The DNS Abuse Institute

GAC Capacity Building: What Does DNS Abuse Look Like?

DNS ABUSE INSTITUTE

DNS Abuse

What is it*, and what does it look like?

- Phishing
- Malware
- Spam
- Botnet Command and Control
- Pharming

* Definitions taken or adapted from I&J Operational Approaches

DNS ABUSE INSTITUTE

Malicious vs. Compromised

- Malicious domains were registered for the primary purpose of causing harm.

- A compromised website, domain name, service, or resource is one that was created for a benign purpose, and was later used for harm by a third party without the consent of the operator.

Phishing – What is It?

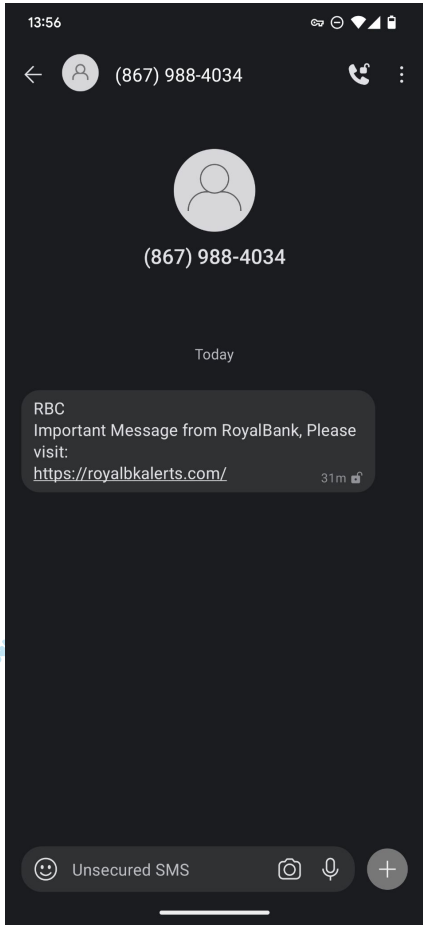
An attack that uses deception to trick a victim into revealing sensitive information via email or website.

- Information can be: personal, corporate, or financial (e.g. account numbers, login IDs, passwords)
- Deception is typically visual, using branding and typos

What does phishing look like?

- Malicious Domain
- Compromised Website
- Malicious Subdomain

Malicious Domain Used for Phishing



Your account are currently suspended.

Royal Bank

Your account has been suspended.

We have detected unusual activity on your account starting with 4519 0*** **** ****.
For your protection, we have temporarily placed your account on hold and any pending payments or deposits on hold as well.

Your account will remain on hold until we are able to confirm that you are the authorized owner of the payment method used in the recent transaction.
To restore access to your account, sign in and follow the on-screen instructions.

Sign In

Once you have provided the required information, we will review it and respond within 24 hours.

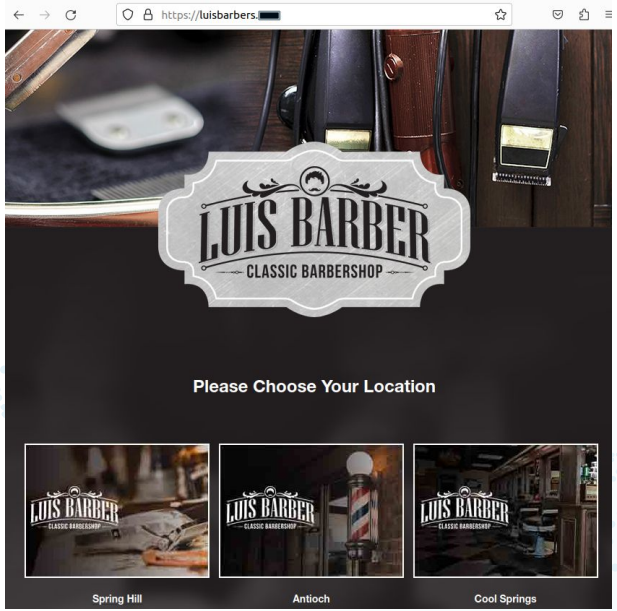
We are sorry for any inconvenience this may have caused.

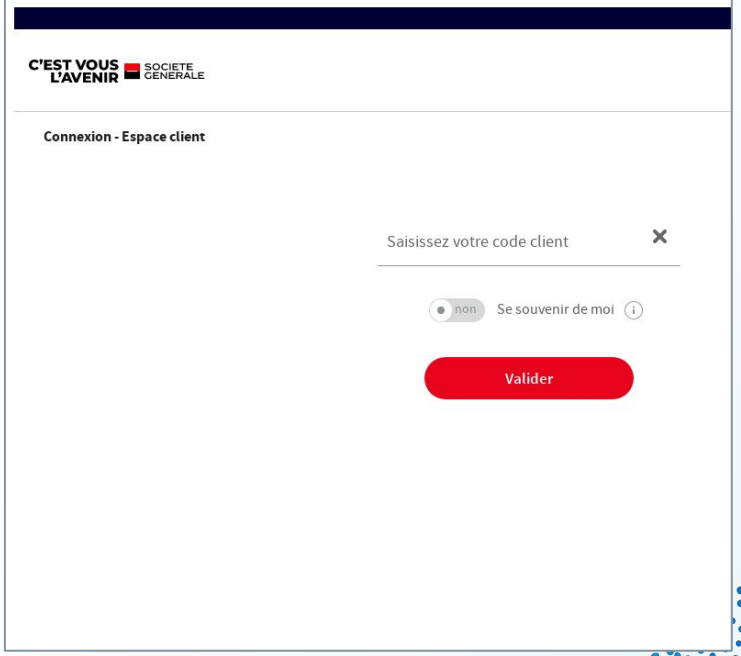
For further information, please refer to the RBC Terms and Conditions.

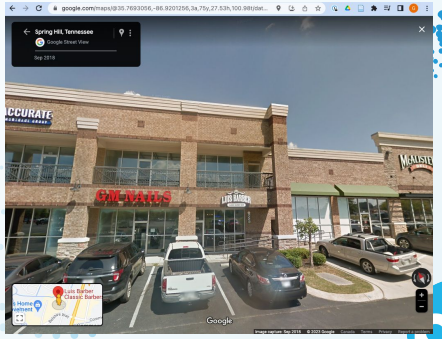
DNS ABUSE INSTITUTE

Compromised Website

- hxxps://coolsprings.luisbarbers.TLD/dbs/sg/SG22/
- Phishing at URL
- Benign content at domain
- Real business

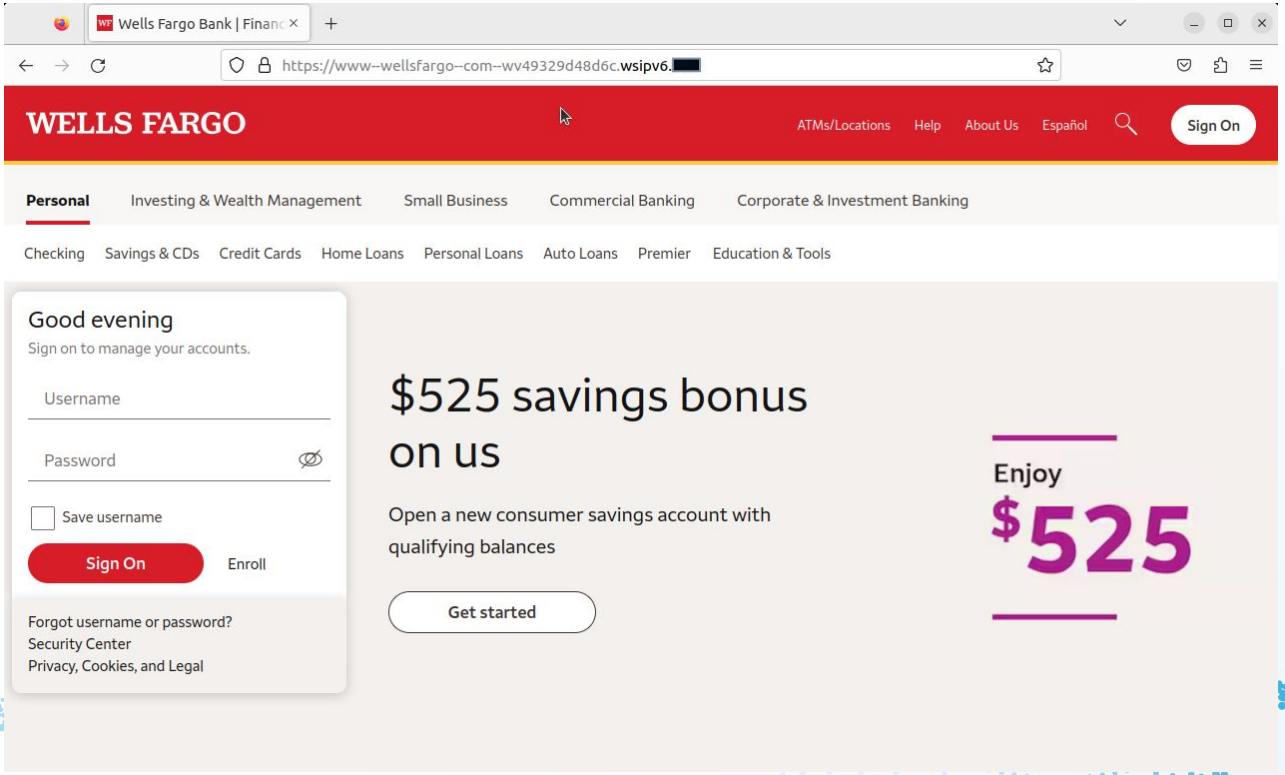






DNS ABUSE INSTITUTE

Malicious Subdomain



DNS ABUSE INSTITUTE

Malware - What is it?

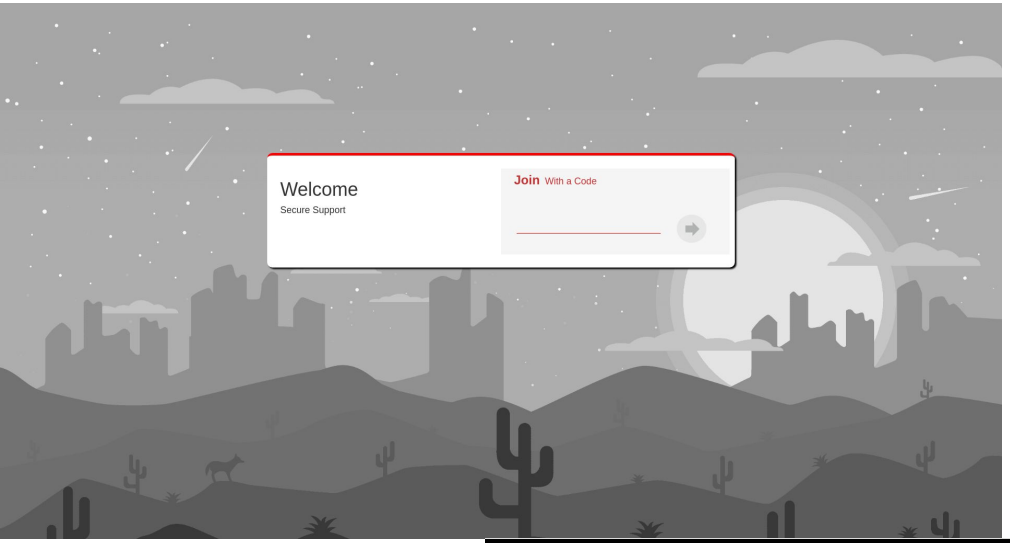
Malware is **malicious software**, installed on a device without the user's consent.

- Steals sensitive information
- Uses resources to send spam or join botnets

Malware includes **viruses, spyware, ransomware**, and other unwanted software.

Malware - What does it look like?

- Often uses a tech support scam
- Files in email, messages, or tricked into downloading
- Rise in cryptocurrency has seen a corresponding rise in Crypto mining or stealing malware



pcsupport.tld

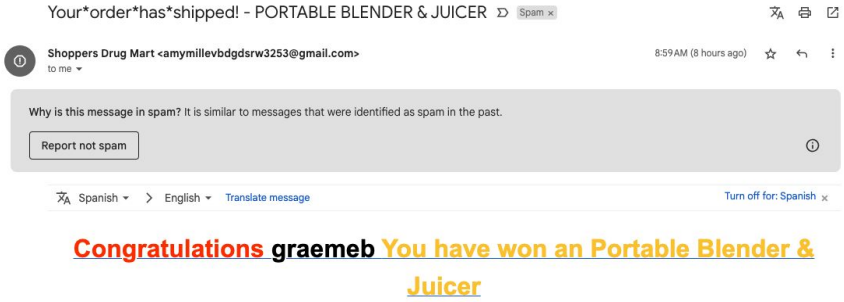
geek47.tld

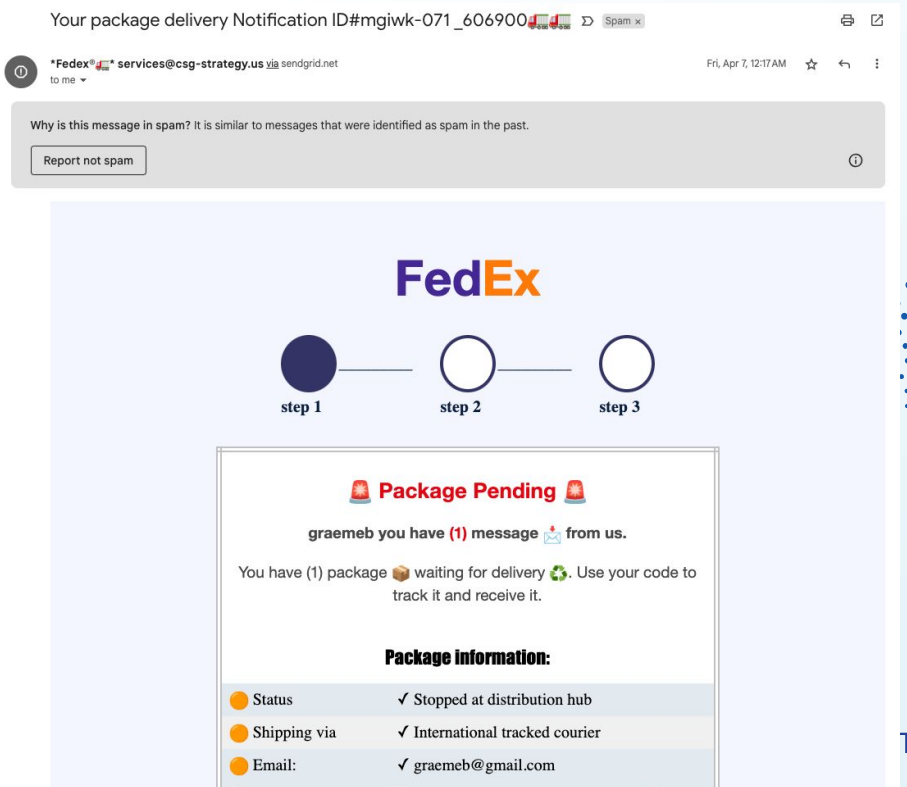
Spam – What is it?

Spam is **unsolicited bulk email.**

Spam email may carry malware, and/or deliver phishing or pharming attacks

Spam – What does it look like?

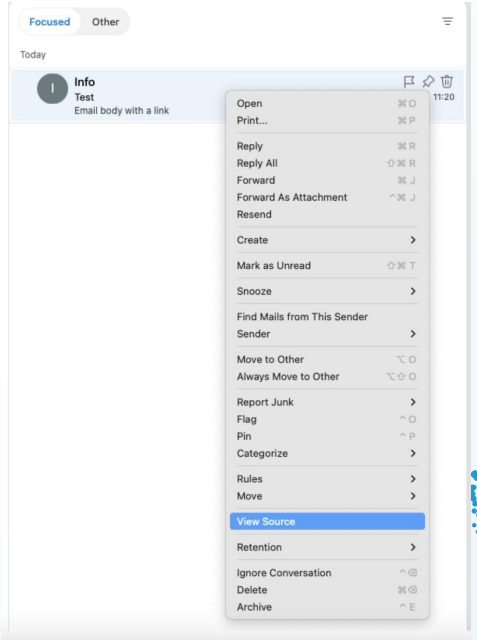




Aside - Reporting DNS Abuse in Email

Reporting DNS Abuse that *only* involves email is **hard**.

- It's VERY easy to fake who sent an email
- **Email headers** and/or source are often required



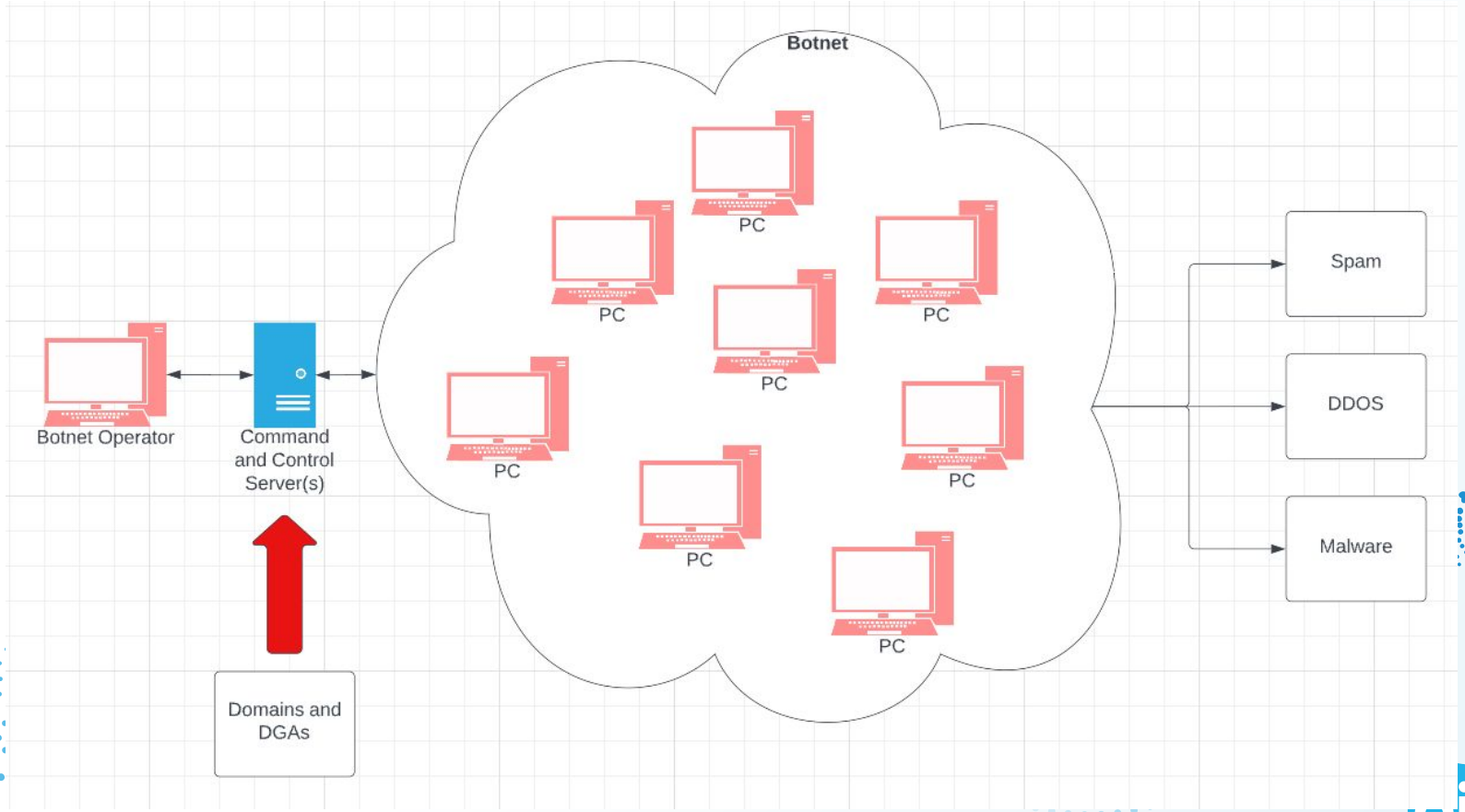
DNS ABUSE INSTITUTE

Botnet C&C - What is it?

Botnets are collections of Internet-connected devices that have been infected with malware and commanded to perform activities under the control of a remote administrator.

Domain names used to command and control Botnets are considered DNS Abuse.

Botnet C&C - What does it look like?



DNS ABUSE INSTITUTE

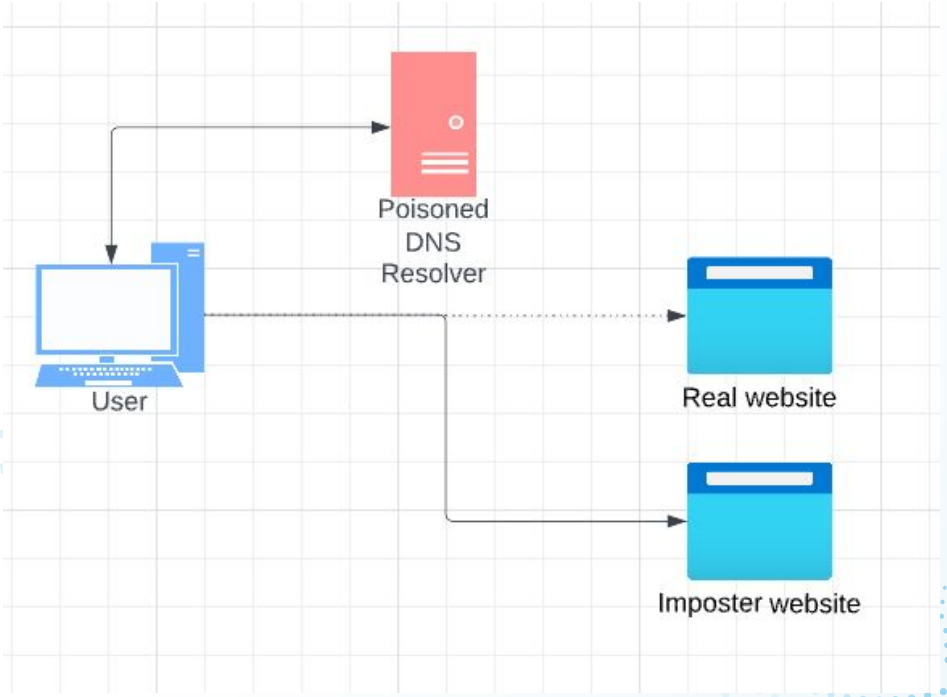
Botnet C&C - What does it look like?

- Likely, nothing to see, or a simple login
- More common:
  - list of domains,
  - List of potential domains
- Generally, complicated investigations across multiple LEAs, TLDs, and jurisdictions

Pharming – What is it?

Pharming is the redirection of unknowing users to fraudulent sites or services, typically through DNS hijacking or poisoning.

Pharming – What does it look like?



DNS ABUSE INSTITUTE

Useful Links

- Email Spoofing Explained
- How to report phishing
- CPH Guide to Abuse Reporting
- RySG Framework on Domain Generating Algorithms
- NetBeacon.org