DNS Based OSINT Techniques for Product and Service Discovery

Speaker: Rishi (@rxerium)

Date: 17th October 2025

Event: BSides Cymru

whoami

Security researcher based in London specialising in vulnerability research, attack surface management, threat intelligence, OSINT and risk management, dedicated to strengthening cyber resilience through proactive discovery and defence.

Rishi (@rxerium)

Security Researcher

Handle: @rxerium

LinkedIn

Twitter / X

The Realm of DNS Records & TXT Records

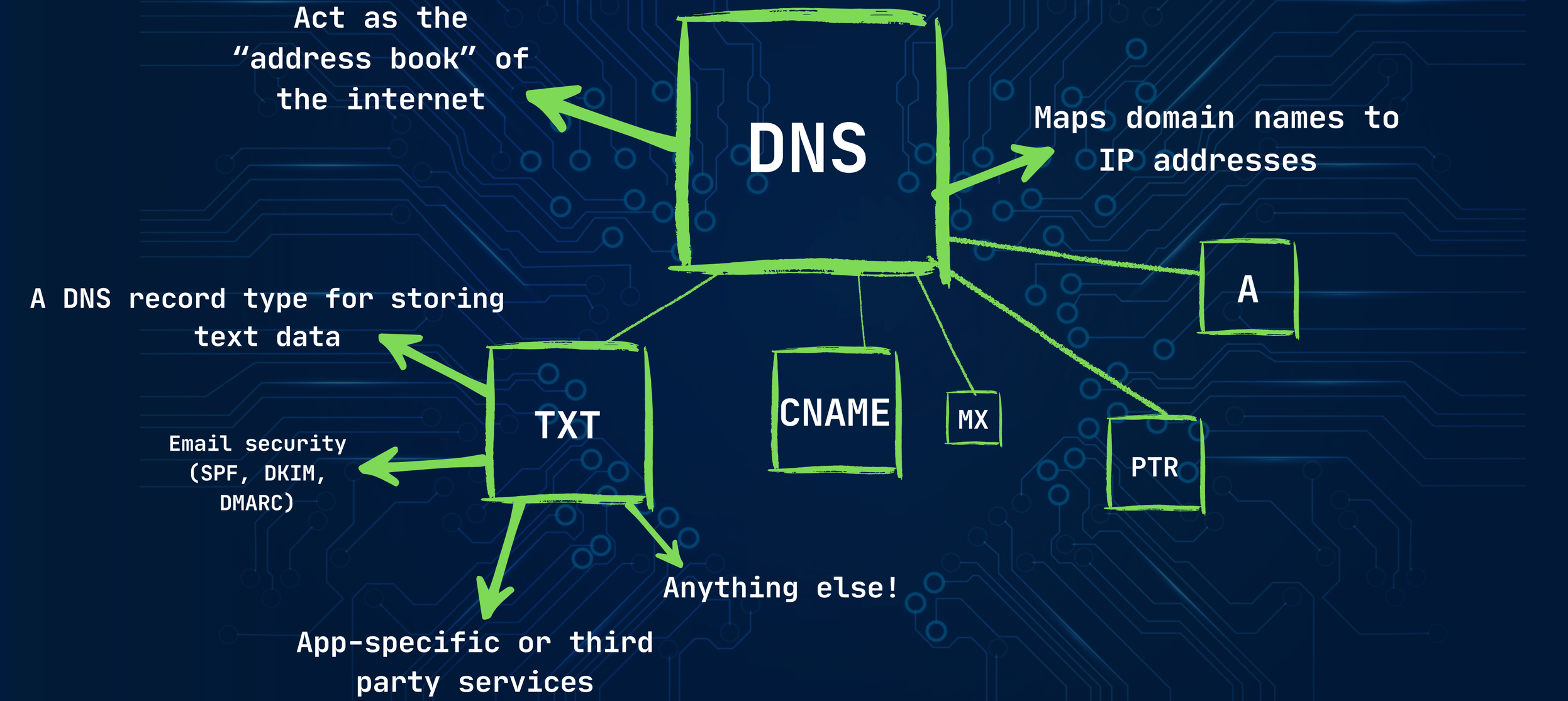
DNS RECORDS

- Map domain names (e.g., example.com) to IP addresses, mail servers, or verification data.
- Act as the “address book” of the internet.

TXT RECORDS

- DNS record type for storing text data.
- Common uses:
  - Email security (SPF, DKIM, DMARC).
  - Domain ownership verification (Google, Microsoft etc..)
  - App-specific or third party information + anything else

The Realm of DNS Records



Example TXT Records

```
> echo adobe.com | dnsx -txt -re -silent

adobe.com [TXT] [openai-domain-verification=dv-xsmu3zewiau4l5v23bd1l0ts]
adobe.com [TXT] [_globalsign-domain-verification=lnj0izgjup0bosg71asjuwlkcoksamz2emkst9_cus]
adobe.com [TXT] [atlassian-domain-verification=9uyxhbbyogbk9b1ain6fhelo/cg08ihvd7rwduadq8ivehyffecc6gtaxw3kwshw]
adobe.com [TXT] [google-site-verification=iwlts5bv60rglzcktgxcltsunlb9ct_09-pevxid2o8]
adobe.com [TXT] [cisco-ci-domain-verification=6e22d6f101dd96dc12fabfe843ff4e6748b9f7a89af1ff342476b923f01e4292]
adobe.com [TXT] [drift-domain-verification=502160a86dc2f7411dec54f019b785a7010eb9f38a6152011c1be40b89f68e9b]
```

Real world use case

GitHub Account Compromise Led to Salesloft Drift Breach Affecting 22 Companies

Supply Chain Attack / API Security

Sep 08, 2025 Ravie Lakshmanan

Salesloft has reve
GitHub account.

Google-owned M
UNC6395, acces
the digital intruc
impacted by a s

"With this acce
and establish

News
kers Exploit Pandoc CVE-2025
91 to Target AWS IMDS and Steal
2 IAM Credentials

Salesloft confirmed the impact is much more severe and widespread. (imageBROKER/Timon Schneider/Alamy)

Salesloft pinned the root cause of the Drift supply-chain attacks to a threat group gaining access to its GitHub account as far back as March, the company said in an update Saturday.

During a 10-day period in mid-August, the threat group compromised and stole data from hundreds of organizations.

The threat group, which Google tracks as UNC6395, spent time lurking in the Salesloft application environment, downloaded content from multiple repositories, added a guest user and set up workflows over a monthslong period through June, according to Salesloft.

SHARE

NEWS 8 SEP 2025

Qualys, Tenable Latest Vi

Kevin Poireault
Reporter, Infosecurity Magazine
Follow @Kpoireault Connect on LinkedIn

Cybersecurity providers Tenable and Qualys are the lates
companies affected by a significant supply chain attack t
customer data.

The campaign involved the theft of OAuth authentication
Salesloft Drift, a third-party application integrated with Sa
workflows and manage leads and contact information.

In a security alert on September 3, vulnerability assessment firm Tenable said that an unauthorized user gained access to a portion of some of its customers' information stored in the company's Salesforce instance.

This data included subject lines and initial descriptions provided by customers when opening a Tenable support case as well as commonly available business contact information, such as names, business email addresses, phone numbers and location references.

"At this time, we have no evidence that any of this information has been misused," the security provider noted. Tenable products and data within the Tenable product suite were unaffected.

Three days later, risk management firm Qualys issued a similar alert, stating the credentials stolen during the campaign of OAuth token theft had allowed attackers "limited access to some Qualys Salesforce information."

Zeljka Zorz, Editor-in-Chief, Help Net Security
September 8, 2025

Share

Salesloft Drift data breach: Investigation reveals how attackers got in

The attack that resulted in the Salesloft Drift data breach started with the compromise of the company's GitHub account, Salesloft confirmed this weekend.

Supply chain compromise

On August 26, the company publicly revealed that earlier that month, a threat actor exfiltrated data from their customers' Salesforce instances by leveraging stolen OAuth credentials that enable the integration of their Drift (Salesloft) chatbot with said instances.

Google Threat Intelligence Group attributed the attack to an attack group they track as UNC6395.

They also said that the attackers were after sensitive access credentials – AWS access keys, passwords, Snowflake-related access tokens – that may be included in support tickets sent to those organizations by their customers.

A number of organizations, including Cloudflare, Zscaler, Palo Alto Networks, Elastic, Bugcrowd, and others, have since confirmed the data theft.

Most of the companies proceeded to analyze the potentially compromised data and, where they discovered customers secrets in support tickets, to notify affected customers. (Whether their reaction was quick enough to prevent the secrets' misuse remains to be seen.)

Impacting Facilities in North America

NEWS 26 AUG 2025
US: Maryland Confirms Cyber Incident Affecting State Transport Systems

NEWS 18 AUG 2025
Colt Customers Face Prolonged Outages After Major Cyber Incident

NEWS 13 AUG 2025
Staffing Company Manpower Discloses Data Breach

Salesloft Drift Supply Chain Attack

- Salesloft Drift was breached in August / September
- Exploited stolen OAuth tokens from Salesloft's Drift app were used to access and steal Salesloft data
- Over 700 companies were breached (Cloudflare, Workday, Elastic)

Salesloft Drift Detection via TXT Records

```
~ → cat input.txt | dnsx -silent -txt -re | grep "drift"
adobe.com [TXT] [drift-domain-verification=ce77053dc2d9b73c71437d5afda3b6d06fbc34a1b0e4527fe81c55e0d99ca4b4]
workday.com [TXT] [drift-domain-verification=c27c30cb5d3220cb0eb600eb65e1e6cec4f6d879afcce75a77d530854d500d00]
cloudflare.com [TXT] [drift-domain-verification=f037808a26ae8b25bc13b1f1f2b4c3e0f78c03e67f24cefdd4ec520efa8e719f]
netapp.com [TXT] [drift-domain-verification=52b9f655153f557dfa494e77ee44158246fd173da5fe107a371597dffa3de06a]
```

Why is this important?

- Prioritise threat hunting
- Assess third-party risk by understanding shared supply chain exposure
- Accelerate incident response through proactive detection

How do I run this myself?

Amass

In-depth attack surface mapping and asset discovery framework

owasp-amass/amass: In-depth attack surface mapping and asset discovery

In-depth attack surface mapping and asset discovery - owasp-amass/amass

GitHub

Nuclei

Fast, community-driven vulnerability scanning tool

projectdiscovery/nuclei: Nuclei is a fast, customizable vulnerability scanner powered by the global security community and built on a...

Nuclei is a fast, customizable vulnerability scanner powered by the global security community and built on a simple YAML-based DSL, enabling collaboration to tackle trending vulnerabilities on the ...

GitHub

Thank you for listening!