



# Discovering a Vulnerability in Internet Infrastructure That Can Affect Anyone

Brent Eskridge  
Staff Threat Researcher





# SITTING DUCKS: DOMAIN HIJACKING AT SCALE

Brent Eskridge  
Staff Threat Researcher



Infoblox  
Threat Intel

Hunt for bad guys on the  
internet using **DNS** ...

... and **statistics**.

70 billion **DNS events** analyzed per day

4 million **new indicators** added to feeds per month

# WHAT IS DOMAIN HIJACKING?

## AKA DOMAIN THEFT

- Using unauthorized methods to change the registration of a domain name
  - Often by abusing registrar or hosting provider services
- Threat actor then
  - Sells the domain to someone else
  - Redirects it to malicious content
  - Uses it for spam and phishing
- Common methods
  - Registrar hijacking
  - Domain shadowing
  - Dangling records



# REGISTRAR HIJACKING

## POP GOES THE SOURCE OF TRUTH

### Technique

- Gain access to the **registrar** via compromised customer or employee credentials
- Attacker either creates new domains under the customer account or modifies existing domains to point to malicious nameservers

### Example: 2013 NYTimes.com hijack

- Attackers social engineered registrar support team into transferring control of domain
- Domain was redirected to the Syrian Electronic Army



# DOMAIN SHADOWING

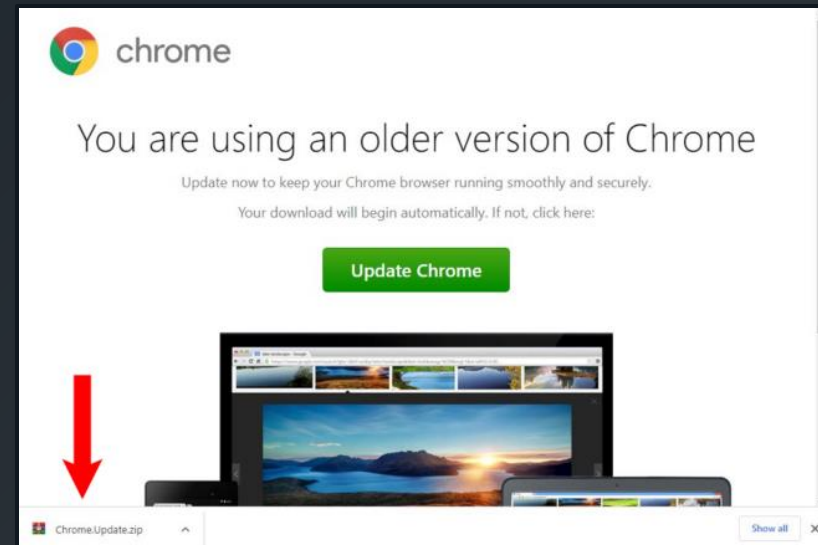
## WHO'S HIDING IN THE SHADOWS?

### Technique

- Gain access to the **authoritative DNS provider** for a zone(s)
- Create subdomain(s) without owner noticing
- Route victims to malicious infrastructure via trusted domain

### Example: SocGhosh campaigns

- Active since 2017
- 2022 campaign included **649 subdomains** across **16 benign SLDs**



# DANGLING RECORDS

## KEEP YOUR HOUSE TIDY

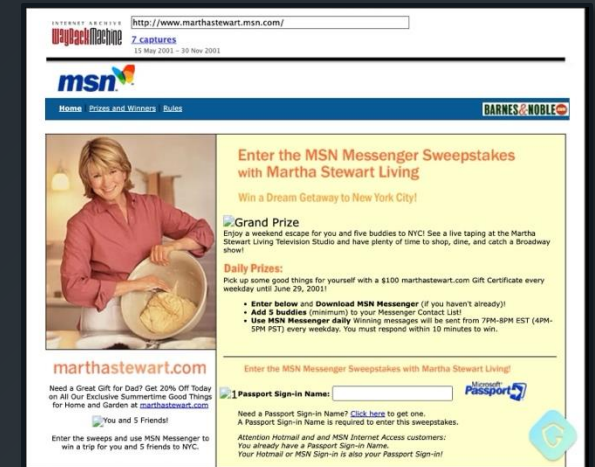
### Technique

- Attacker identifies legacy DNS records on victim domain(s) pointing to **external resources** that are no longer in use
- Attacker creates resources at location where dangling records point
  - Resource records (**A** / **CNAME** / **MX** / **NS**)

### Example: Guardio Labs

Discovered over **8,000** domains with subdomain hijacking -- "SubdoMailing"

- MSN
- CBS
- VMWare
- McAfee
- eBay
- Marvel



<https://labs.guardio.io/subdomailing-thousands-of-hijacked-major-brand-subdomains-found-bombarding-users-with-millions-a5e5fb892935>

# DISCOVERING SITTING DUCKS

- Proofpoint published on **404TDS** in Feb 2023
  - Russian **T**raffic **D**istribution **S**ystem
  - Uses 404 redirects to deliver malware, scams, and phishing
  - Used by multiple threat actors including TA571, TA866
- We began analyzing infrastructure in early 2024
  - Activity is much larger than 404TDS
  - Tracked as DNS threat actor **Vacant Viper**
  - **7,629** hijacked domains this year alone
  - Old and brand-protected domains
  - Multiple owners and multiple registrars





“

A situation where a DNS server is designated as **authoritative** for a domain but **does not have the proper zone information** to answer queries for that domain.

Lame delegation

”

# LAME DELEGATION EXAMPLE

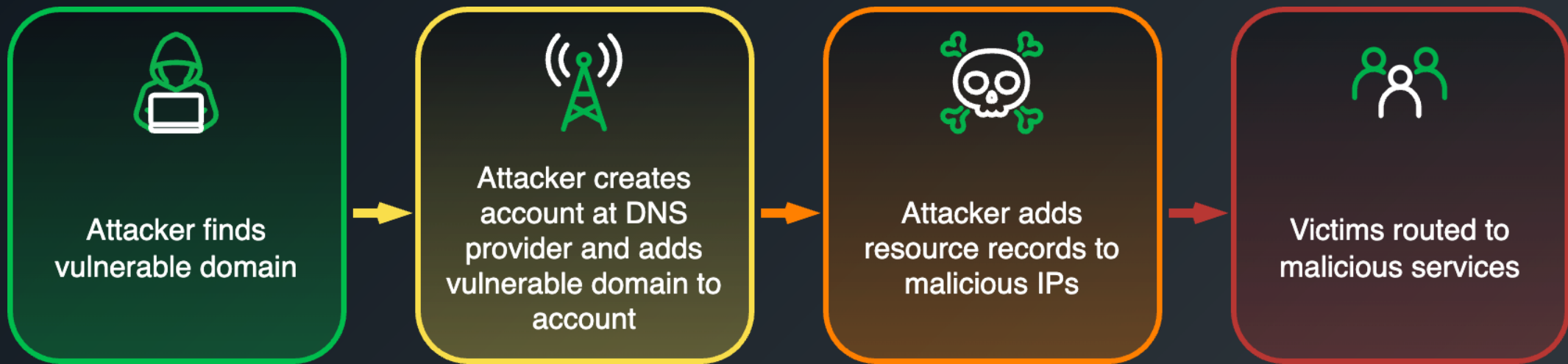
1. Company registers `brand[.]com` and `brand[.]net`
2. Company points the NS records to domains with DNS provider
3. Company configures `brand[.]com` at DNS provider to get services online
4. Company doesn't configure `brand[.]net`
5. The domain `brand[.]net` is considered a **lame delegation**

**Very common!**

**Do you know all the domains you own?**

Lame  
Delegation + Exploitable  
DNS  
Provider = Vulnerable  
Domain

Conditions for a Sitting Ducks Attack



## Sitting Ducks Attack Vector

# SITTING DUCK EXAMPLE

www.oesterreich.gv.at

85.158.225.16 Public Scan

Submitted URL: <https://calebandlouellen.com/qrlxp>  
Effective URL: <https://www.oesterreich.gv.at/>  
Submission Tags: @phish\_report

Submission: On July 16 via api (July 16th 2024, 5:34:46 am UTC) from FI+ - Scanned from FI+

Summary HTTP 35 Redirects Links 9 Behaviour Indicators Similar DOM Content API Verdicts

### Page URL History

This captures the URL locations of the websites, including HTTP redirects and client-side redirects via JavaScript or Meta fields.

1. <https://calebandlouellen.com/qrlxp> Page URL
2. <https://2in82j.ru/> HTTP 302  
<https://oesterreich.gv.at/> HTTP 301  
<https://www.oesterreich.gv.at/> Page URL

oesterreich.gv.at ID Austria eAusweise Lebenslagen Themen Services

## Informationen und Services der österreichischen Verwaltung

Überblick und Video

Suche nach ...

```
;; record times: 2016-09-09 20:20:33 .. 2017-04-19 22:13:14 (~222d 1h 52m)
;; count: 85; bailiwick: calebandlouellen.com.
calebandlouellen.com. A 107.170.2.22

;; record times: 2017-04-27 03:35:00 .. 2017-06-22 07:23:15 (~56d 3h 48m)
;; count: 43; bailiwick: calebandlouellen.com.
calebandlouellen.com. A 127.0.0.1

;; record times: 2023-03-02 11:53:23 .. 2023-04-02 00:26:24 (~30d 12h 33m)
;; count: 8; bailiwick: calebandlouellen.com.
calebandlouellen.com. A 193.3.19.203


;; record times: 2024-07-14 08:19:36 .. 2024-07-25 21:11:26 (~11d 12h 51m)
;; count: 12; bailiwick: calebandlouellen.com.
calebandlouellen.com. A 193.3.19.77
```

## Verwaltung geht jetzt noch besser.

Powered by Digital Austria


2024 wird das Angebot von oesterreich.gv.at kontinuierlich verbessert.

Neuerungen entdecken



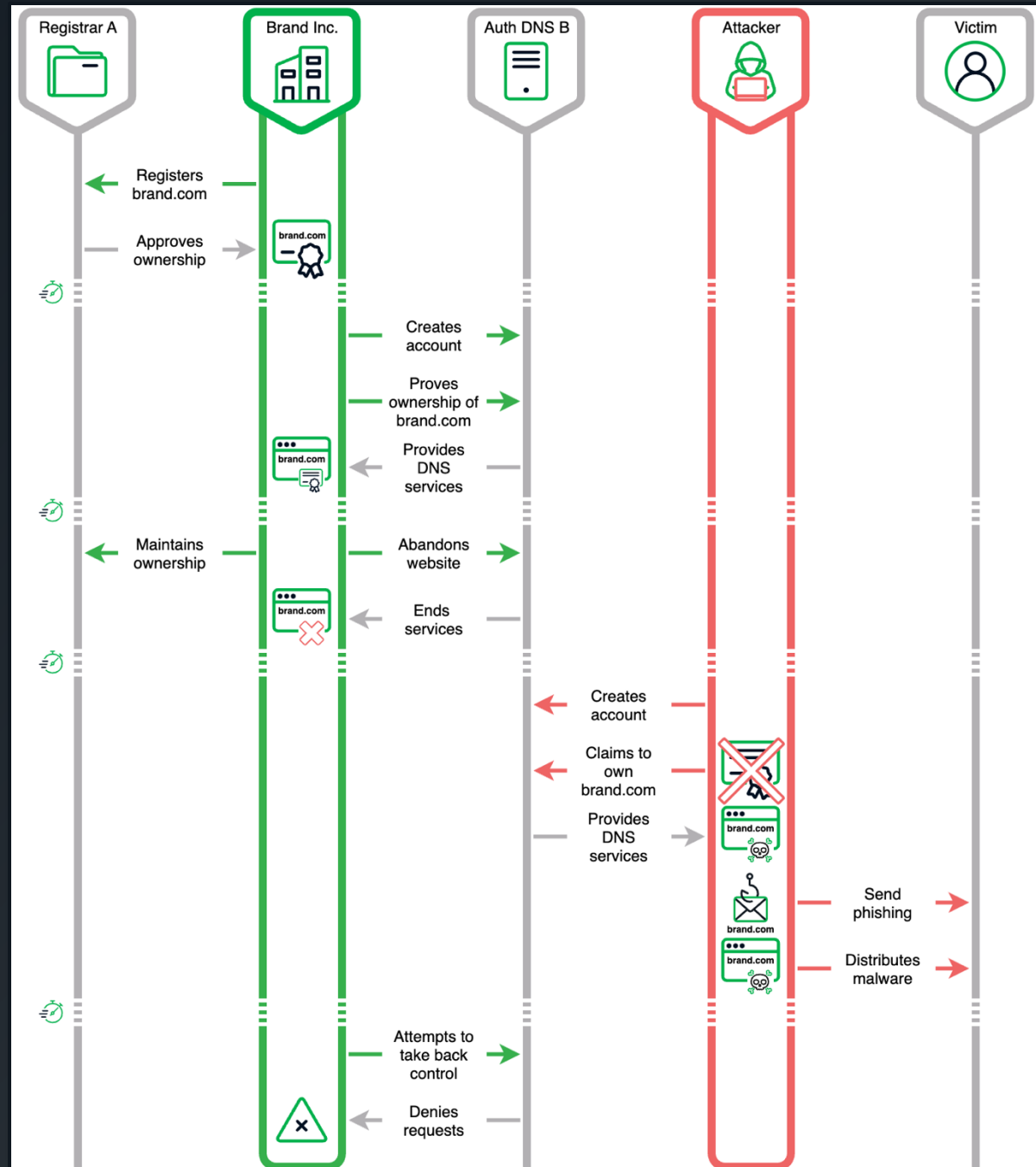
### Orientierung in meiner Lebenslage

Die wichtigsten Informationen zu verschiedenen Situationen kompakt zusammengefasst: [Alle Lebenslagen](#)



# ATTACK SCENARIO

1. **brand[.]com** is registered
2. Domain owner uses Auth DNS B for DNS authoritative server
3. Domain owner uses it for website
4. Domain owner stops using website and Auth DNS B services but still owns domain
5. Attacker creates account with DNS Auth B and claims **brand[.]com**
6. Attacker uses DNS Auth B to resolve **brand[.]com** to fake content
7. Attacker uses domain to send phishing emails and distribute malware
8. Domain owner tries to reconfigure DNS records for **brand[.]com** and is denied



# A HISTORY OF LAME DELEGATION WARNINGS

Dec 2016

"The Orphaned Internet – Taking Over 120K Domains via a DNS Vulnerability in AWS, Google Cloud, Rackspace and Digital Ocean"

- Matt Bryant

Nov 2020

Notification from Group-IB to Russian authorities

Jun 2024

Sitting Ducks  
Infoblox & Eclysium

Aug 2016

"Floating Domains – Taking Over 20K DigitalOcean Domains via a Lax Domain Import System"

- Matt Bryant

Jan 2019

"Bomb Threat, Sextortion Spammers Abused Weakness at GoDaddy.com"

- Brian Krebs, KrebsOnSecurity

Mar 2021

"The prevalence, persistence, and perils of lame delegations"

- Guatam Akiwate, APNIC

# SITTING DUCKS IN THE WILD

## VACANT VIPER IS DOING THIS – WHO ELSE IS?

- Generic detection of a Sitting Ducks attack is very hard
  - Requires human-in-the-loop analysis
  - We use a **model of threat actor behavior**
- **Over a dozen distinct actors** using Sitting Ducks
- All threat actors have a **Russian nexus**
- Earliest confirmed hijack is **November 2019** by Vacant Viper
- We found **6 exploitable providers** and **>20k hijacked domains**
- **Why so many Russian actors?** Group-IB published a similar attack in November 2020 – but only in Russian media. They reported to Russian authorities and providers about attacks against Russian entities using Sitting Ducks. Their report is a special case of Sitting Ducks and coincides with early Vacant Viper activity.



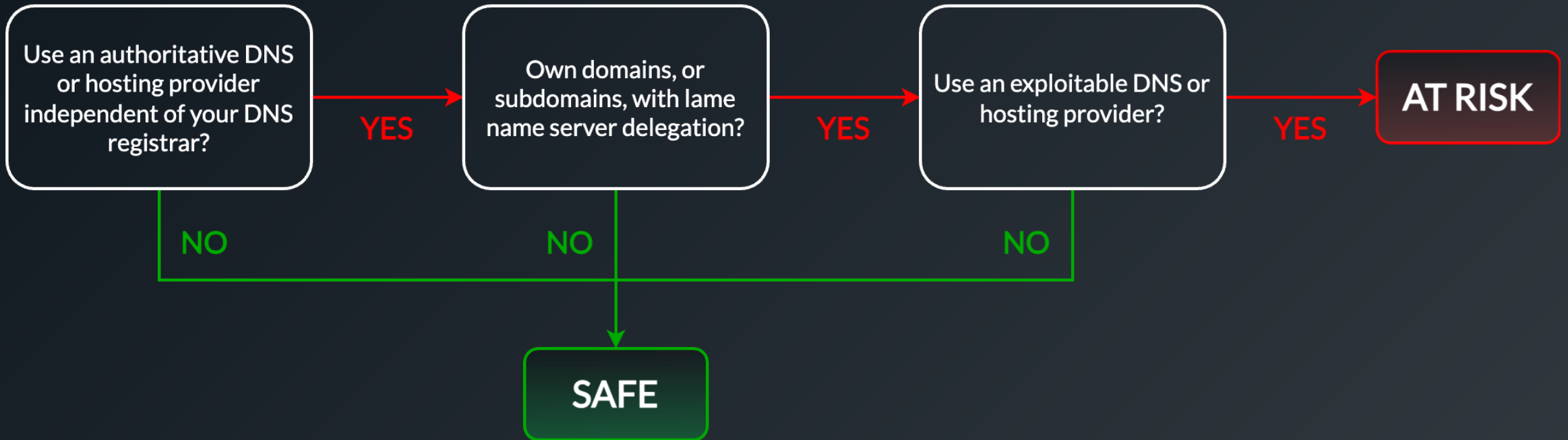


# WHO IS VULNERABLE?

528,070

Vulnerable domains

Are you at risk for a sitting duck attack? Do you:



Determining Your Risk

# PREVENTING LAME DELEGATION HIJACKS



Domain owners should audit and create delegations for all owned zones

- Create zone file config, or
- Change primary and secondary NS to the registrar's or use dummy placeholders



Providers use dynamically assigned NS from a large pool when adding a zone to a DNS provider

- Requires access to registrar to make sure they match



Registrar could test for lame delegations and modify NS records to placeholders

THANK YOU!



**Infoblox  
Threat Intel**

[www.infoblox.com/threat-intel/](http://www.infoblox.com/threat-intel/)

TALK TO US ON MASTODON  
[infobloxthreatintel@infosec.exchange](mailto:infobloxthreatintel@infosec.exchange)

GET OUR RESEARCH

