attack service if it needs to send both legit emails to us as molesec and phishing emails to users)

Do have a document that explains the steps from buying a domain to using it in the attack service

Domains to buy

Verify availability and reasonable price of domains with https://www.namecheap.com/domains/registration/results/

I don’t think it’s worth looking too much into these, once we start phishing for real we might have a better understanding of what works and what doens’t

General email provider sounding domains (verified availability):

- eu-inbox.com
- mailpilot.eu
- proto-mail.com

Example emails we would send from these domains:

- “hey X, it’s Y, I can’t access my work email, could you do Z”?

For email providers, it might be worth setting up a simple webflow page to look like a real email provider, so that we pass the quick lookup on google test

Legit sounding domains (not third party tools lookalike)

- data-code-action.com
- codegrid.ai (pricey, 70 bucks)
- code-actions.com
- zoauth.com
- qaoauth.com
- zauth0.com

Legit sounding domains (third-party tools lookalike)

- github-actions.com
- github-code.com
- gitlab-ci-cd.com

- sendgrid-mail.com
- stackoverflow-qa.com

Resolution

We decided to go with:

- 1 gmail account
- 3 custom domains