ATHENE
National Research Center for Applied Cybersecurity

TECHNISCHE UNIVERSITÄT DARMSTADT

Fraunhofer SIT

IONIX

GOETHE UNIVERSITÄT FRANKFURT AM MAIN

Cloudy with a Chance of Cyberattacks: Dangling Resources Abuse on Cloud Platforms

Jens Frieß, Tobias Gattermayer, Nethanel Gelernter, Haya Schulmann & Michael Waidner

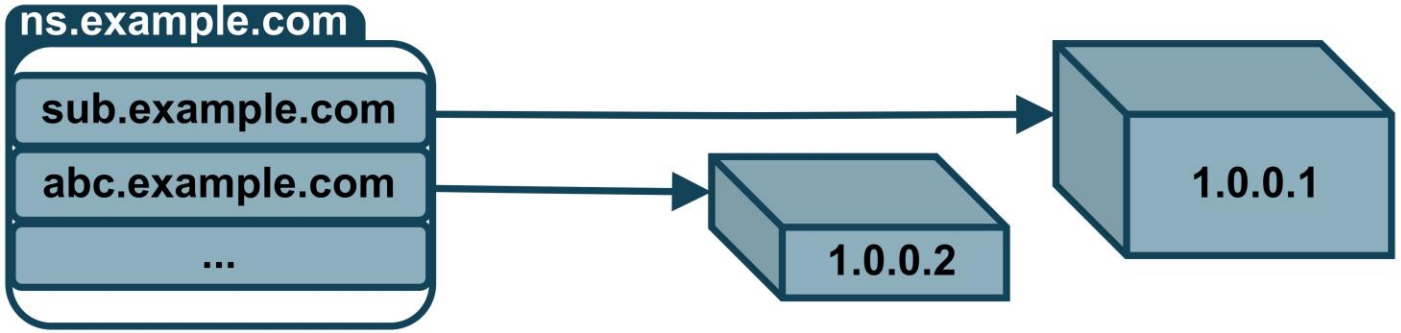
ATHENE | Fraunhofer SIT | Technische Universität Darmstadt | IONIX | Goethe-Universität Frankfurt

USENIX NSDI'24
Santa Clara, CA, USA - April 18th 2024

What Are Dangling DNS Records?

/ Dangling DNS / IP Lottery

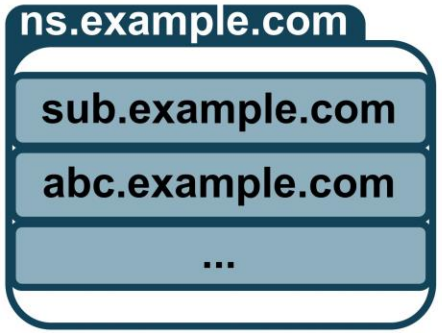
Domain example.com hosts services on subdomains sub, abc, etc. using IP addresses 1.0.0.1 and 1.0.0.2



What Are Dangling DNS Records?

/ Dangling DNS / IP Lottery

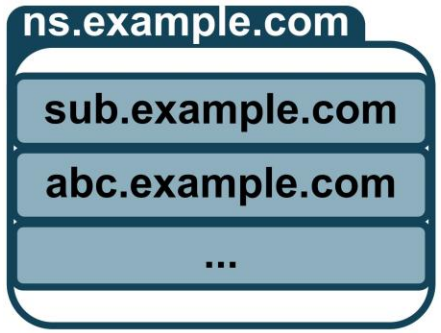
Domain example.com sets up a new service using a cloud provider



What Are Dangling DNS Records?

/ Dangling DNS / IP Lottery

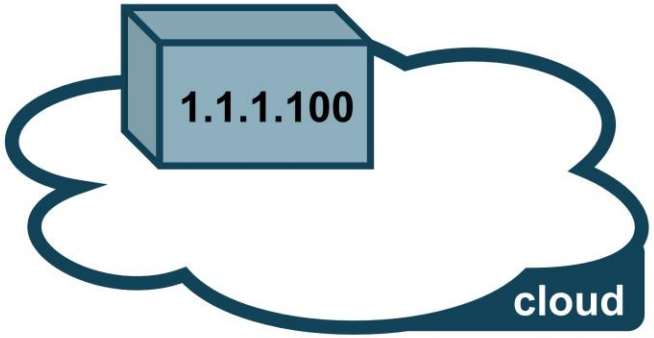
Domain example.com sets up a new service using a cloud provider

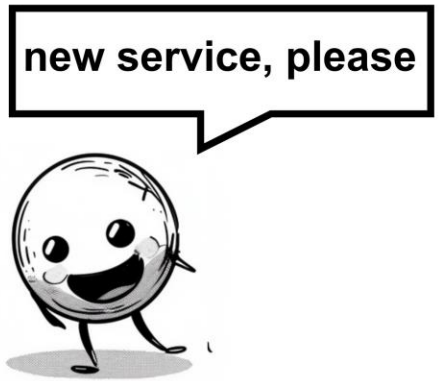


What Are Dangling DNS Records?

/ Dangling DNS / IP Lottery

The new resource is assigned the IP address
1.1.1.100

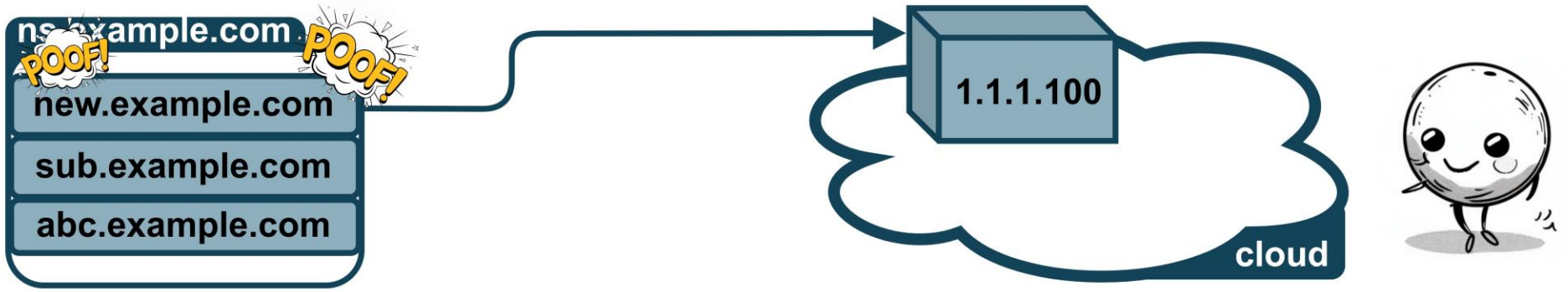




What Are Dangling DNS Records?

/ Dangling DNS / IP Lottery

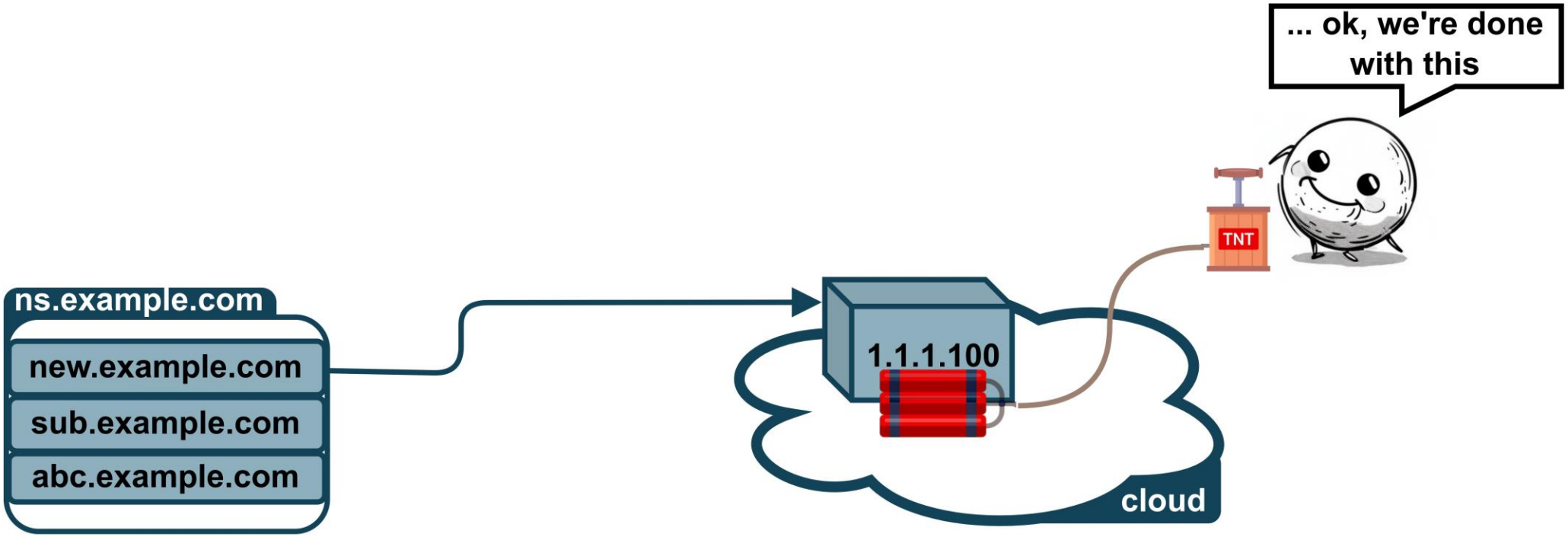
Domain owner creates new DNS record new.example.com,
resolving to 1.1.1.100



What Are Dangling DNS Records?

/ Dangling DNS / IP Lottery

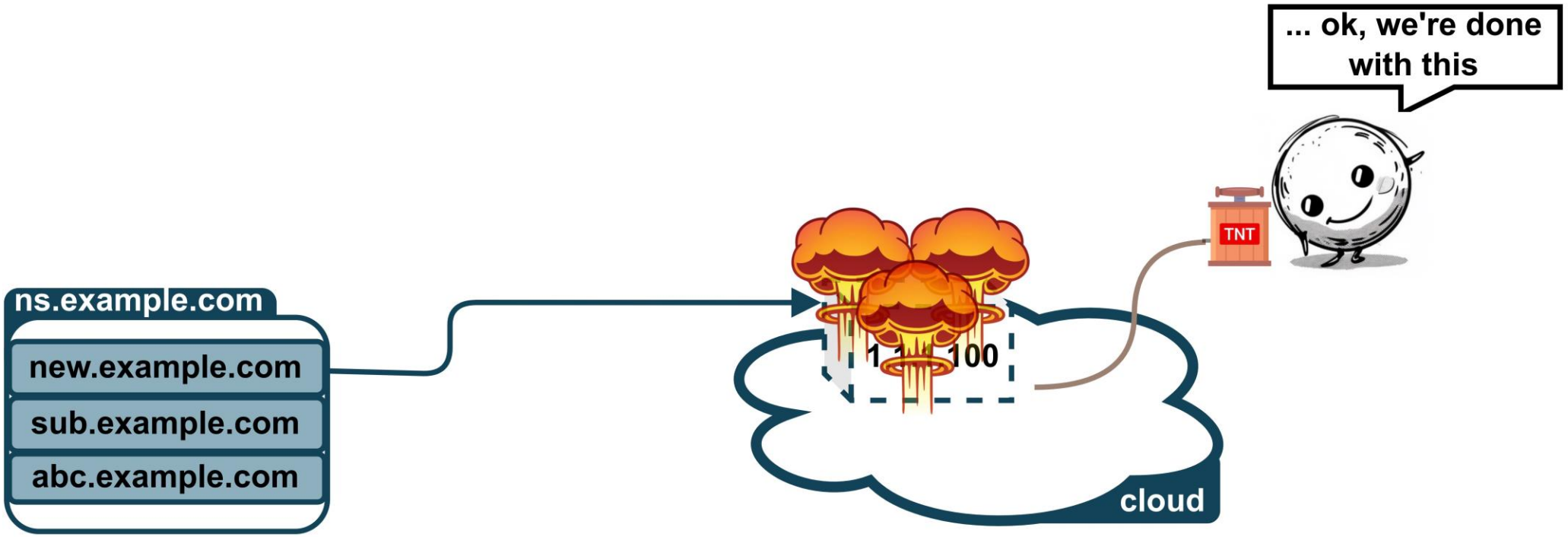
Domain owner releases the cloud resource at
1.1.1.100



What Are Dangling DNS Records?

/ Dangling DNS / IP Lottery

Domain owner releases the cloud resource at
1.1.1.100



What Are Dangling DNS Records?

/ Dangling DNS / IP Lottery

Domain owner forgets to purge DNS record for new.example.com

What Are Dangling DNS Records?

/ Dangling DNS / IP Lottery

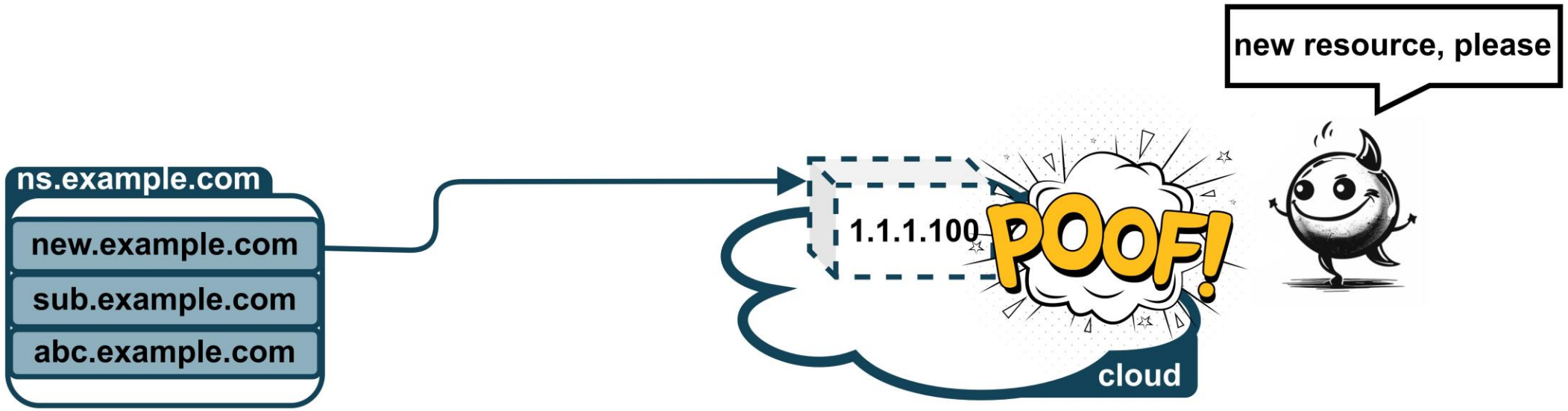
Domain owner forgets to purge DNS record for new.example.com

Attacker sees public DNS record resolving to cloud IP

What Are Dangling DNS Records?

/ Dangling DNS / IP Lottery

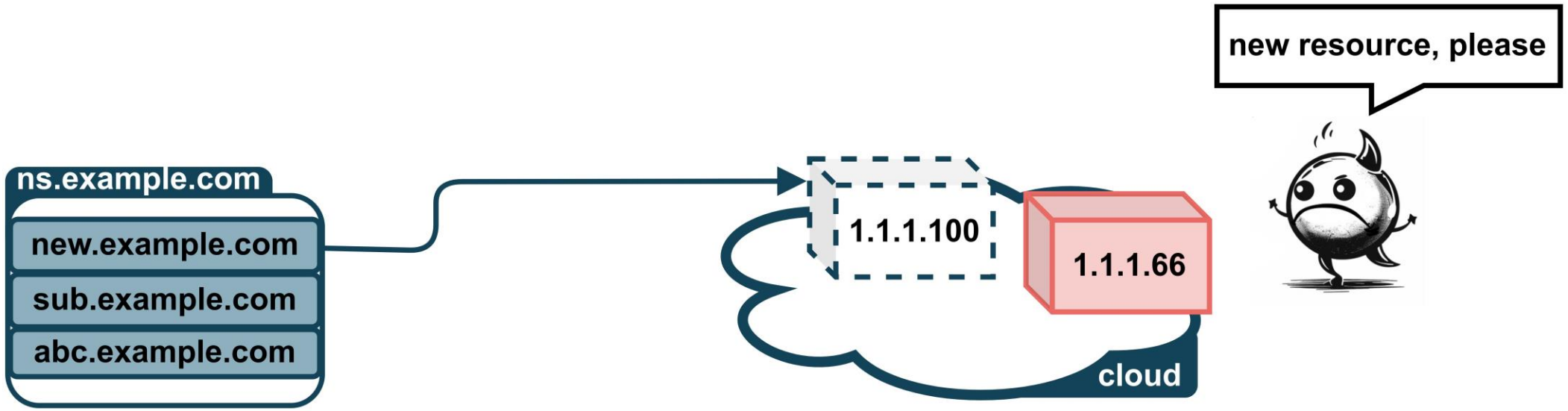
Attacker creates cloud resources, hoping to be assigned 1.1.1.100



What Are Dangling DNS Records?

/ Dangling DNS / IP Lottery

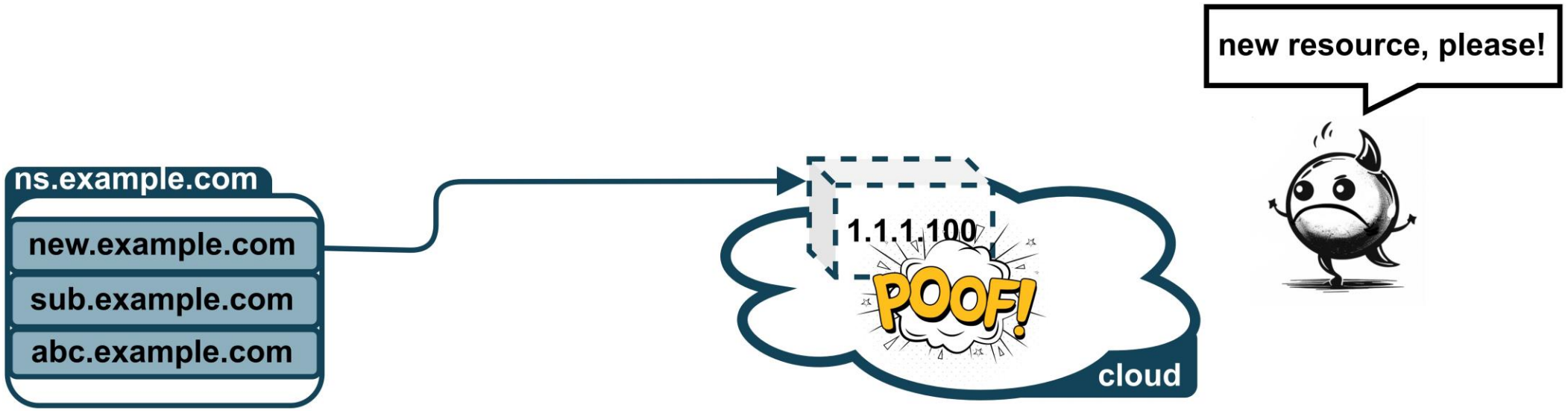
Attacker creates cloud resources, hoping to be assigned 1.1.1.100



What Are Dangling DNS Records?

/ Dangling DNS / IP Lottery

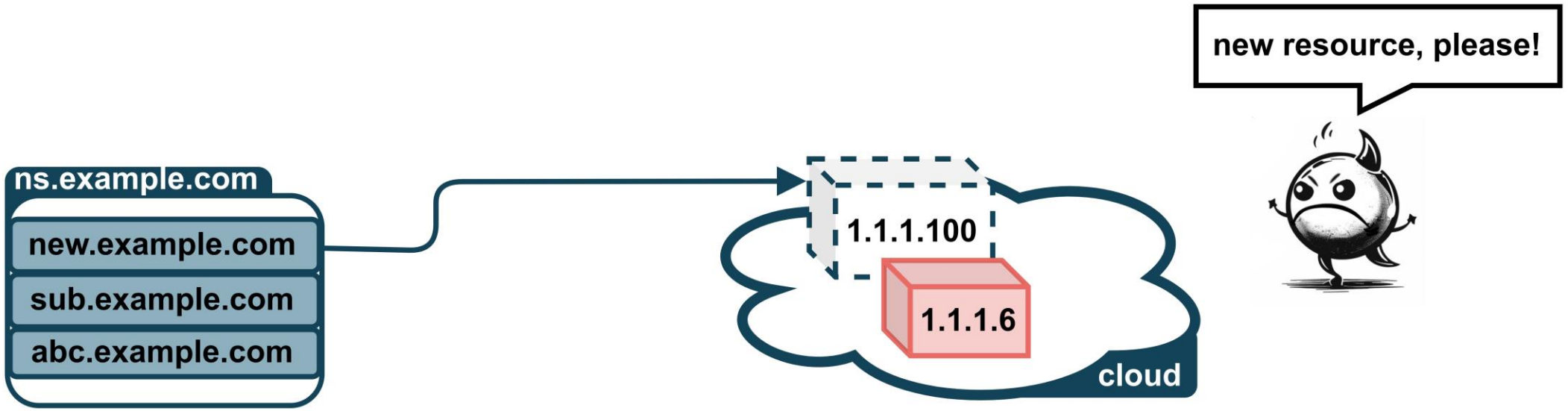
Attacker creates cloud resources, hoping to be assigned 1.1.1.100



What Are Dangling DNS Records?

/ Dangling DNS / IP Lottery

Attacker creates cloud resources, hoping to be assigned 1.1.1.100



What Are Dangling DNS Records?

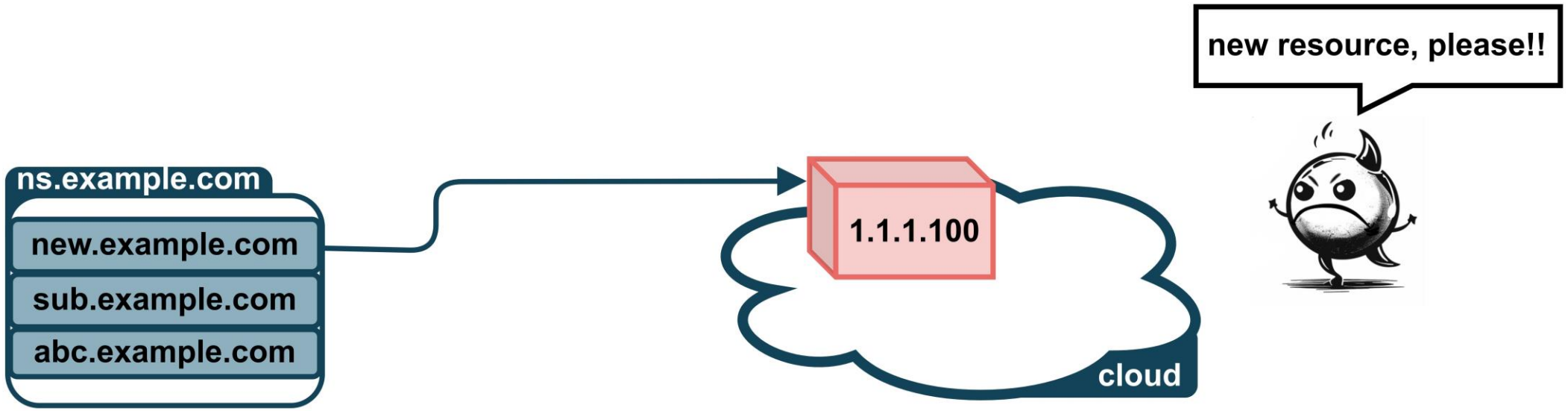
/ Dangling DNS / IP Lottery

Attacker creates cloud resources, hoping to be assigned 1.1.1.100

What Are Dangling DNS Records?

/ Dangling DNS / IP Lottery

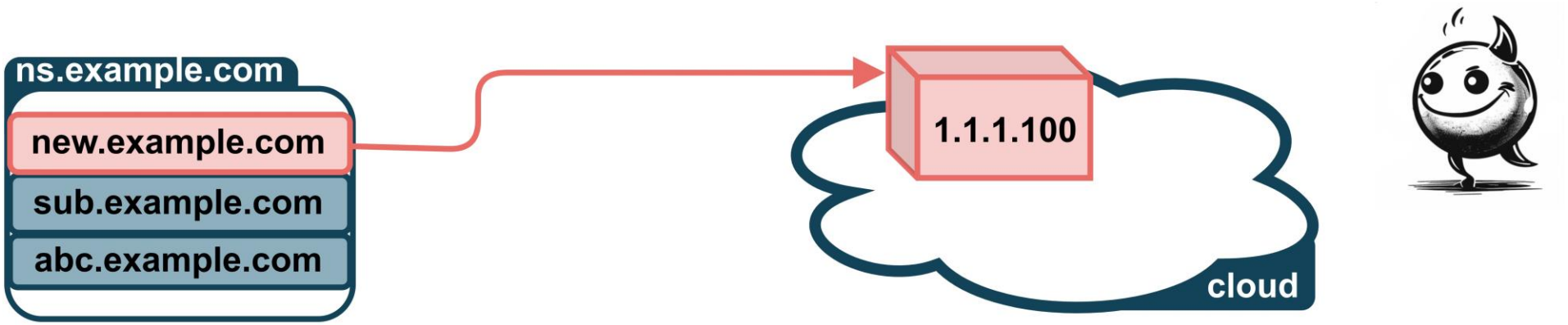
Attacker creates cloud resources, hoping to be assigned 1.1.1.100



What Are Dangling DNS Records?

/ Dangling DNS / IP Lottery

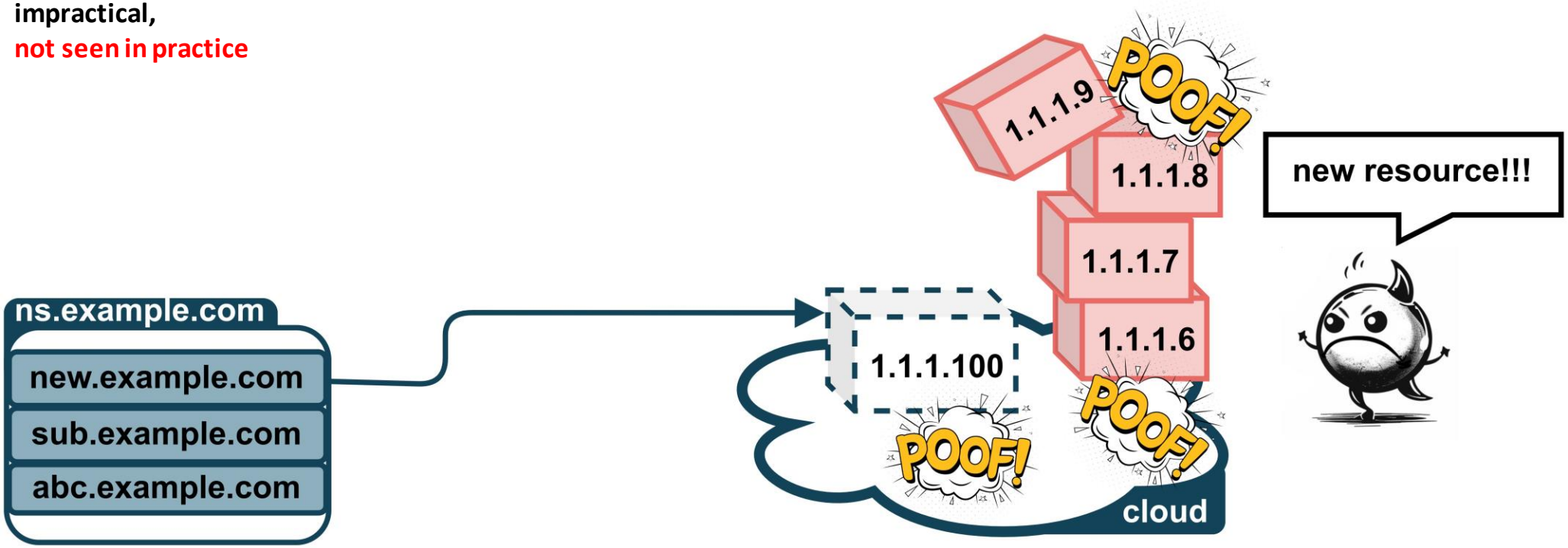
new.example.com successfully resolves to attacker-controlled resource / content



Takeaway 1: Attackers Don't Play IP Lottery

/ Dangling DNS / IP Lottery

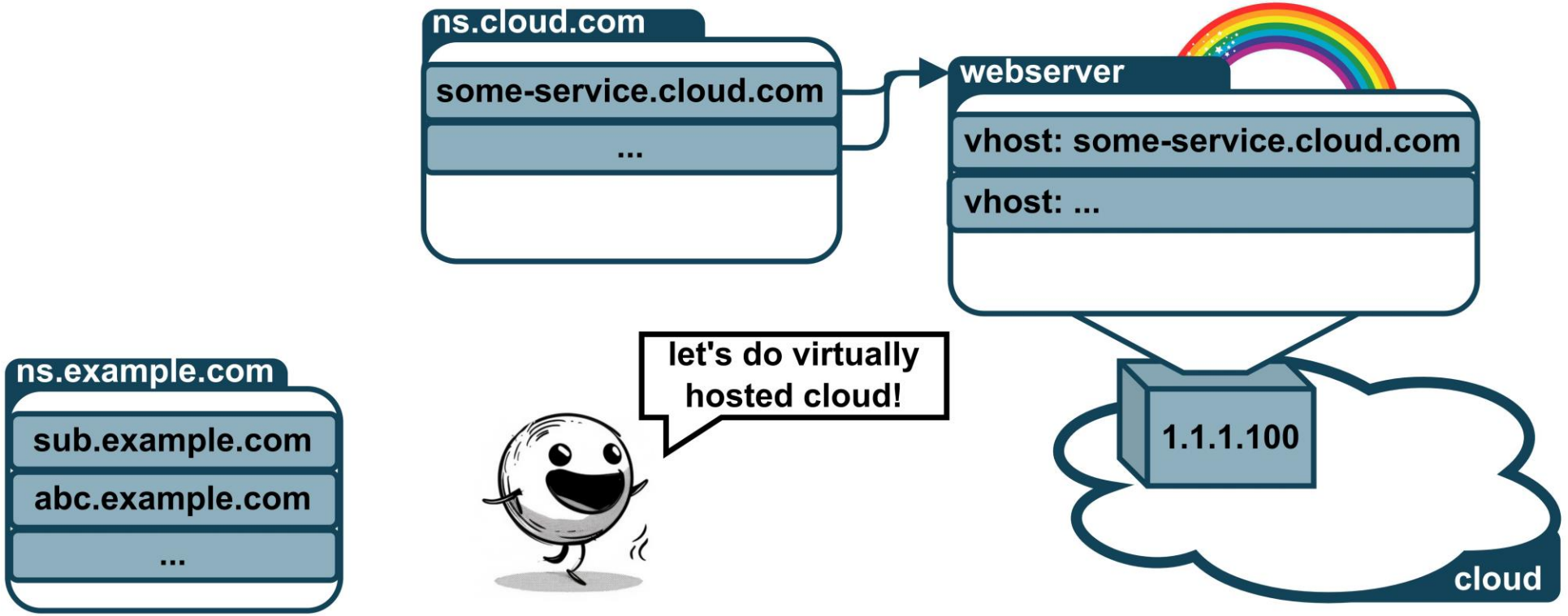
Theorized, but…
inefficient,
impractical,
not seen in practice



Going After Virtually Hosted Resources

/ Dangling DNS / Virtual Hosting

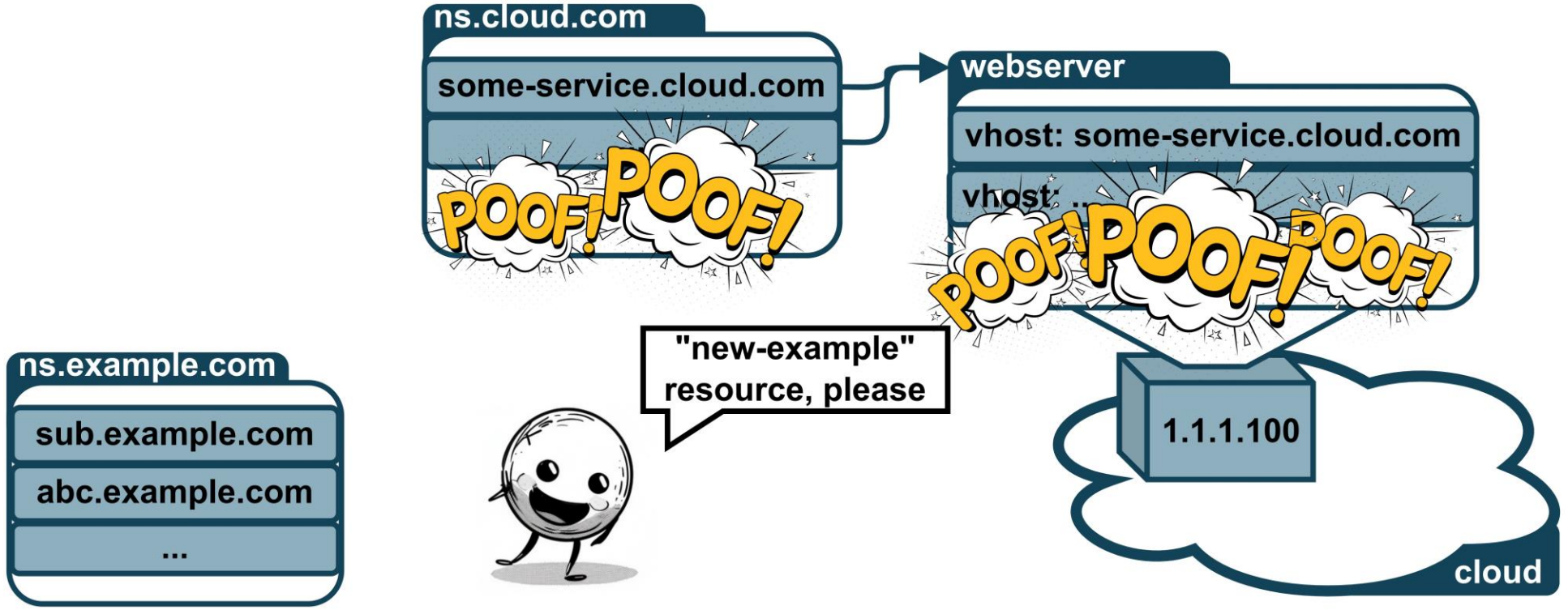
Virtually hosted resources addressed via hostname



Going After Virtually Hosted Resources

/ Dangling DNS / Virtual Hosting

Domain owner creates resource
new-example

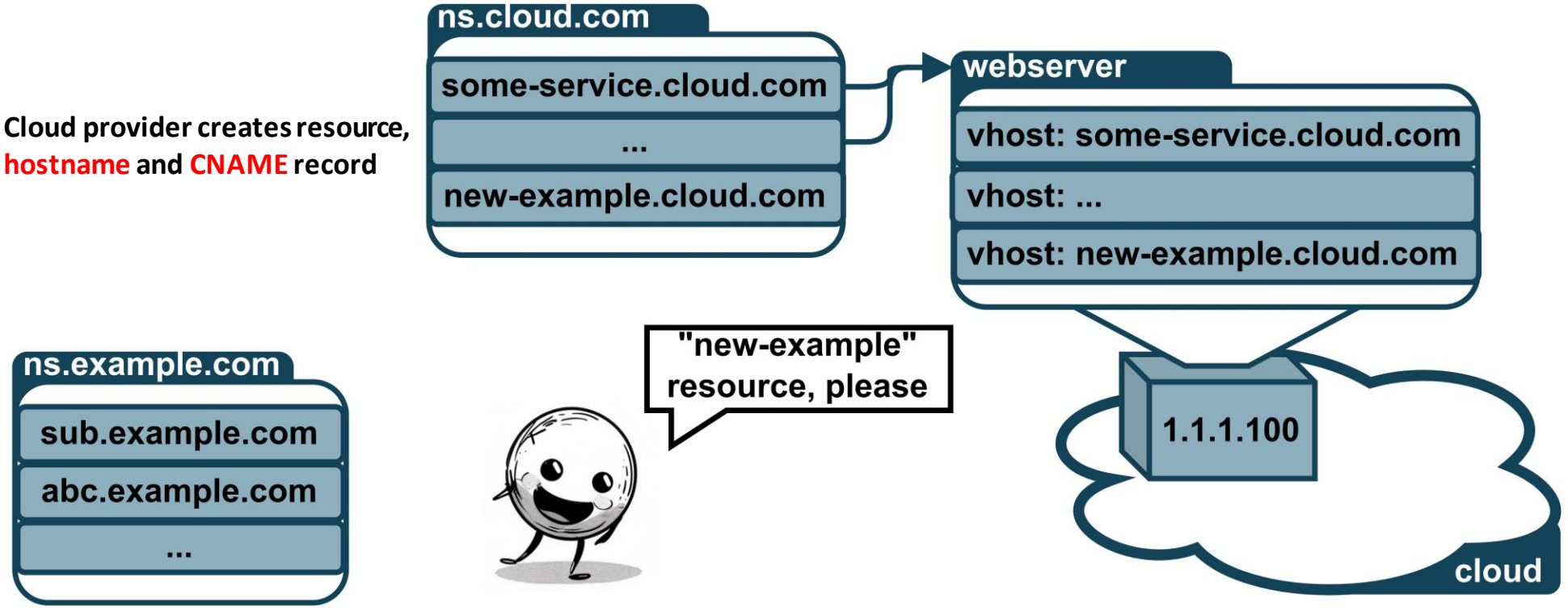


Going After Virtually Hosted Resources

/ Dangling DNS / Virtual Hosting

Domain owner creates resource
new-example

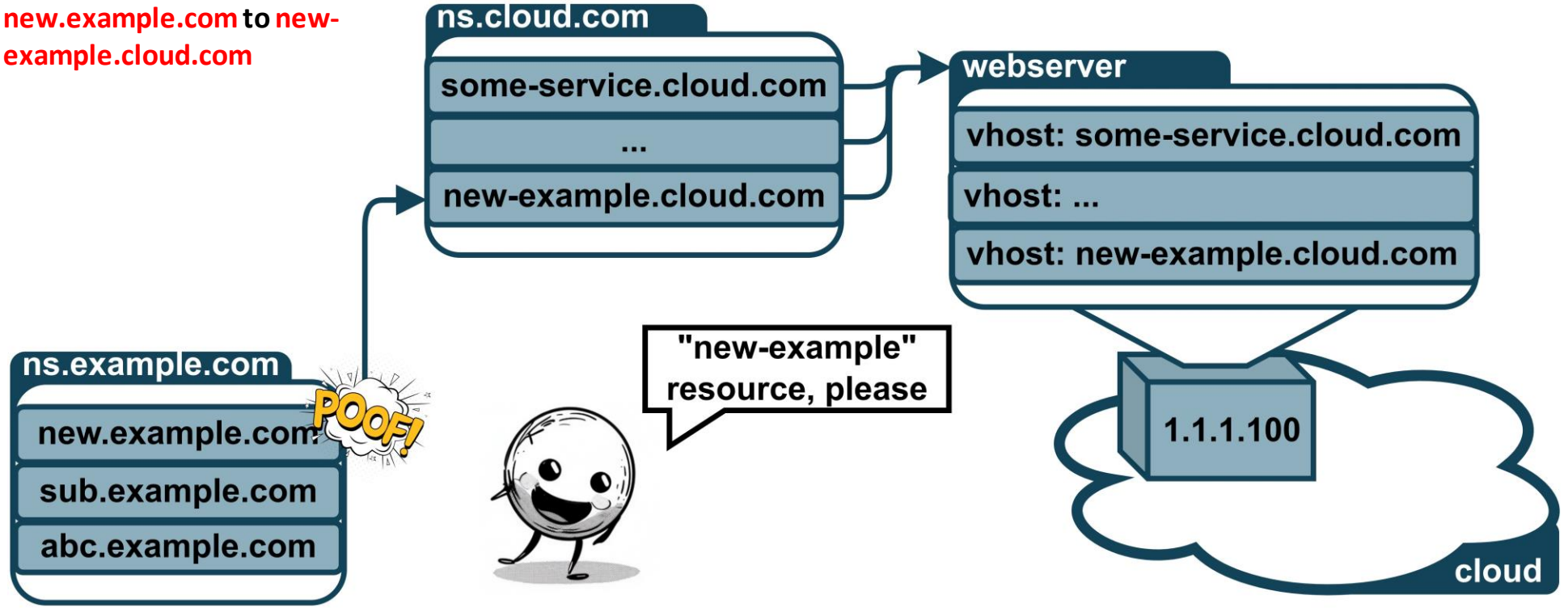
Cloud provider creates resource,
hostname and CNAME record



Going After Virtually Hosted Resources

/ Dangling DNS / Virtual Hosting

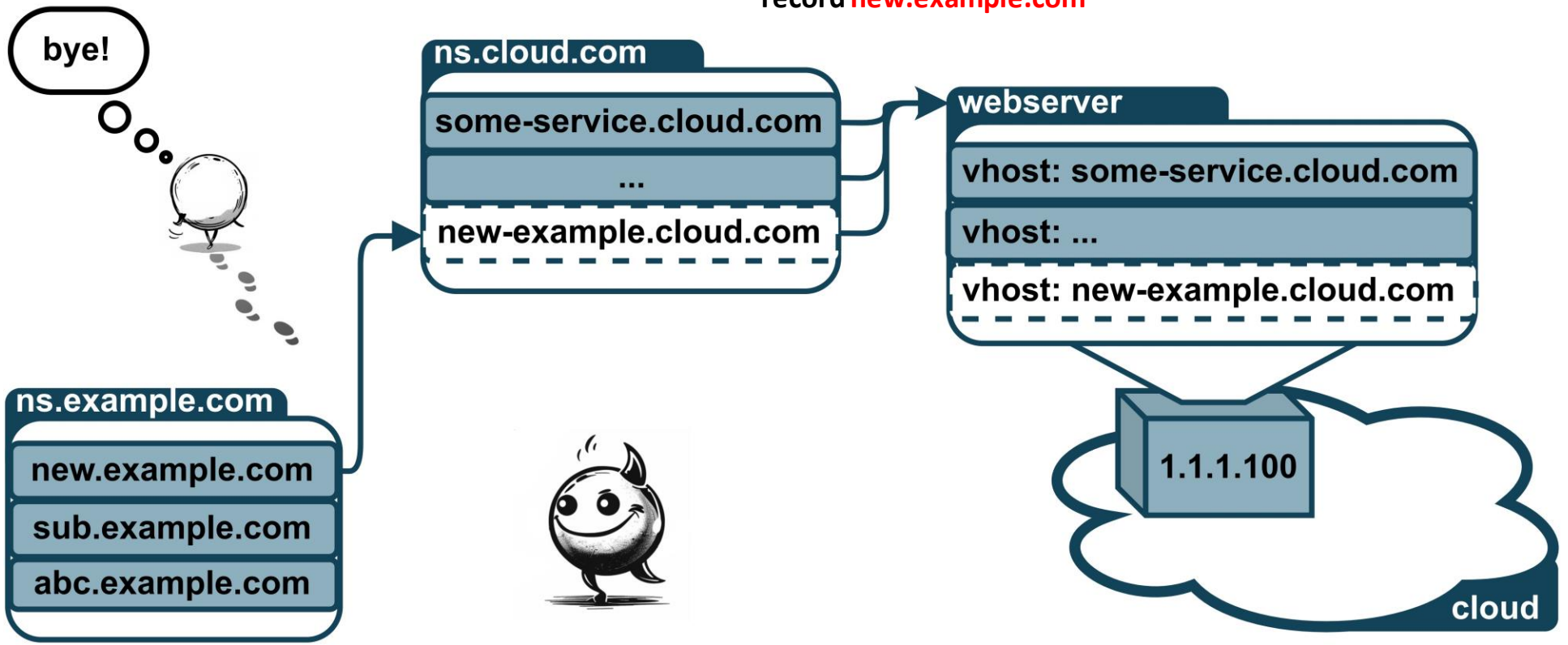
Domain owner creates CNAME record, resolving new.example.com to new-example.cloud.com



Going After Virtually Hosted Resources

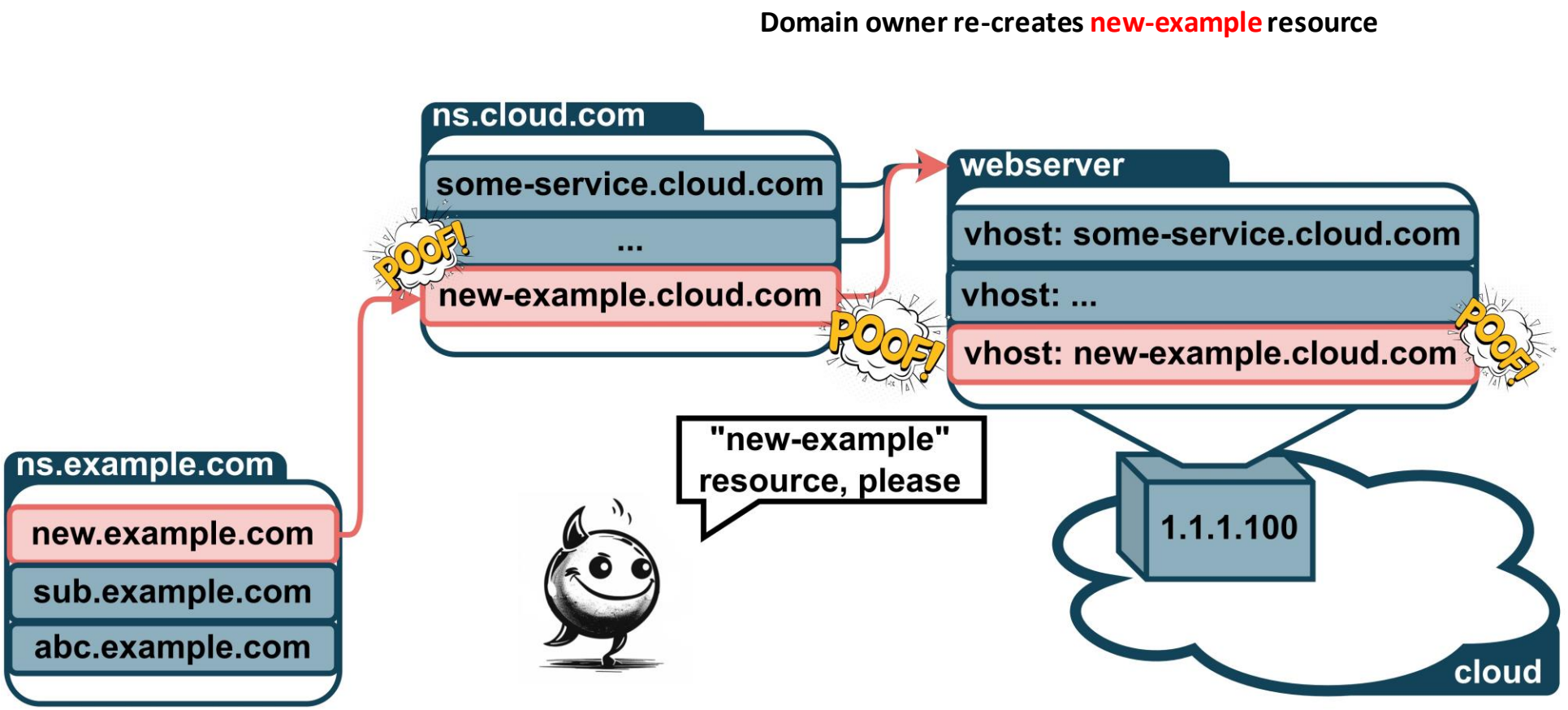
/ Dangling DNS / Virtual Hosting

Domain owner releases cloud resource, but forgets to purge DNS record new.example.com



Going After Virtually Hosted Resources

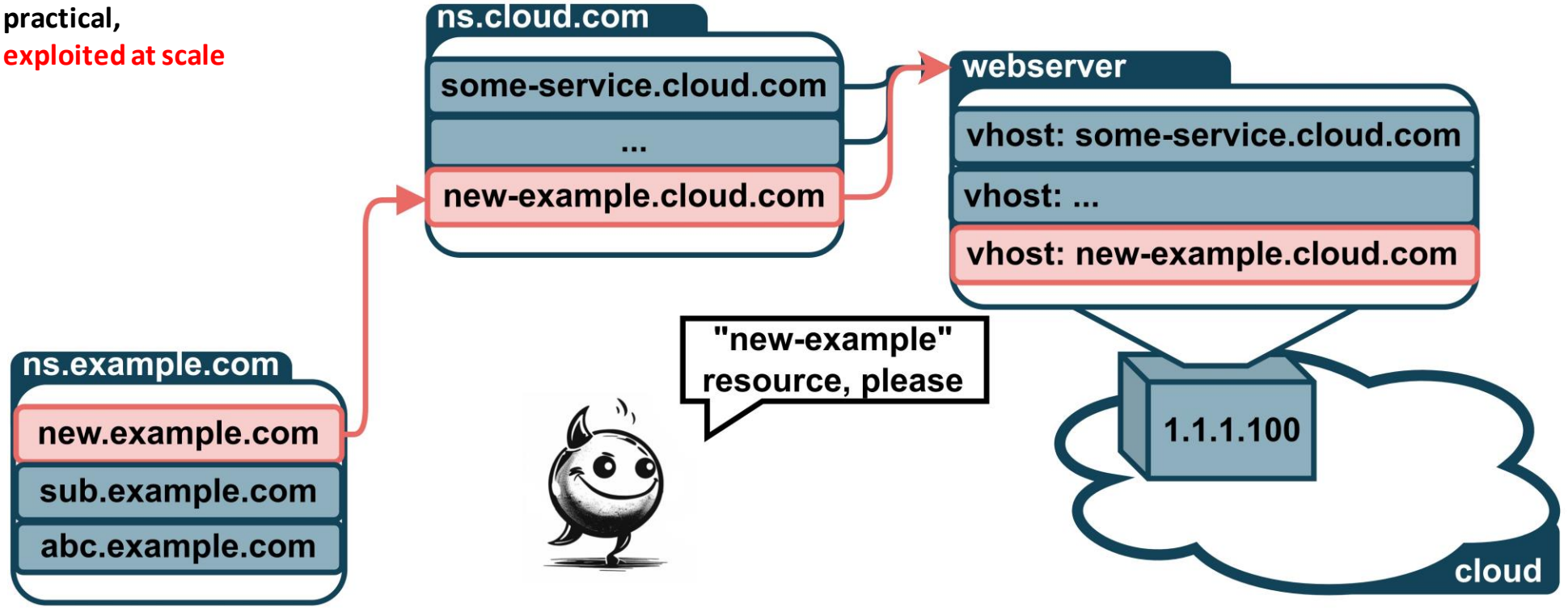
/ Dangling DNS / Virtual Hosting



Going After Virtually Hosted Resources

/ Dangling DNS / Virtual Hosting

Deterministic,
efficient,
practical,
exploited at scale

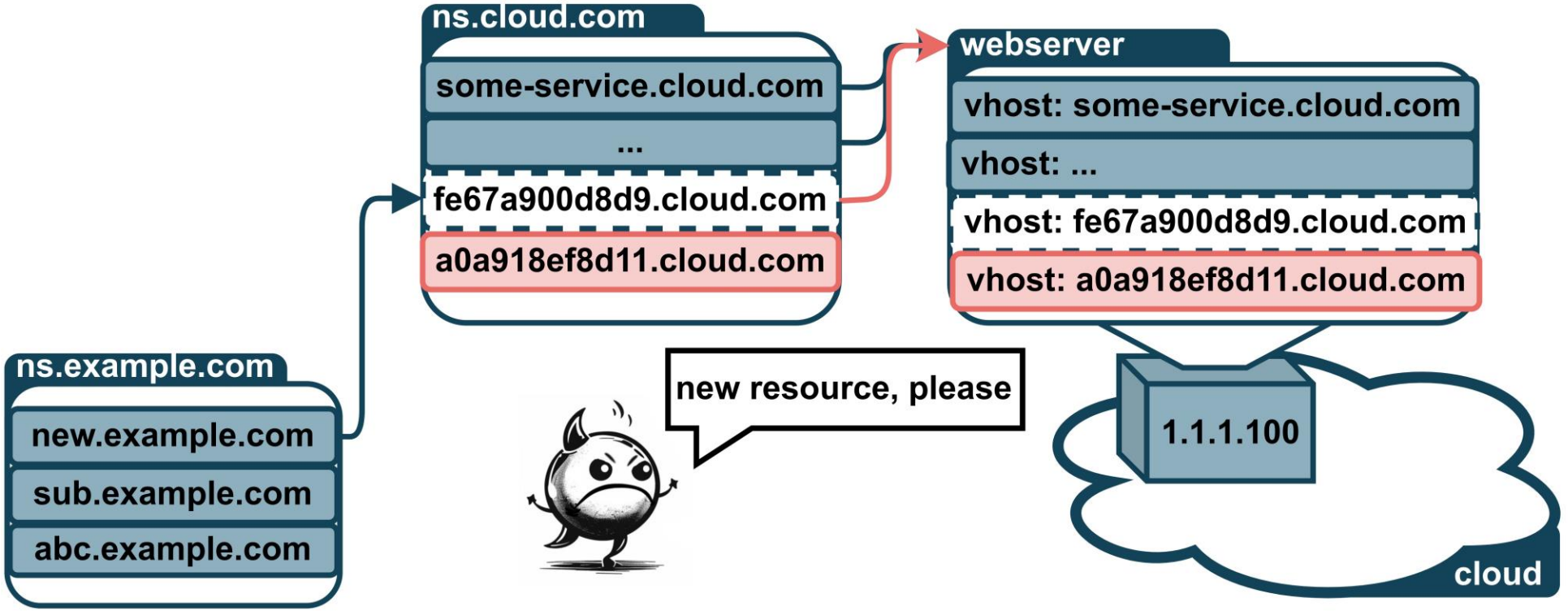


Takeaway 2: Randomize Virtual Hostnames!

/ Dangling DNS / Virtual Hosting

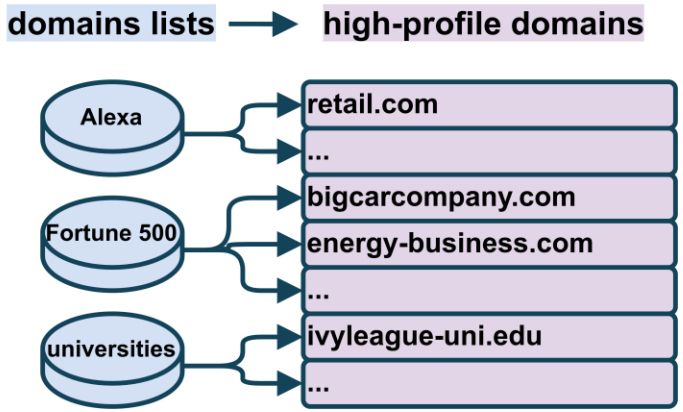
see Google cloud

not exploited



Hunting for Real-World Exploitation

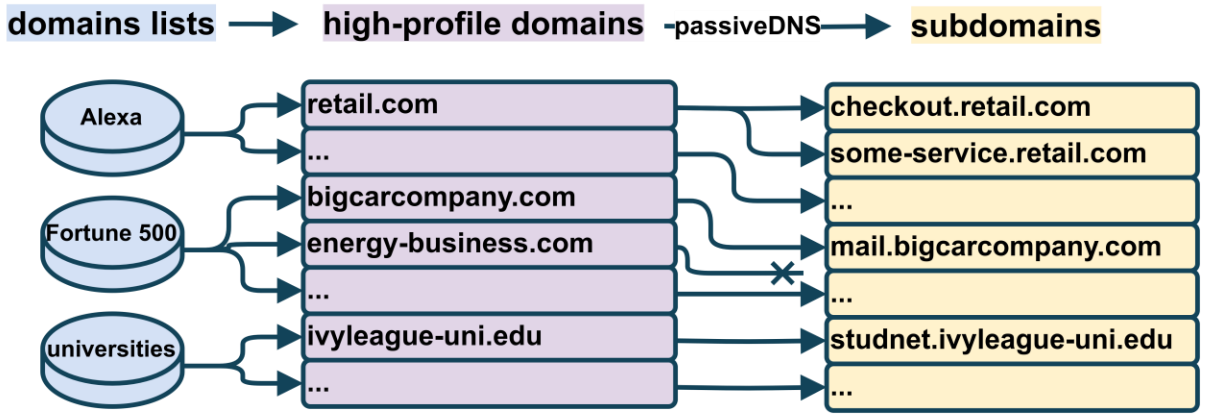
/ Methodology / Domain Collection



collect high-profile domains from well-known sources

Hunting for Real-World Exploitation

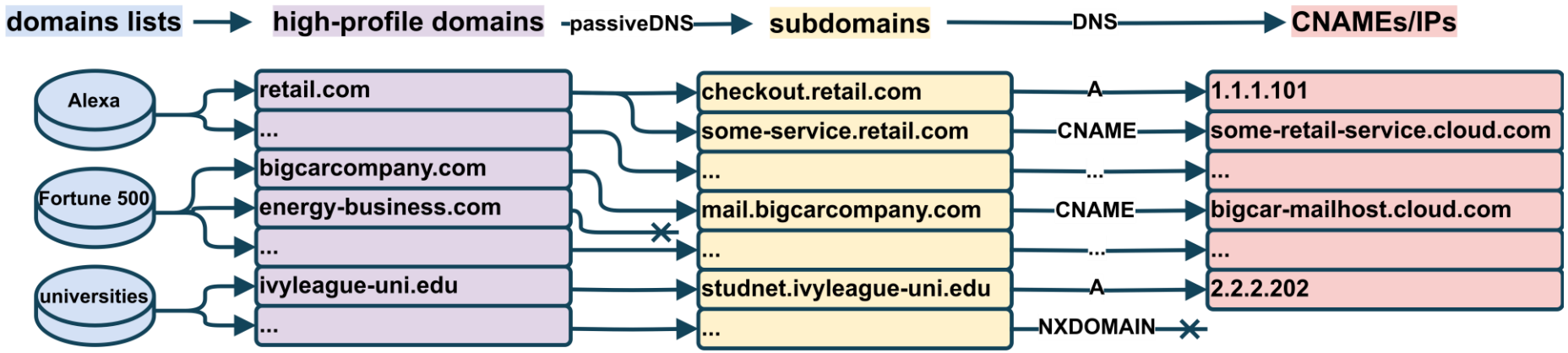
/ Methodology / Domain Collection



find active subdomains for high-profile domains

Hunting for Real-World Exploitation

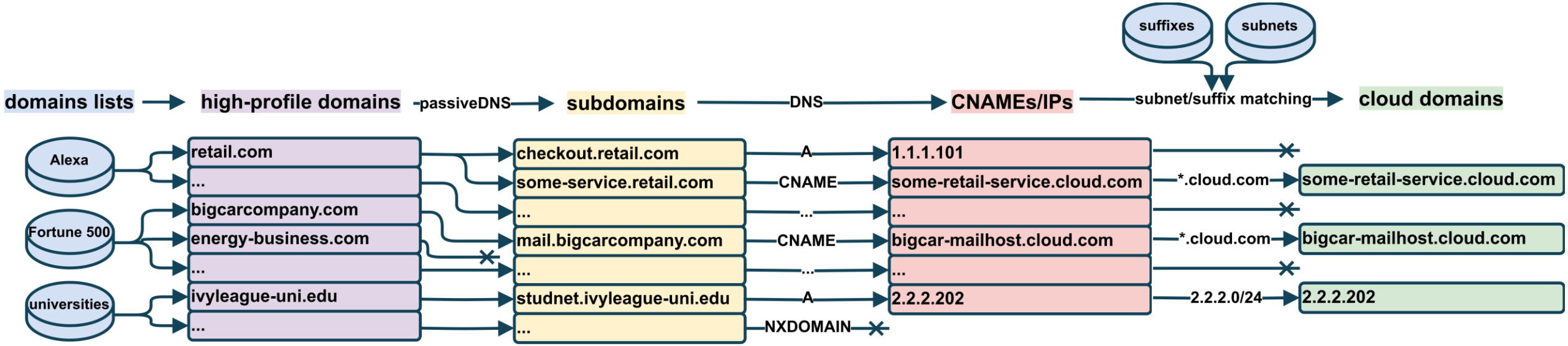
/ Methodology / Domain Collection



determine IPs & CNAMEs of active subdomains

Hunting for Real-World Exploitation

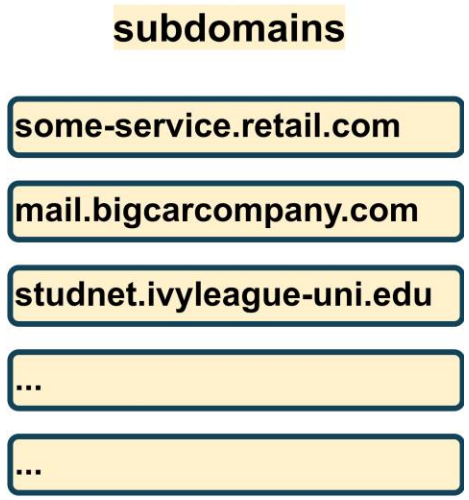
/ Methodology / Domain Collection



determine IPs in known cloud subnets & CNAMEs matching known cloud suffixes

Hunting for Real-World Exploitation

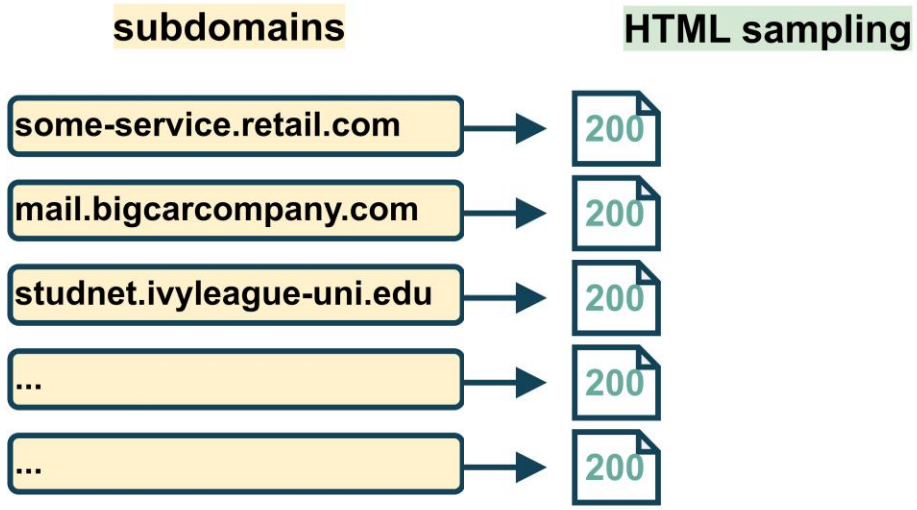
/ Methodology / Hijack Detection



subdomains linked to cloud

Hunting for Real-World Exploitation

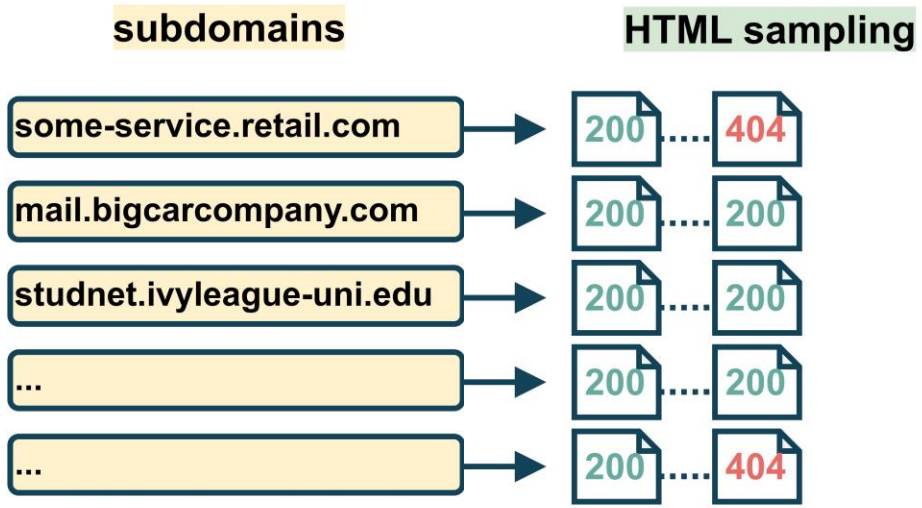
/ Methodology / Hijack Detection



periodically download HTML to track content over time

Hunting for Real-World Exploitation

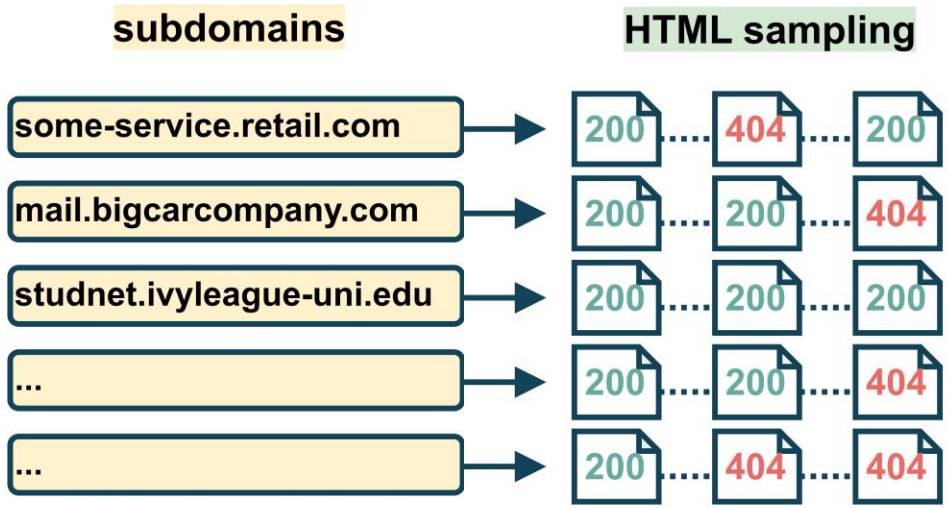
/ Methodology / Hijack Detection



periodically download HTML to track content over time

Hunting for Real-World Exploitation

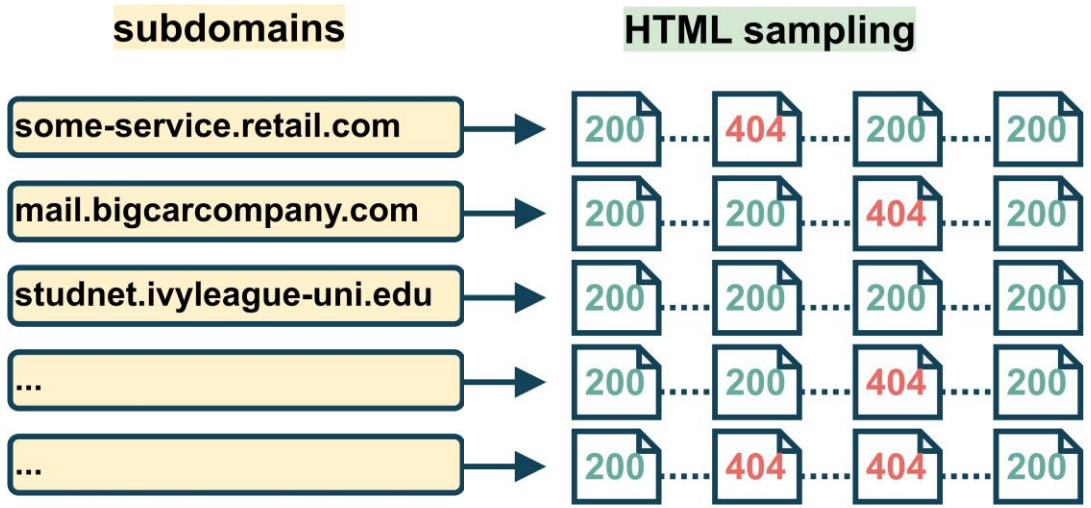
/ Methodology / Hijack Detection



periodically download HTML to track content over time

Hunting for Real-World Exploitation

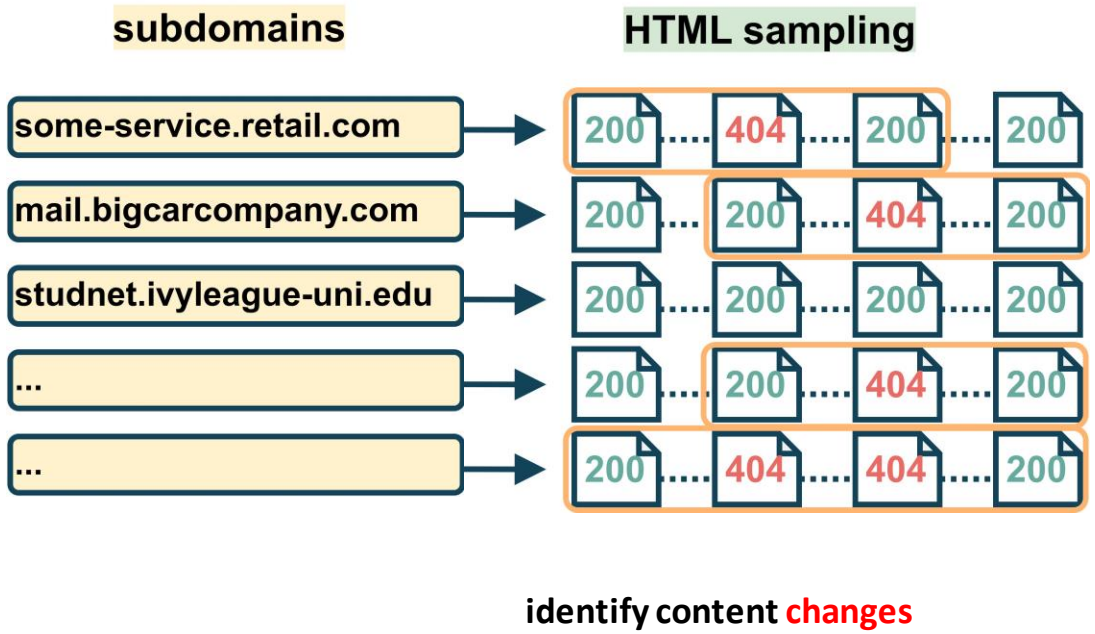
/ Methodology / Hijack Detection



periodically download HTML to track content over time

Hunting for Real-World Exploitation

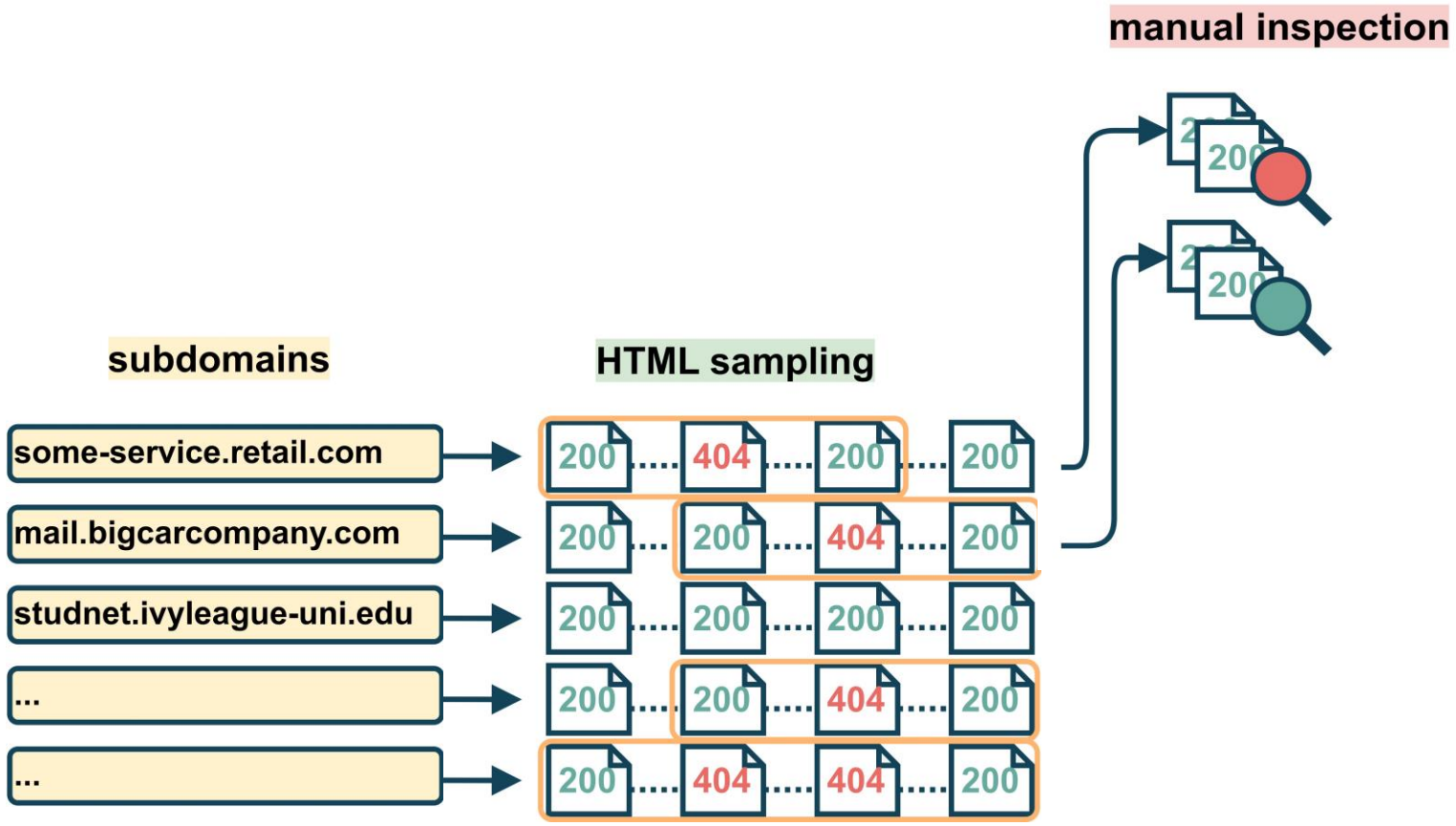
/ Methodology / Hijack Detection



identify content changes

Hunting for Real-World Exploitation

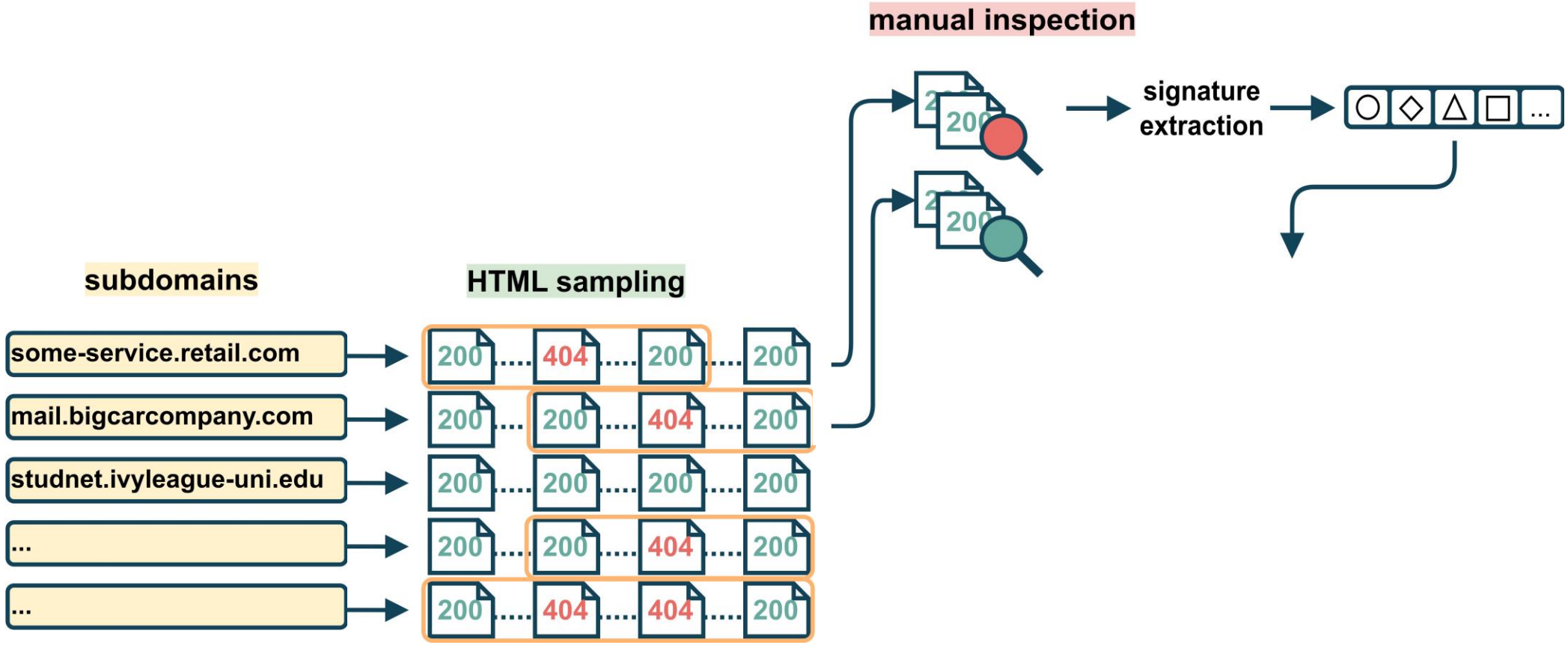
/ Methodology / Hijack Detection



manually verify malicious content on selected pages

Hunting for Real-World Exploitation

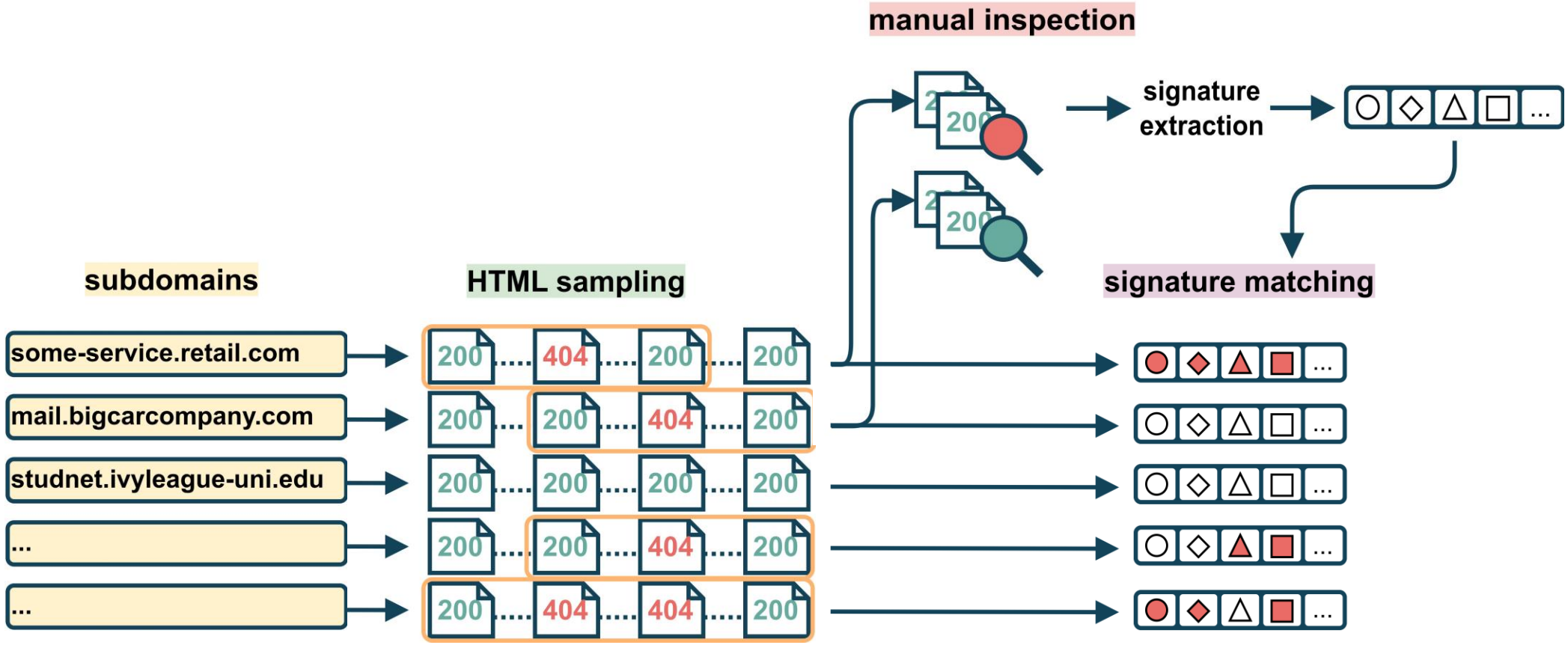
/ Methodology / Hijack Detection



create signatures of malicious content (e.g. keywords, sitemap size, ...)

Hunting for Real-World Exploitation

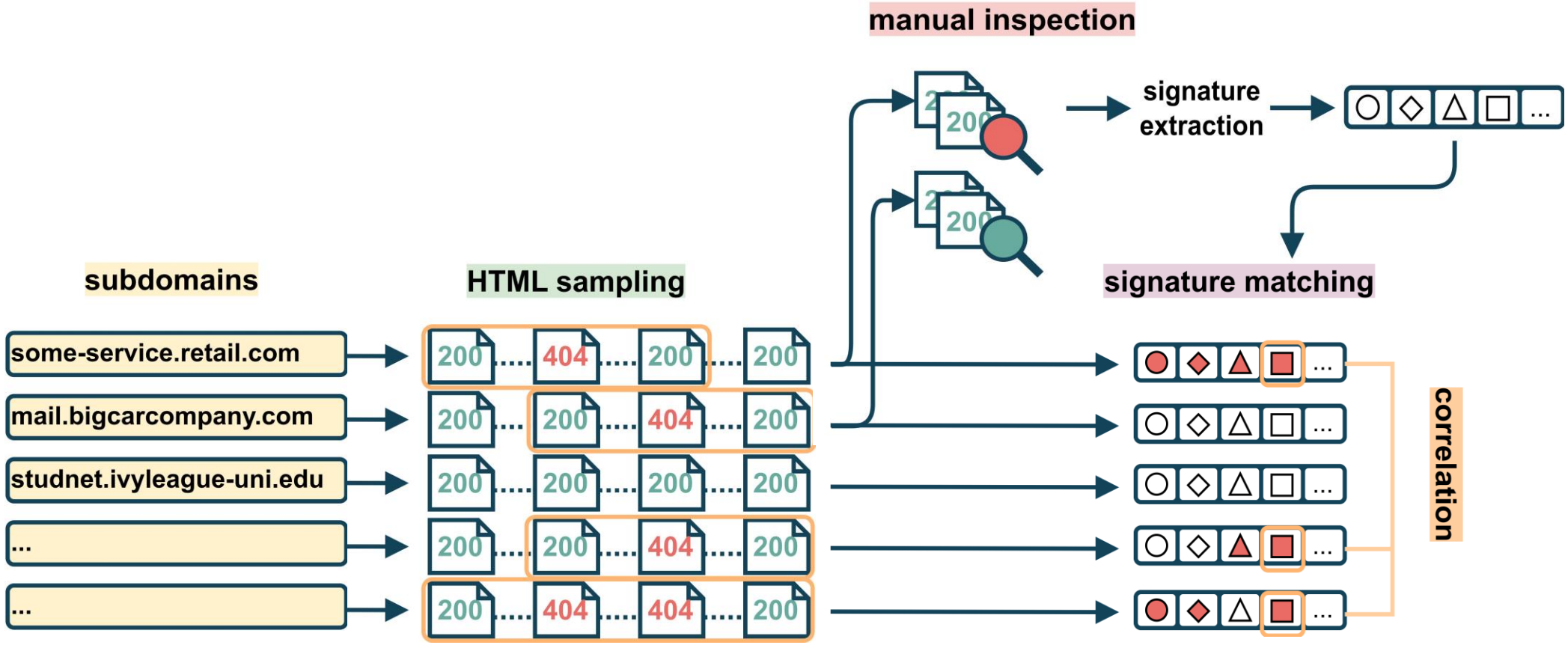
/ Methodology / Hijack Detection



match signatures with other samples

Hunting for Real-World Exploitation

/ Methodology / Hijack Detection

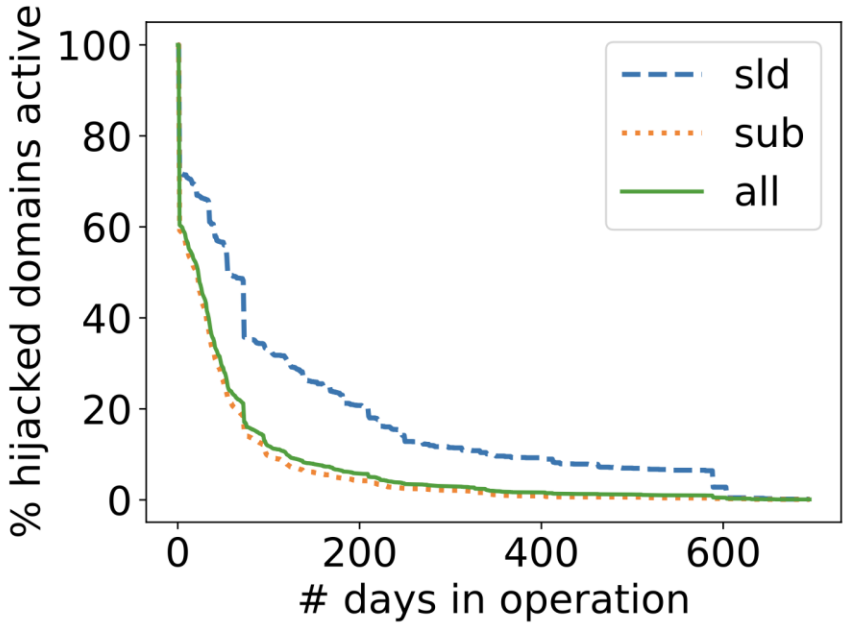


correlate signature matches across domains

Facts & Figures

/ Results / Domains & Dataset

- **3 year study** from **1.5M** to **3.1M** FQDNs that point to cloud FQDNs via A or CNAME.
- **17 698** abused dangling records in **31%** of Fortune 500 companies and **25.4%** of Global 500 companies.
- **1 565** Second- Level Domains and **218** top-level domains affected.
- Abuse duration: **15** days > **1** year.



Facts & Figures

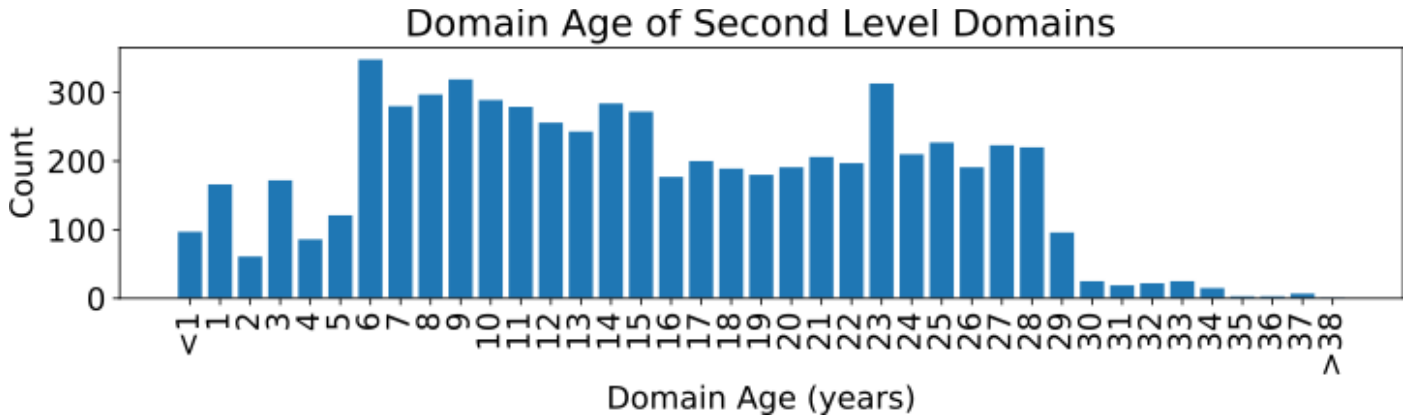
/ Results / Content Analysis

- **500M / 25.8TB** total files uploaded, with an average of **31 810** HTML files per abused FQDN
- **54 325** HTML index.html samples downloaded, **22%** were WordPress blogs.
- **56 946** keywords, **~3** keywords used to classify HTML index page as abused.
- **792** unique WhatsApp phone numbers
- **1 884** unique Telegram, Twitter, Instagram and Facebook handles
- **2 671** unique forwarding links provided by URL shortening services

What Do Attackers Use Hijacked Domains For?

/ Results / Content Analysis / Blackhat SEO

- Domain Age
- Keyword Stuffing
- SSL/TLS Certificate Creation
- Private Link Networks with Cloaking
- Click-Jacking
- Doorway Pages



#	Keyword	Count	#	Keyword	Count
1	slot	144,108	2	online	77,669
3	judi (gambling)	60,521	4	situs (website)	35,265
5	joker123	23,630	6	terpercaya (trusted)	19,407
7	gacor (hot streak)	18,006	8	agen (agent)	16,939
9	daftar (register)	12,881	10	game	12,113
11	bola (football)	11,688	12	pulsa (credit)	10,467

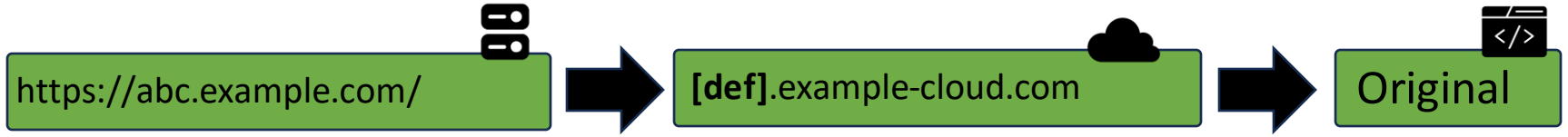
Overlay Ad Networks for Indonesian Gambling

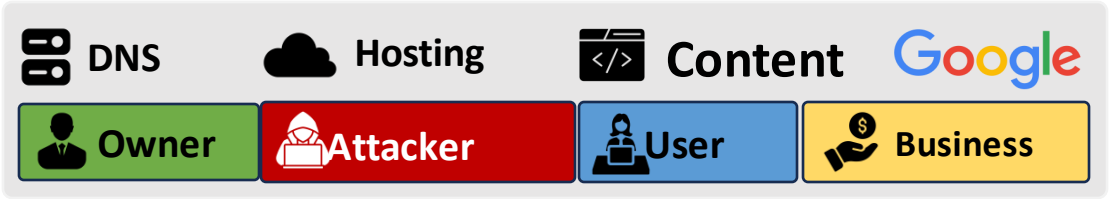
/ Results / Content Analysis / Example

- Both gambling & promoting gambling are **illegal** in Indonesia.
- The inherent reputation of hijacked domains enables **advertising illegal content**.
- We observe an infrastructure for **fraudulent traffic referral.**

How To Monetize Hijacked Domains

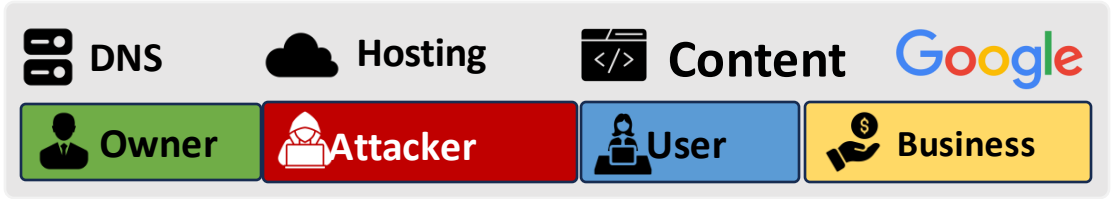
/ Results / Content Analysis / Monetization





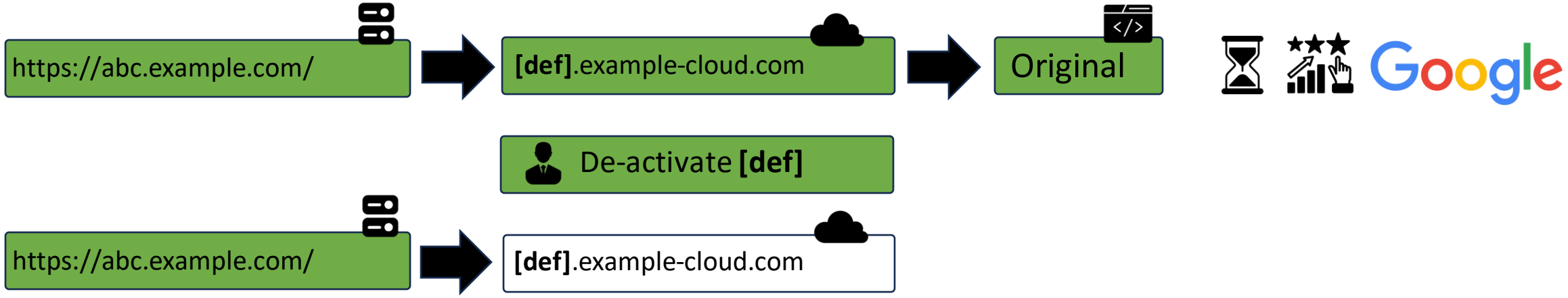
How To Monetize Hijacked Domains

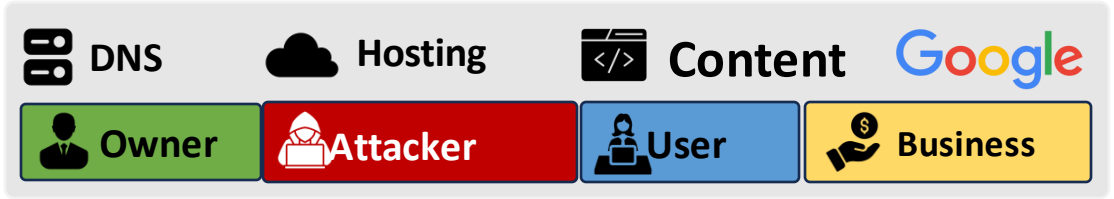
/ Results / Content Analysis / Monetization



How To Monetize Hijacked Domains

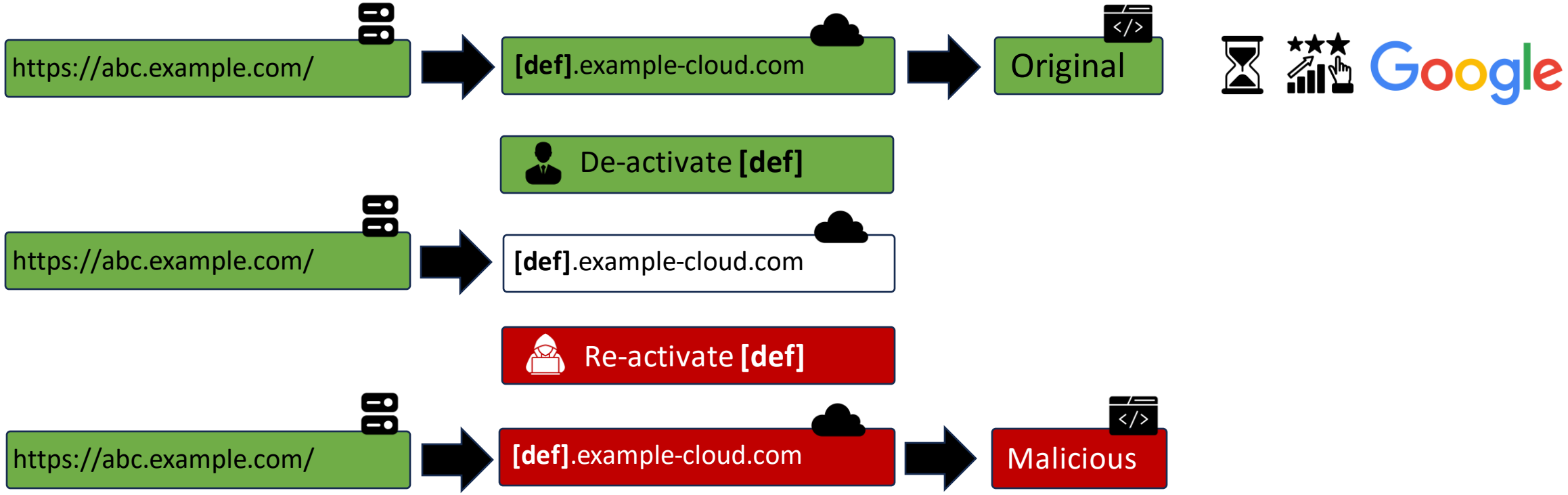
/ Results / Content Analysis / Monetization

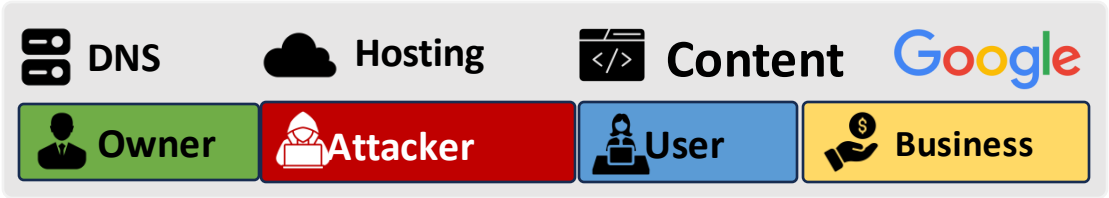




How To Monetize Hijacked Domains

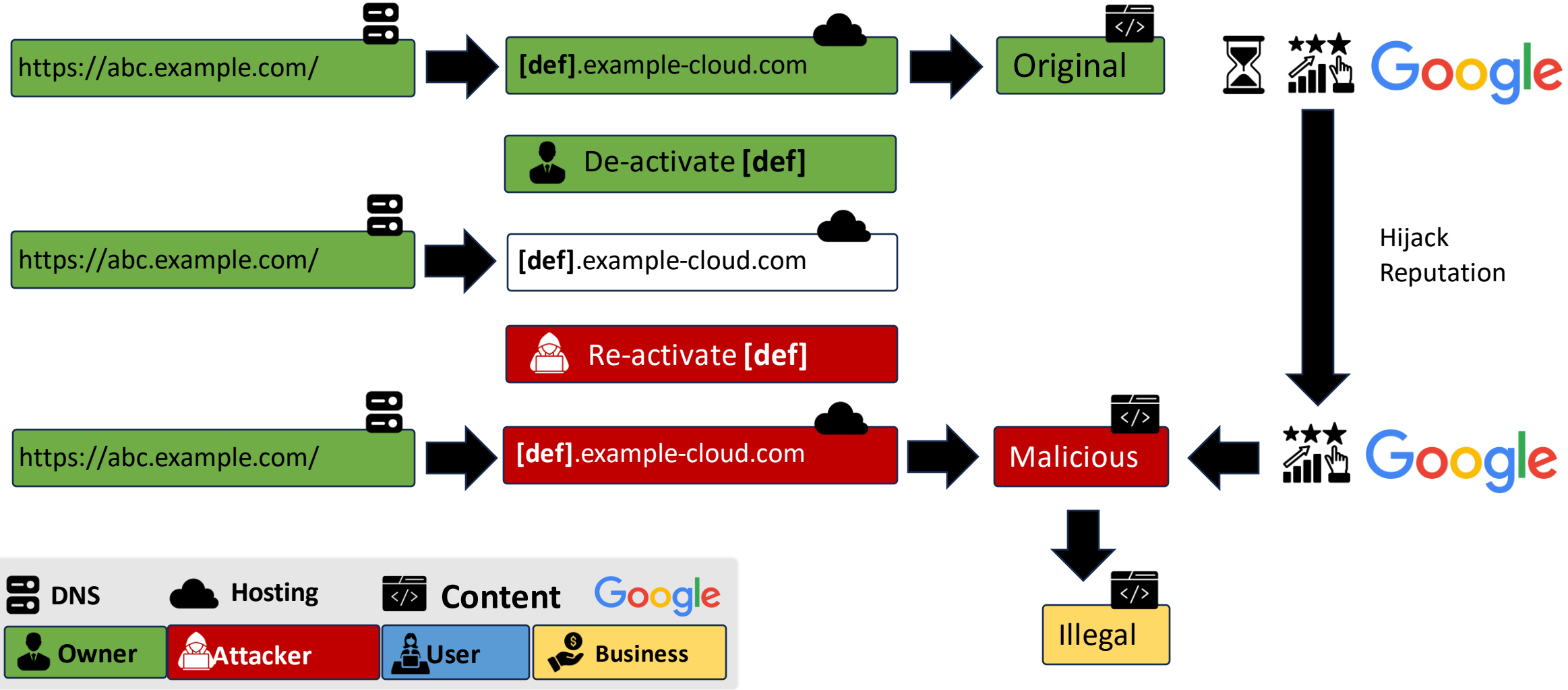
/ Results / Content Analysis / Monetization





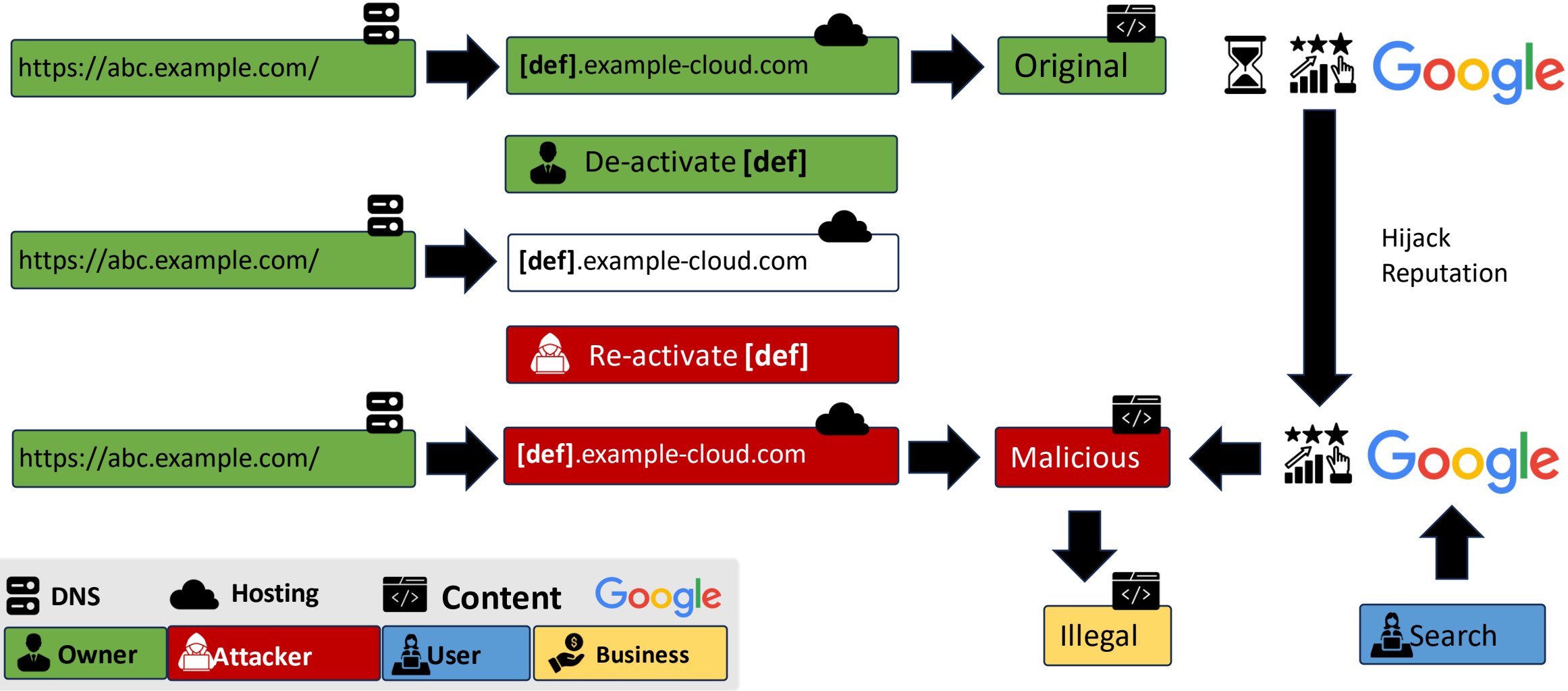
How To Monetize Hijacked Domains

/ Results / Content Analysis / Monetization



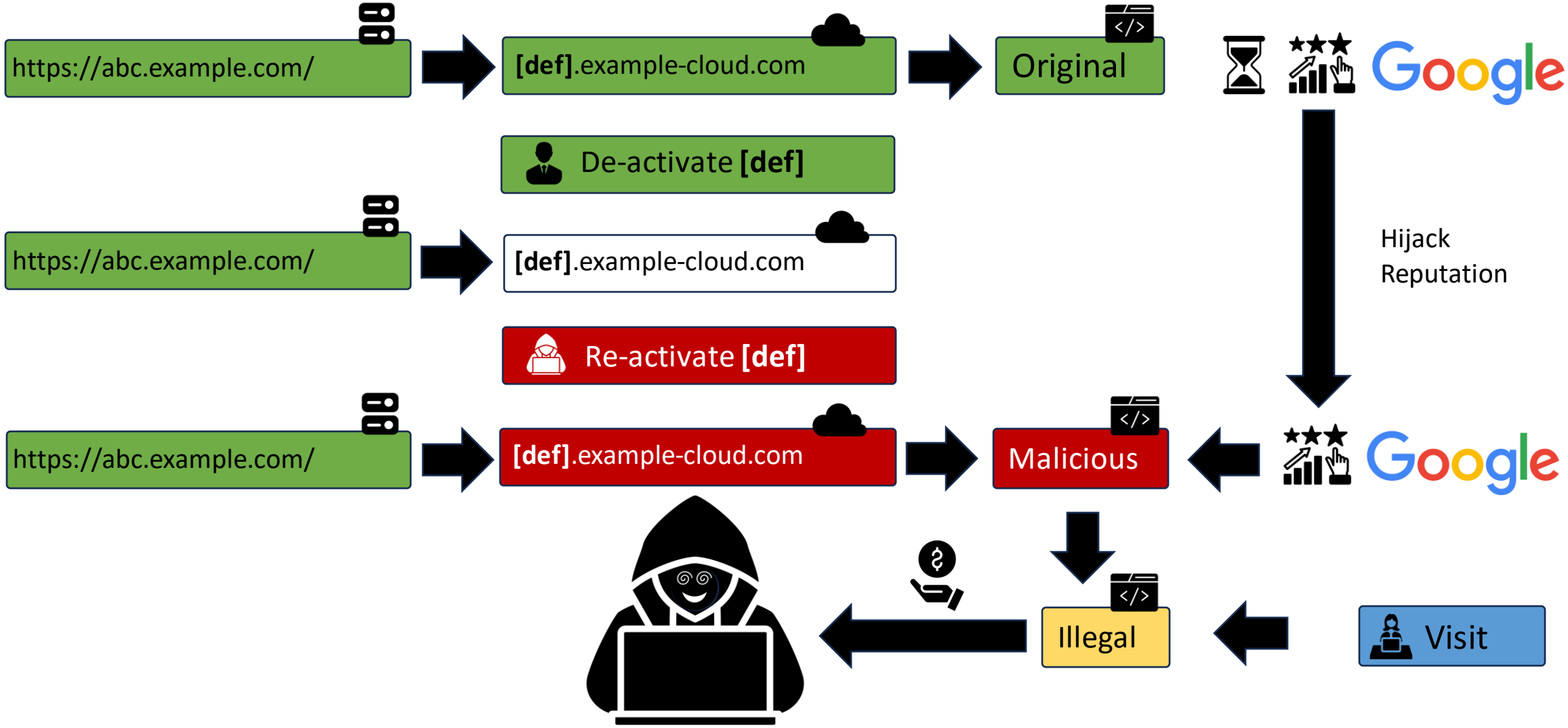
How To Monetize Hijacked Domains

/ Results / Content Analysis / Monetization



How To Monetize Hijacked Domains

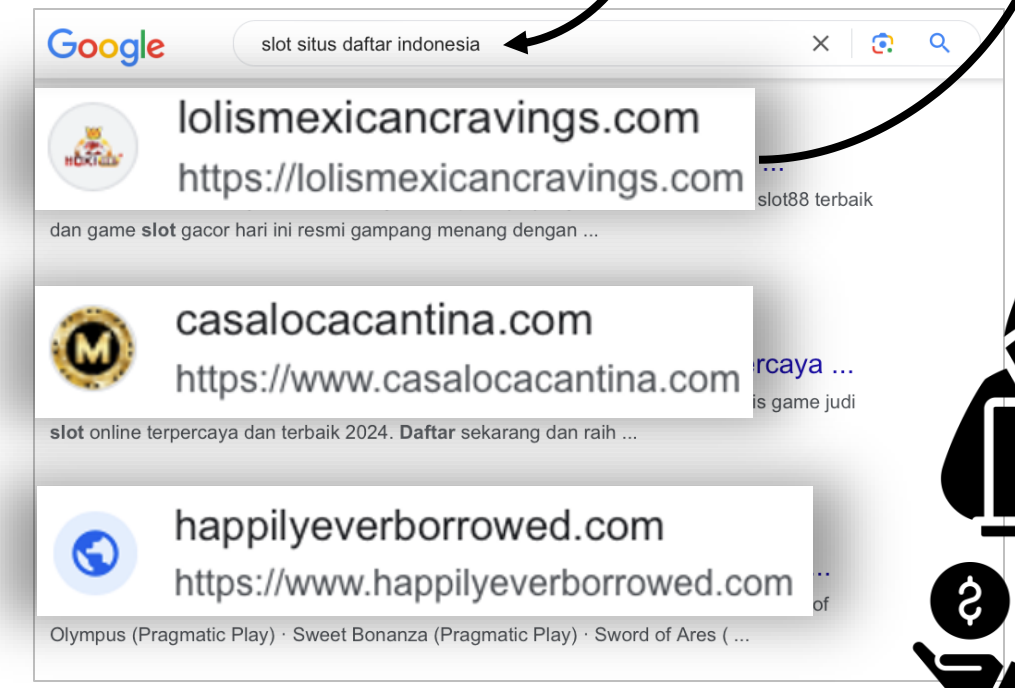
/ Results / Content Analysis / Monetization



Overlay Ad Networks for Indonesian Gambling

/ Results / Content Analysis / Example

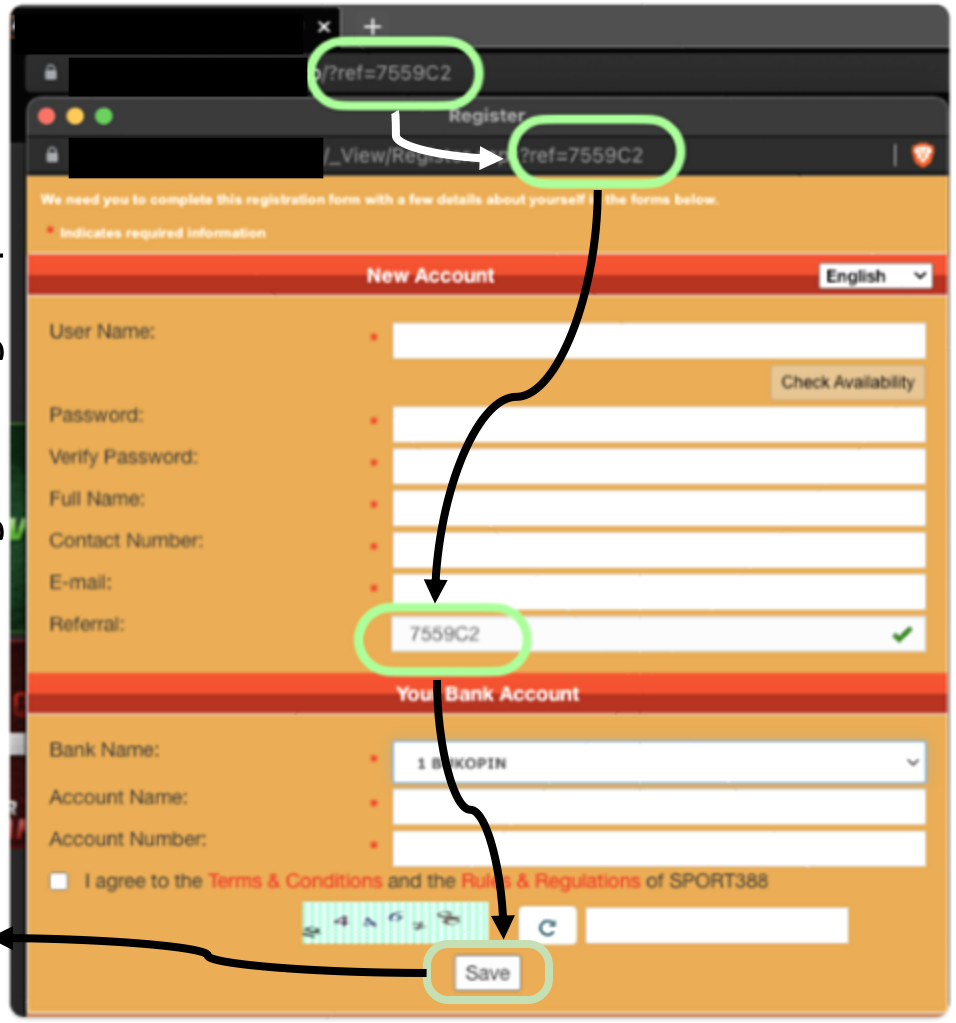
#	Keyword	Count	#	Keyword	Count
1	slot	144,108	2	online	77,669
3	judi (gambling)	60,521	4	situs (website)	35,265
5	joker123	23,630	6	terpercaya (trusted)	19,407
7	gacor (hot streak)	18,006	8	agen (agent)	16,939
9	daftar (register)	12,881	10	game	12,113
11	bola (football)	11,688	12	pulsa (credit)	10,467



=7559C2

"Doorway Page" hosted on hijacked domain with referral code attached to link

"Real" Gambling Site Sign-up



Thank you!