DNS Triage

https://github.com/Wh1t3Rh1n0/dns-triage

Written by Michael Allen || linkedin.com/in/wh1t3rh1n0/
Reviewed by Dale Hobbs || linkedin.com/in/dale-hobbs/

What is it?

Fast, actionable, tech reconnaissance for attackers.

DNS Triage is a reconnaissance tool that finds information about an organization's infrastructure, software, and third-party services as fast as possible. The goal of DNS Triage is not to exhaustively find every technology asset that exists on the internet. The goal is to find the most commonly abused items of interest for real attackers.

How does it work?

DNS Triage uses a combination of DNS queries and web requests to collect interesting information. Specifically:

1. It gathers TXT, MX, and NS records of the target domain.
2. It queries DNS records of commonly abused Microsoft services and checks whether they are hosted in Microsoft's cloud or on-premises.
3. It resolves a hand-picked selection of very common subdomains on the target domain, where abusable services and infrastructure are often found.
4. It makes targeted DNS and/or HTTP queries of third-party services to determine which services are used by the organization.
5. Whenever possible, it displays additional details that may be useful for abusing the resources that have been discovered.

How do I install it?

1. Download and extract the ZIP archive from the project repository at **https://github.com/Wh1t3Rh1n0/dns-triage** or run the following command to download DNS Triage with git:

```
git clone https://github.com/Wh1t3Rh1n0/dns-triage
```

2. Open a terminal window in the folder where you downloaded/extracted the DNS Triage files, and run the following command to install Python libraries used by DNS Triage:

```
python3 -m pip install -r requirements.txt
```

How do I use it?

The recommended way to launch DNS Triage is simply to run dns-triage.py command followed by the domain name that you want to target. An example command targeting example.com is shown below.

```
python3 dns-triage.py example.com
```

Tip: Help documentation describing other additional options can be shown by running DNS Triage without specifying any other arguments.

What does all the output mean?

DNS Triage can sometimes generate a lot of output. Here are some examples of the output it displays and key information you should look for.

TXT Records

Clues in TXT records often reveal technology products and services used by the organization. This information can be very useful, both for social engineering and for technical attacks.

```
TXT records for example.com
-----------------------
atlassian-domain-verification=Zwms6wYibNl10yHl8rJaGNFzJq96MUSWCIbyNg1WuDMgusi9fbuJanqeCKADWjBf
canva-site-verification=O2TSnrbZLq2Zsmc59AZYuw
docusign=3eca8259-748e-4a0c-900c-d5374132c19a
fastly-domain-delegation-67v7EJ9cwh7RdkWE-575288-2023-02-20
jamf-site-verification=Az6mZIKdruDZf-TDNBfGvA
miro-verification=de40aec19ca469948512b053eec7fd3fa1d64856
notion-domain-verification=MATLqlLiSvHSDYZEDMdkLAWxdaqERmHce8teR6dbZZt
stripe-verification=8fe88582423fc4d3b75ce1d191806730daafddbc24cc9c5519cce814a6d55c79
twilio-domain-verification=16eae8c3b53caf7d425877239f2f84b4
vmware-cloud-verification-ade55cf1-cfe6-4292-bdfb-a008b2b7d826
zoom-domain-verification=72479dc7-8727-486a-a3a0-1dc8774df145
```

MX Records

May indicate the organization's email defenses. In this case, ProofPoint has been detected.

```
MX records for example.com
-----------------------
10 mxa-00123123.gslb.pphosted.com.
10 mxb-00321321.gslb.pphosted.com.

[!] ProofPoint detected as default incoming email service.
    Numeric ID from the subdomain name may be used here:
    - https://app.explore.proofpoint.com/v2/apps/login/?usercenter=false
```

Microsoft Services

On-premises and cloud-hosted Microsoft services are frequently affected by known vulnerabilities and exploitation paths. In the example below, a Microsoft Exchange Smart Host has been detected, which is often vulnerable to email spoofing attacks. The link to a relevant blog, with exploitation details, is included in the output.

```
==========================================================================
Checking for Microsoft Exchange Smart Hosts...
==========================================================================
[+] example-com.mail.protection.outlook.com > 52.101.20.2
    [💥]  Microsoft Exchange Online smart host detected!
        - May allow email spoofing. See:
          https://www.blackhillsinfosec.com/spoofing-microsoft-365-like-its-1995/
```

Interesting Subdomains

Subdomains often indicate the presence of abusable infrastructure. In the example below, the securemail subdomain was detected, and DNS Triage recommends URLs that the attacker should investigate to abuse this service.

Tip: Registering a new account on an organization's own encrypted email portal and then phishing them from that account is a favorite way to bypass email filters.

```
Checking for interesting subdomains...
--------------------------------------
[+] securemail.example.com > pe-00123123.gslb.pphosted.com.
    Possible Secure Mail app. Try:
    - https://securemail.example.com/
    - https://securemail.example.com/encrypt  (ProofPoint Encrypted Mail user registration)
    - https://securemail.example.com/s/preregister  (Zix Secure Message Center user registration)

[+] adfs.example.com > ex14-crtrs.tng.example.com.
    Possible ADFS portal
    - https://adfs.example.com/adfs/ls/idpinitiatedsignon.htm

[+] mail.example.com > ghs.google.com.
```

Third-Party Services

The final section of the output shows third-party services that were detected. Here, we see that the organization is using ServiceNow, Webex, Jamf, Slack, and GitHub. In addition to leveraging these services for social engineering, detecting Jamf indicates to us that at least some Apple computers are likely present in the environment. This is key information when preparing executable payloads for an attack.

```
================================================================================
Checking third-party services of "example"...
================================================================================

[+] example.service-now.com - ServiceNow likely in use!

[+] example.webex.com - Webex likely in use!
    - Try browsing to this subdomain, and look in Web UI for calendar/meetings.
    - Try Google-dorking this domain to find links to meetings.

[+] example.jamfcloud.com - Jamf Apple Device Management likely in use!

[+] https://example.slack.com - Slack likely in use!

[+] https://github.com/example - GitHub likely in use!
```