
# FISHING FOR PHISHING

USING DNS ZONE FILES

WITH MATT MEIS

# Agenda

1. Introduction
2. Phishing and BEC Problem
3. DNS and Zone Files
4. Finding Phishing with Zone Files
5. Open-Source Tool Demo
    1. And Link!

**Goals Today:**

**Share solutions as a community**

**Walk away with one new idea to protect your org from phishing related attacks.**

# About Me

Software Development background

Recently a Threat Hunter at a financial institution

Currently an IT Security Instructor with Mid-State Technical College

Current Secretary of InfraGard WI

Cofounded DomainAlarm with Ryan Victory

DOMAIN ALARM

# The Phishing Problem

# The Problem

## Phishing

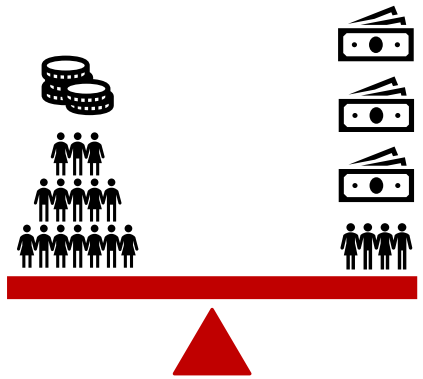
Criminal lures employees or customers to a fake page to steal information, credentials, or money

**$44,213,707**

In Losses in 2021 (US)

**323,972**

US Phishing victims



## Business Email Compromise

Criminal emails employees, pretending to be an executive, and asks for funds to be transferred to the criminal

**$2,395,953,296**

In Losses in 2021 (US)

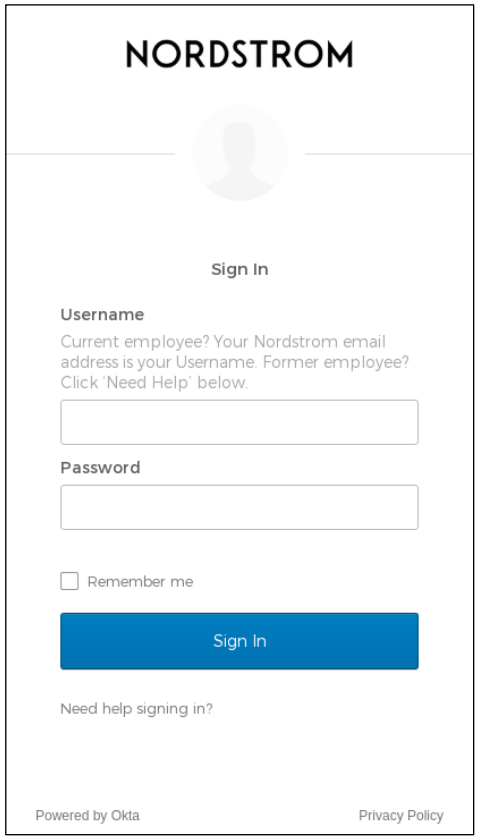
**19,954**

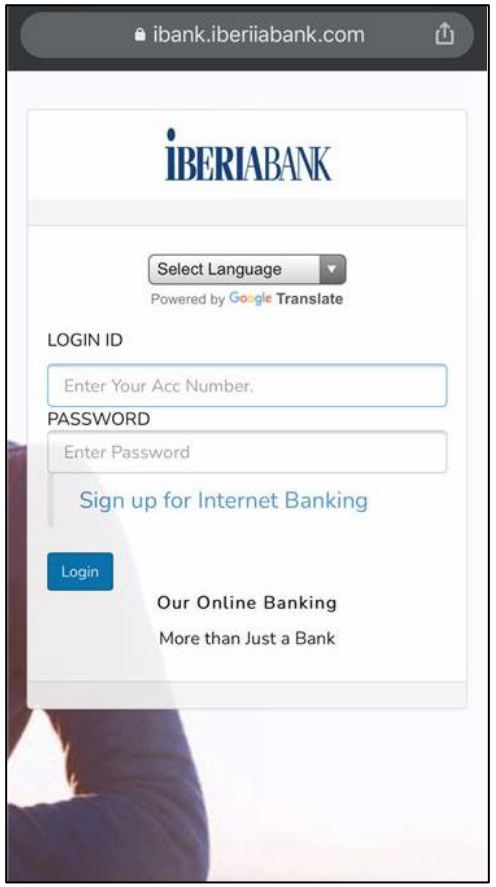
US BEC victims

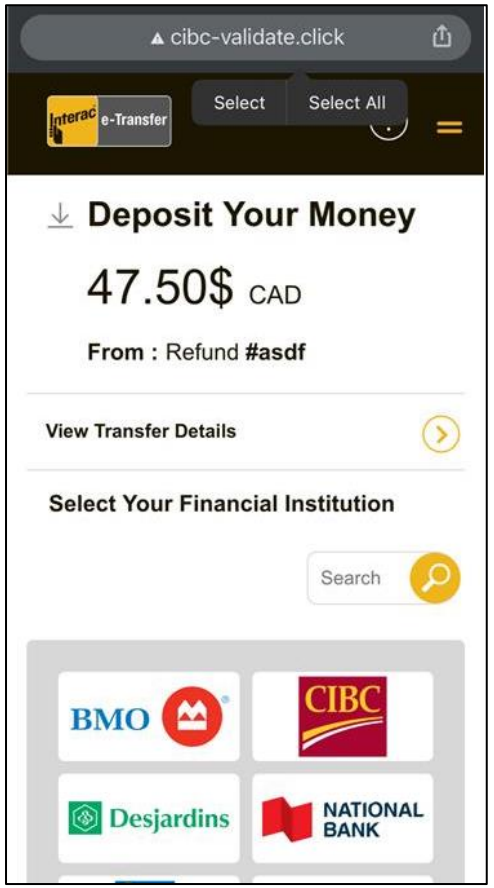
IC3 Annual Report for 2021: https://www.ic3.gov/Media/PDF/AnnualReport/2021_IC3Report.pdf

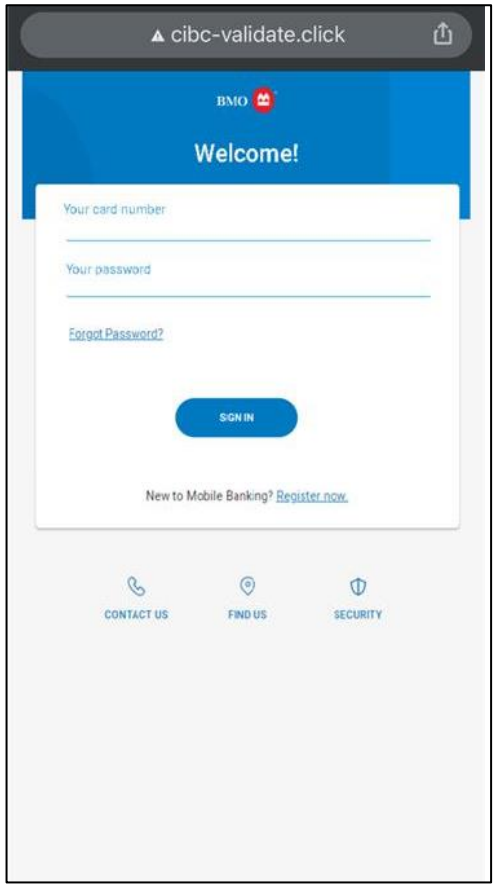
# Real Phishing = Real Losses

https://nordtrom-okta[.]com



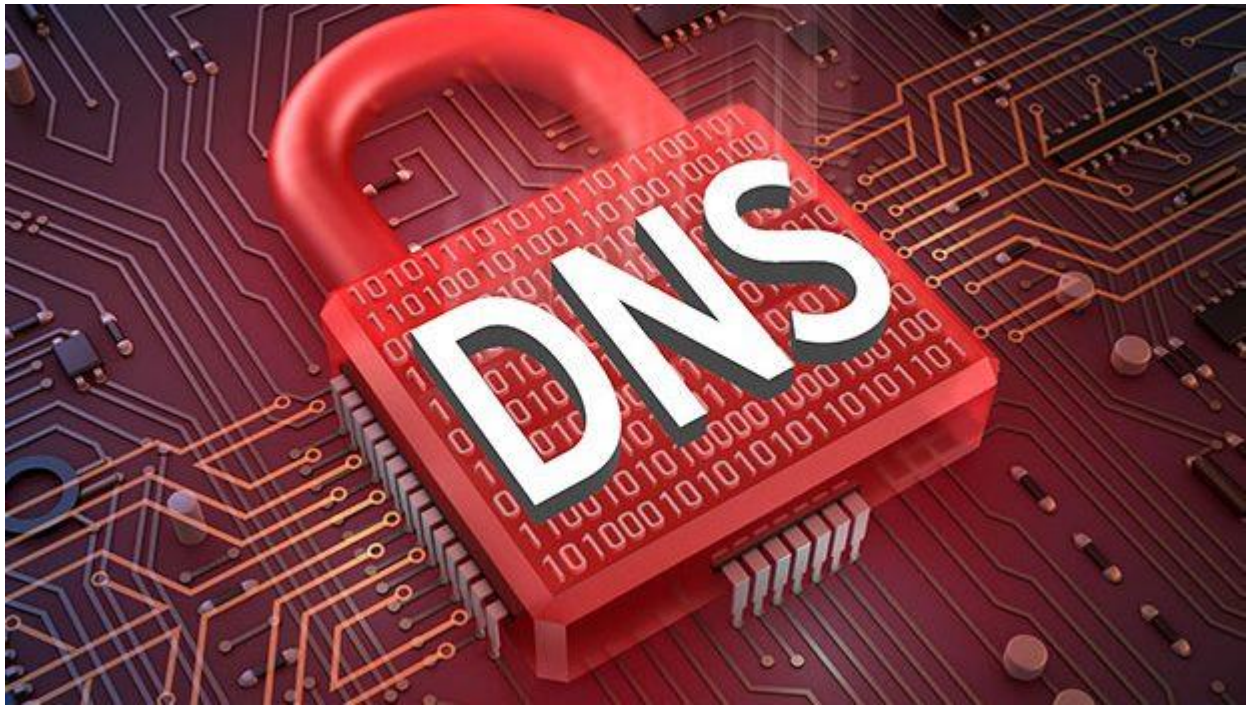



# Low Barrier to Entry for Criminals

1. Hosting
    1. $5 a month for cheap server Digital Ocean
2. Domain
    1. $10 .com domains from GoDaddy
3. Email Provider (optional)
    1. $11 for 100,000 emails a month from Mailchimp

https://www.csoonline.com/article/3340049/how-much-does-it-cost-to-launch-a-cyberattack.html

# DNS
# and
# Zone Files

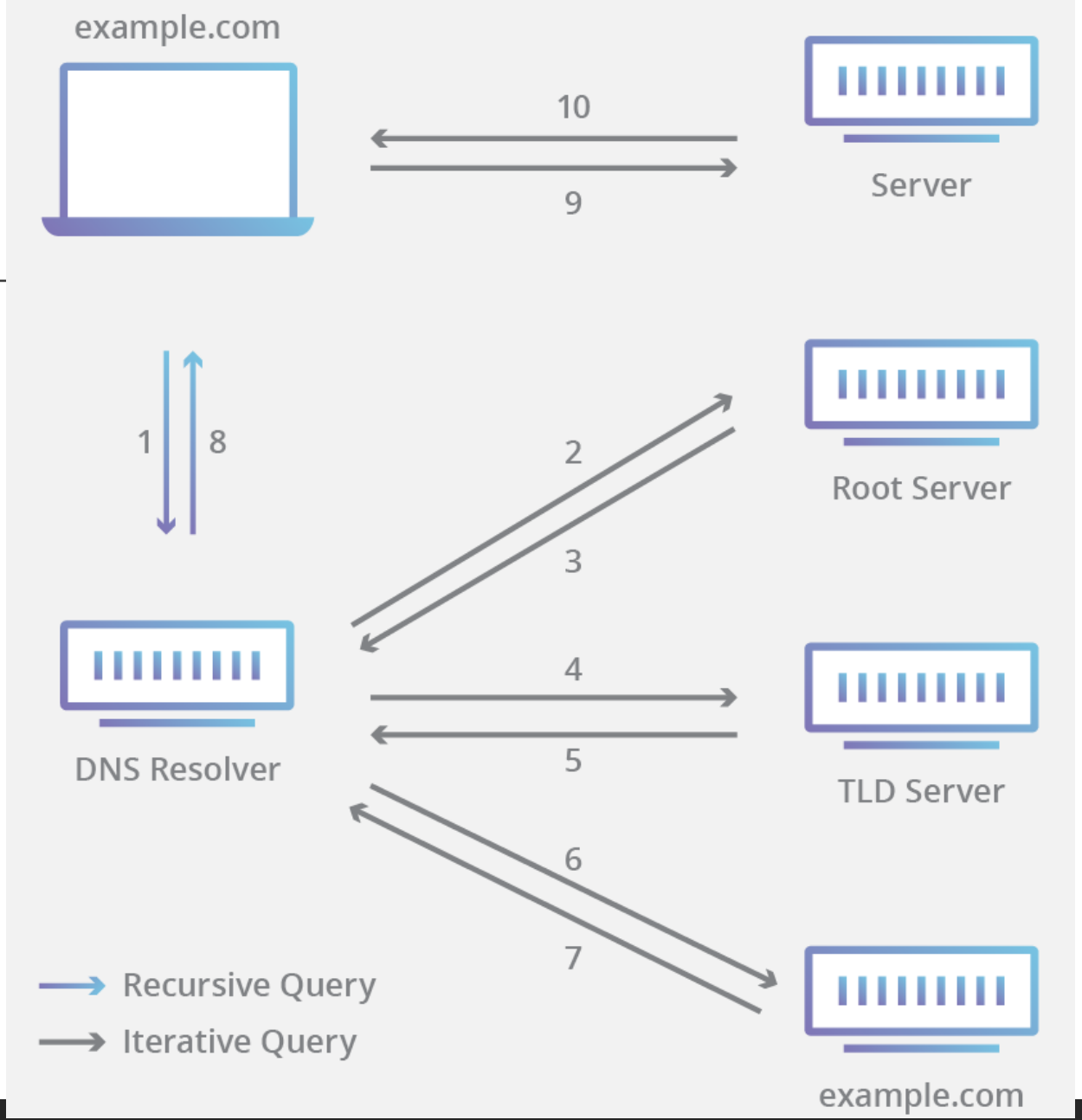


# What is DNS

Domain Name to IP address lookup

This must be public and easily for a domain name to work on the internet

8 steps in the lookup process



# What are Zone Files?

Text files with domain names and ip address.

Distinct file per Top Level Domain (TLD)

Zone file contains every name that the name server knows about

```
1   yachts. 3600    in      soa     ns0.centralnic.net. hostmaster.cen
2   000000.yachts.  3600    in      ns      ns1.uniregistry-dns.com.
3   000000.yachts.  3600    in      ns      ns1.uniregistry-dns.net.
4   000000.yachts.  3600    in      ns      ns2.uniregistry-dns.com.
5   000000.yachts.  3600    in      ns      ns2.uniregistry-dns.net.
6   1097.yachts.    3600    in      ns      ns1.dnsowl.com.
7   1097.yachts.    3600    in      ns      ns2.dnsowl.com.
8   1097.yachts.    3600    in      ns      ns3.dnsowl.com.
9   111.yachts.     3600    in      ns      curitiba.porkbun.com.
10  111.yachts.     3600    in      ns      fortaleza.porkbun.com.
11  111.yachts.     3600    in      ns      maceio.porkbun.com.
12  111.yachts.     3600    in      ns      salvador.porkbun.com.
13  1232.yachts.    3600    in      ns      ns1.dynadot.com.
```

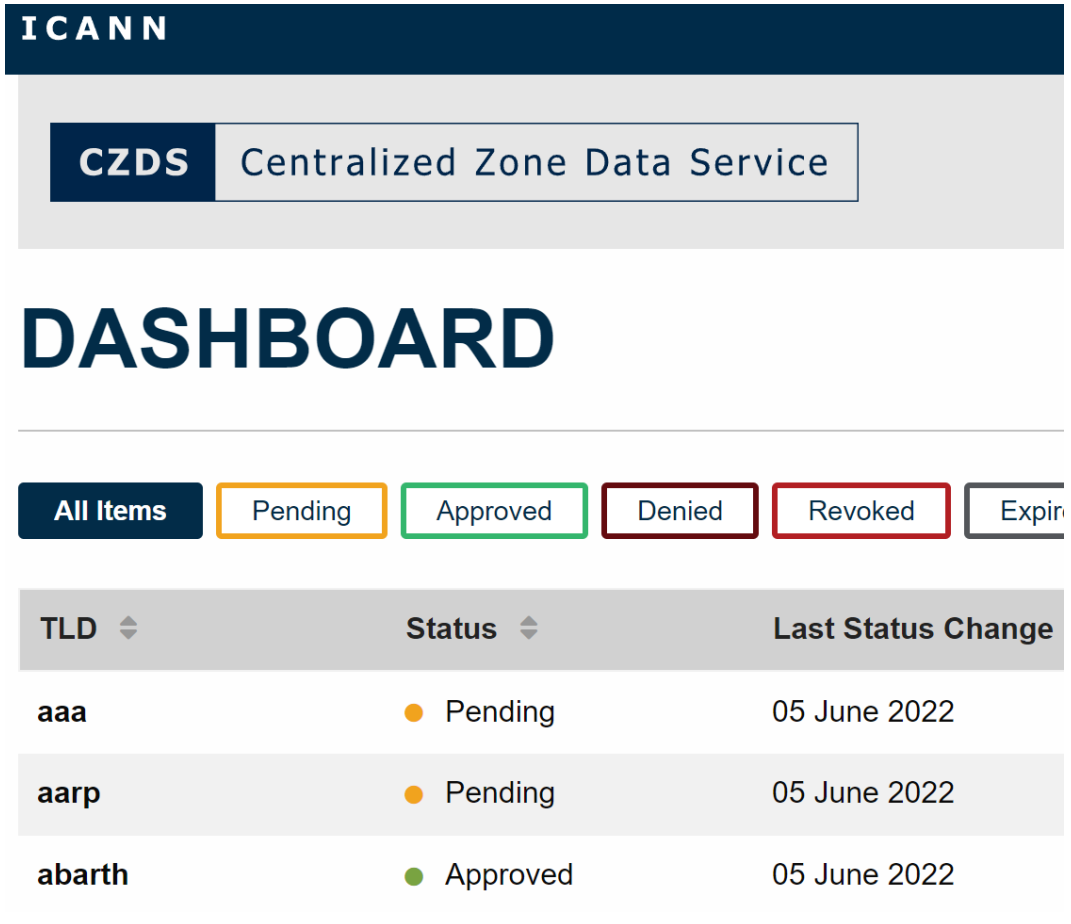
# Using Zone Files

Where to get them:

- ICANN help with that: https://czds.icann.org/home
- API: https://github.com/icann/czds-api-client-python

How can we use this?

- Almost there!



# Putting it All Together

# Results from Phishing Monitoring

## Defend your Company

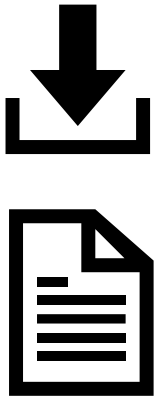
- Detect BEC domains before fraud attempts
- Find phishing targeting your employees
- Monitor Vendor domains to reduce 3rd party risk
- Brand monitoring

## Protect your Customers

- Detect domains impersonating your brand via email to customers
- Detect domains impersonating your customers
- Detect phishing pages that are trying to steal customer login information

# The Process

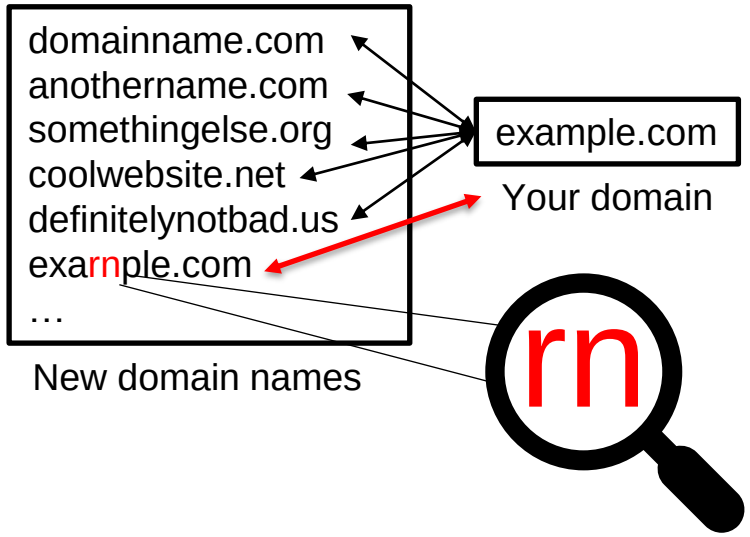
## Load



## Scan

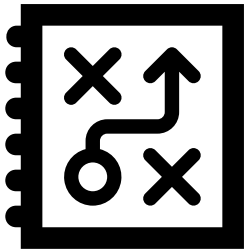
200,000+

New domain names registered daily




## Alert

## Act



# The Tool

GitHub: https://github.com/DomainAlarm/domain-scanner

Requirements:

- DNS Zone Files
- Configuration
  - Detection types to use
  - Directory to scan
  - Result format
  - License: GNU GPLv3

Demo Time!

# Respond to Alerts

# Malicious Site Takedowns

Forward the original phishing email to the following email addresses:

- phishing-report@us-cert.gov
- reportphishing@apwg.org
- reportphishing@antiphishing.org

Copy the malicious URL of the phishing site and use it to report to the following anti phishing services:

- Google: https://www.google.com/safebrowsing/report_phish/?hl=en
- Microsoft: https://support.microsoft.com/en-us/kb/930167

View whois information and contact abuse email.

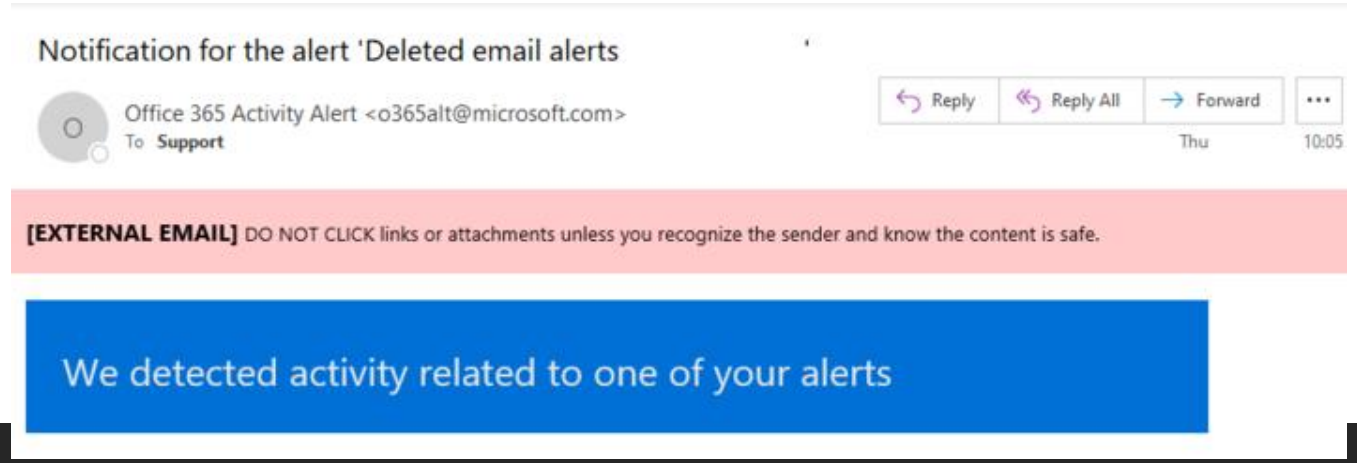
# Email Protection

You can protect your employees and corporate email by blocking risky domains from emailing you.

- How to: https://businesstechplanet.com/how-to-block-domains-in-microsoft-exchange-online-admin-center/

You should also put a banner warning on all external email!

- How to: https://lazyadmin.nl/it/add-external-email-warning-to-office-365-and-outlook/



*We Must be a proactive community to fight criminals!*

Open Discussion

# Other Phishing Opportunities

DNS Twist

Monitor inbound redirects!

Certificate monitoring

# Footnotes

# Setup

Option 1: A Unix system with Ruby and Git installed

Get the code: git clone https://github.com/DomainAlarm/domain-scanner.git

Install Gems:

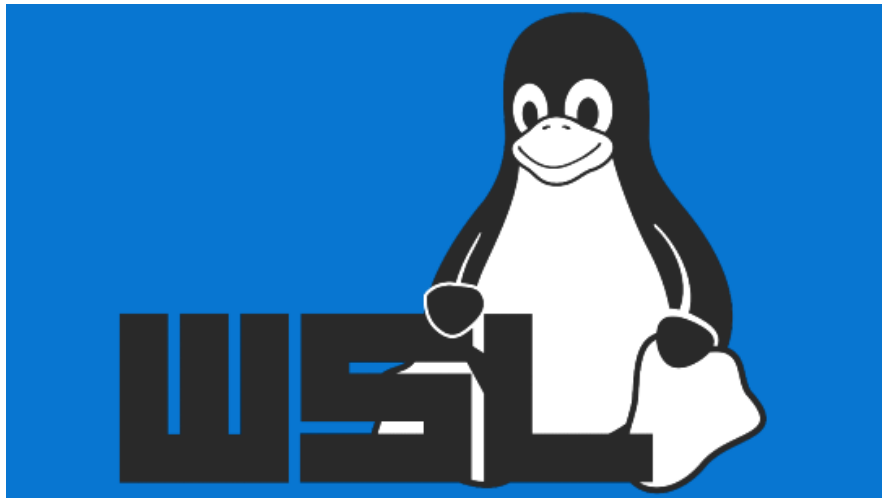
- Sudo gem install bundler
- Get a C compiler for damerau-levenshtein: sudo apt install build-essential
- Install ruby dev tools: sudo apt-get install ruby ruby-all-dev
- Bundle install (this gets the necessary gems for the project)
- Ensure you have the file command: sudo apt install file

Option 2: Use docker

# Other Tools Used in the Demo

Windows Subsystem for Linux (WSL)

Windows Terminal (powershell, linux terminal, command prompt, and azure cloud shell all in one)




# Bonus Content

Weekly Newsletter with security news, tools, and discussions

SecFraudOps Newsletter: https://secfraudops.substack.com/

DOMAIN ALARM

https://domainalarm.net

contact@domainalarm.net

Ryan Victory: 414-617-1675

Matt Meis: 715-513-6347

Proudly based in Stevens Point, WI