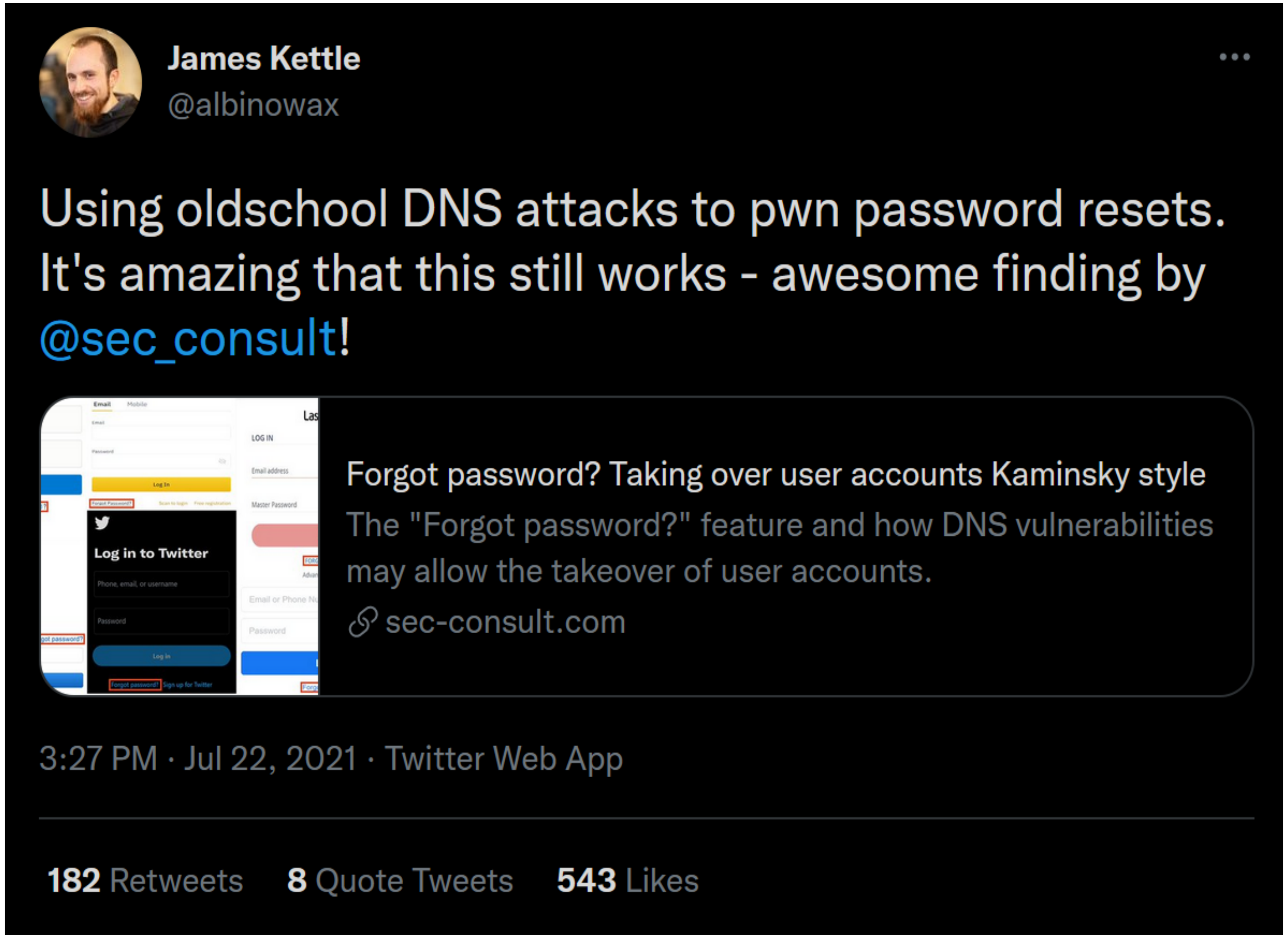
Melting the DNS Iceberg

Taking over your infrastructure Kaminsky style

SEC Consult

an atos company

Intro



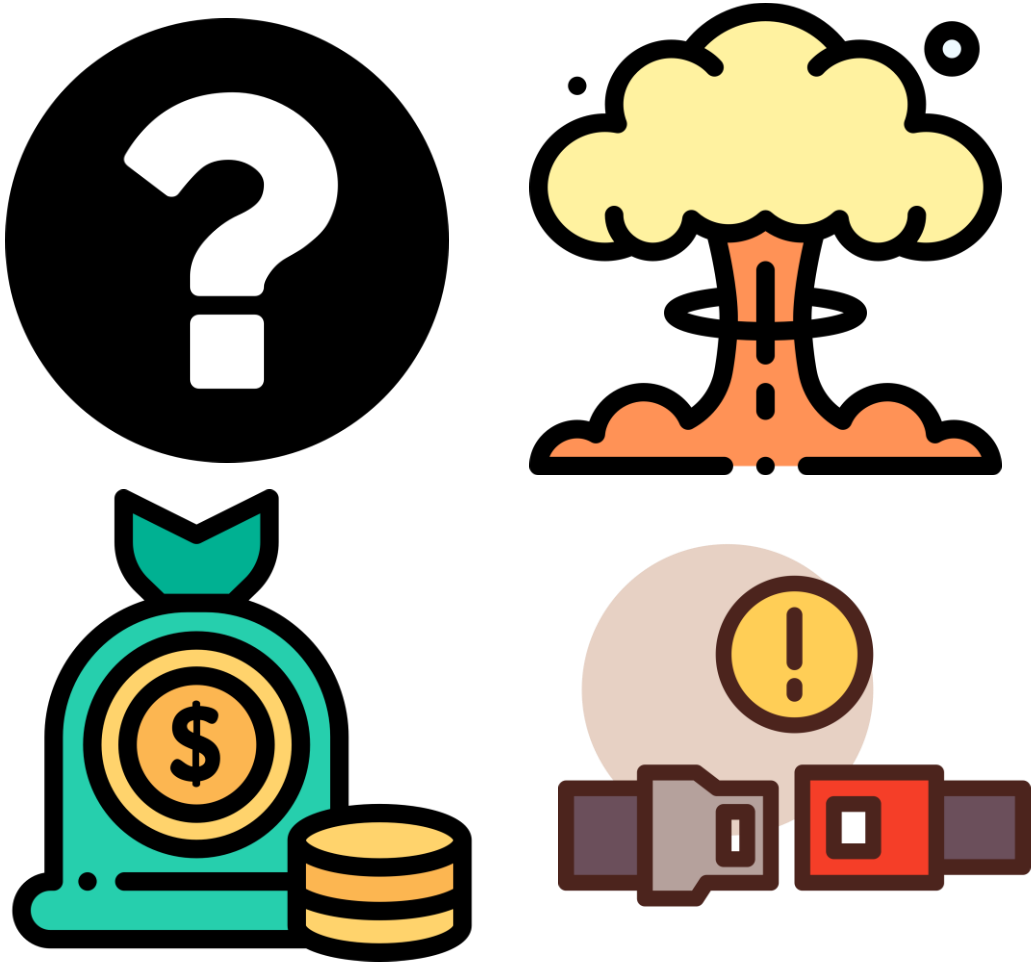
James Kettle
@albinowax

Using oldschool DNS attacks to pwn password resets. It's amazing that this still works - awesome finding by @sec_consult!

Forgot password? Taking over user accounts Kaminsky style
The "Forgot password?" feature and how DNS vulnerabilities may allow the takeover of user accounts.
sec-consult.com

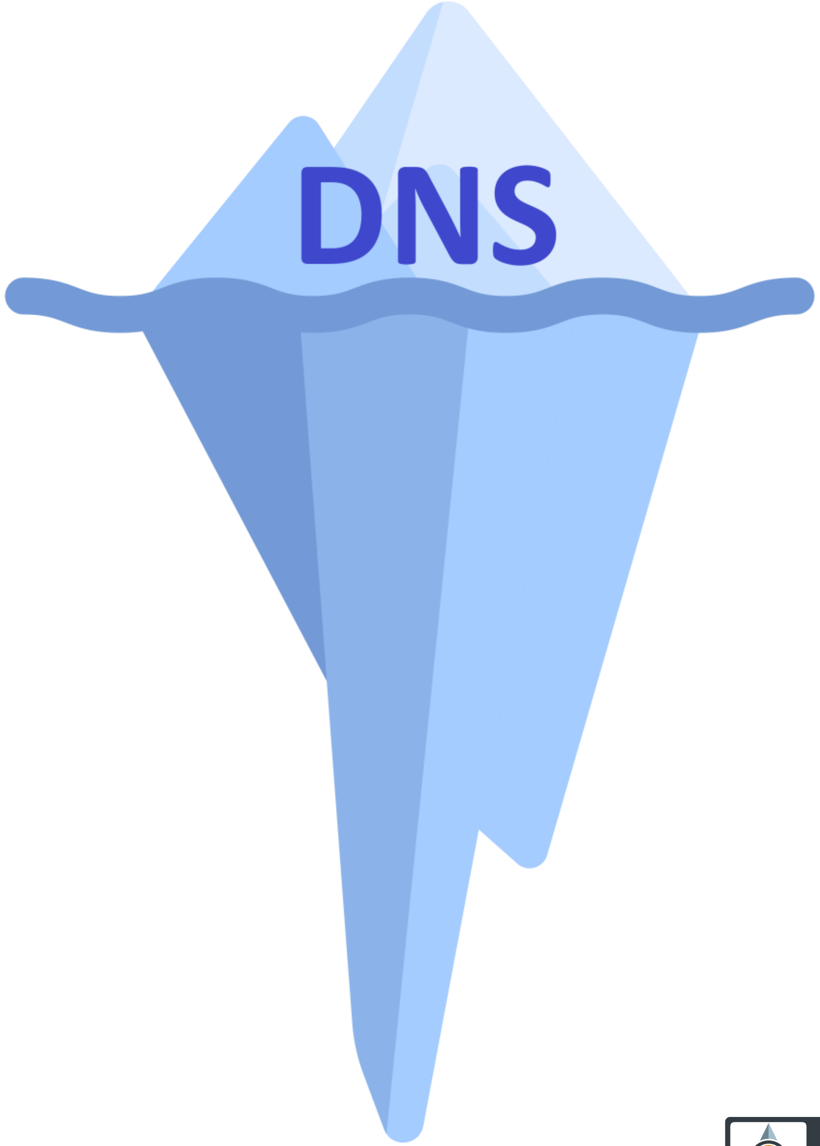
3:27 PM · Jul 22, 2021 · Twitter Web App

182 Retweets 8 Quote Tweets 543 Likes



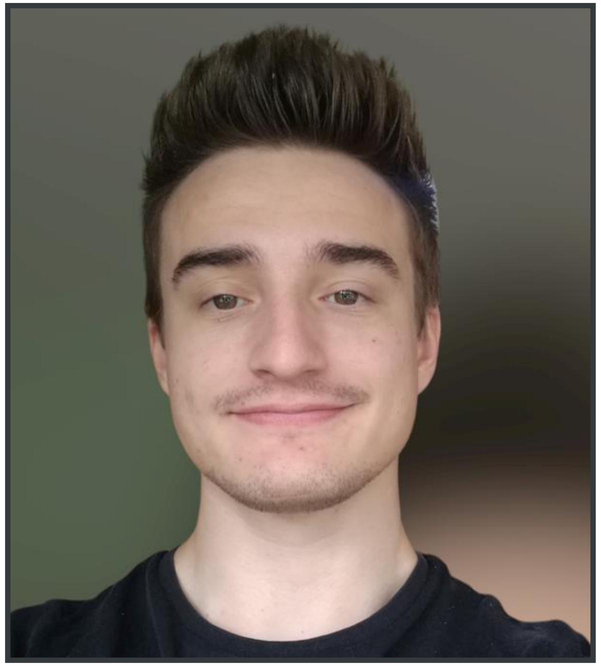
Outline

1. DNS Recap
2. The DNS Iceberg?
3. Melting the DNS Iceberg!
4. The Bottom of the Iceberg
5. Conclusion



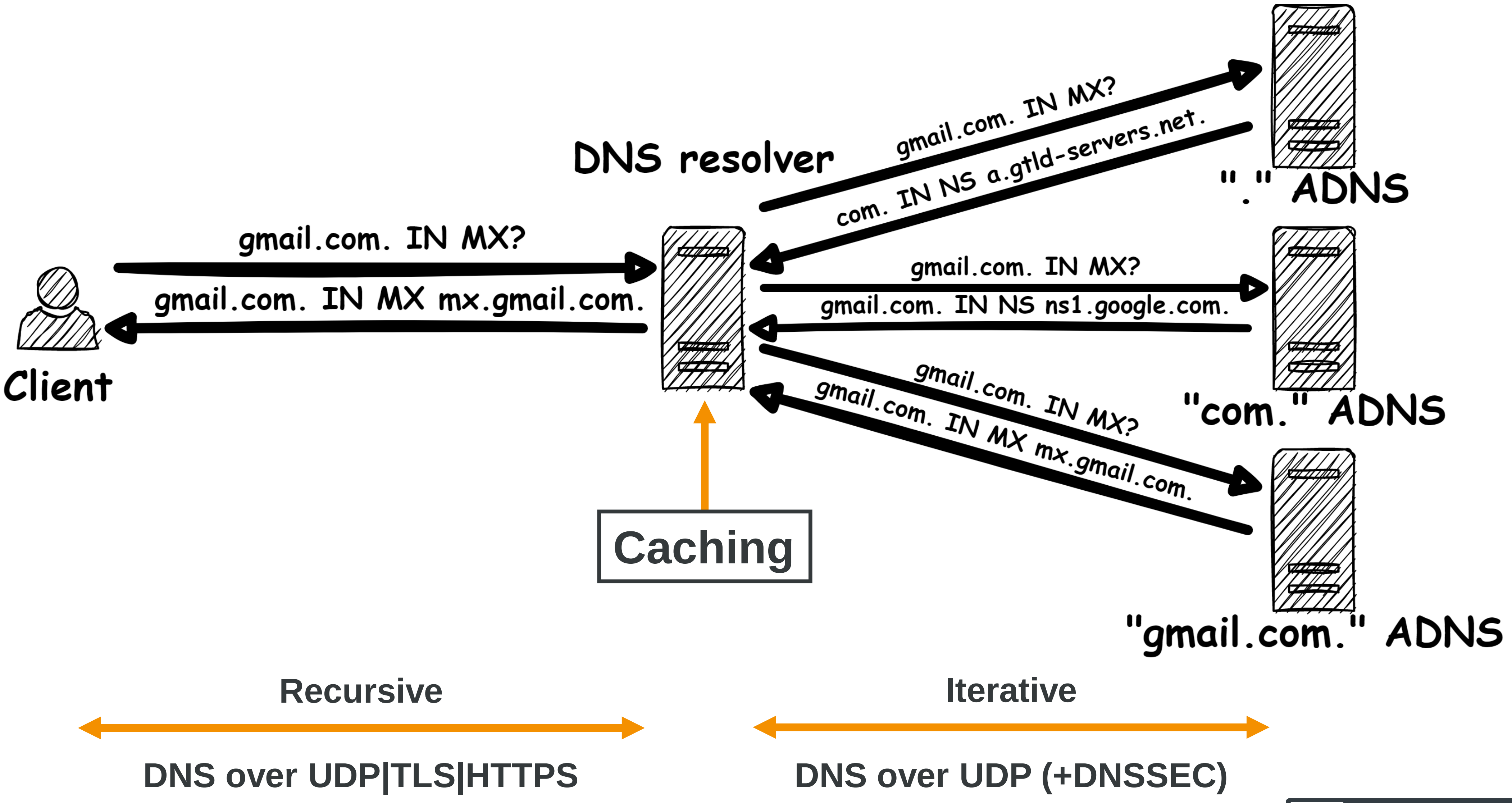
$whoami

- Security Consultant @ SEC Consult since 2018
- Offensive Security Researcher, aka. broken stuff enthusiast
- **Not** a DNS (Security) Expert

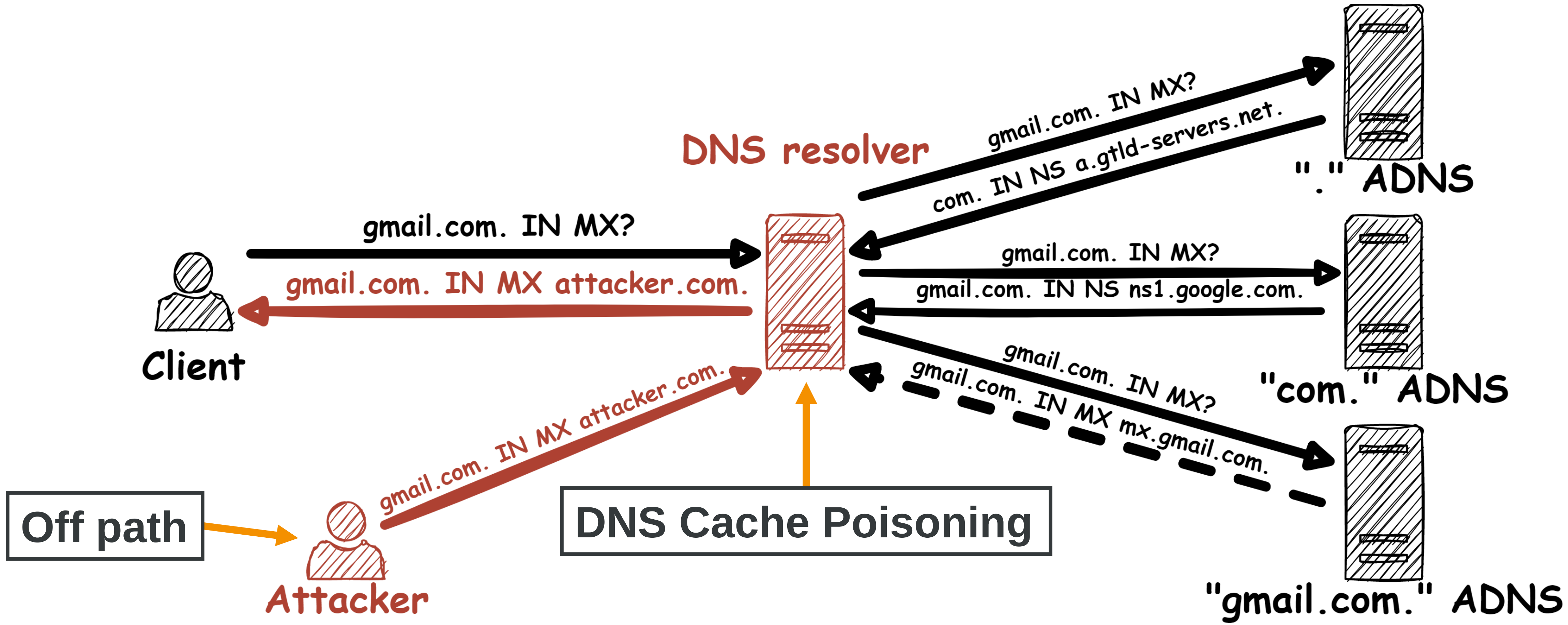


Timo Longin

DNS (Security) Recap



DNS (Security) Recap


DNS resolver
Client
Attacker
"." ADNS
"com." ADNS
"gmail.com." ADNS
gmail.com. IN MX?
gmail.com. IN MX attacker.com.
gmail.com. IN MX attacker.com.
gmail.com. IN MX?
com. IN NS a.gtld-servers.net.
gmail.com. IN MX?
gmail.com. IN NS ns1.google.com.
gmail.com. IN MX?
gmail.com. IN MX mx.gmail.com.

Off path

DNS Cache Poisoning

Recursive

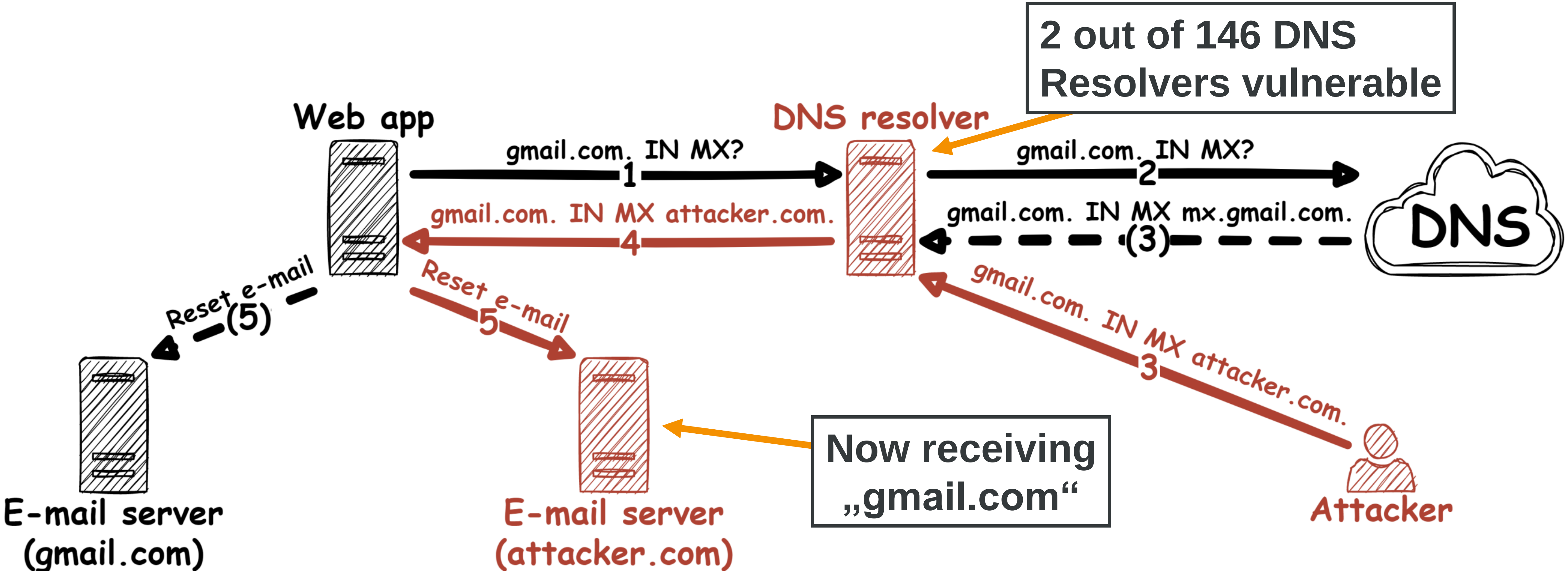
DNS over UDP|TLS|HTTPS

Iterative

DNS over UDP (+DNSSEC)

The DNS Iceberg? – Analyzing the DNS Name Resolution of Web Applications?

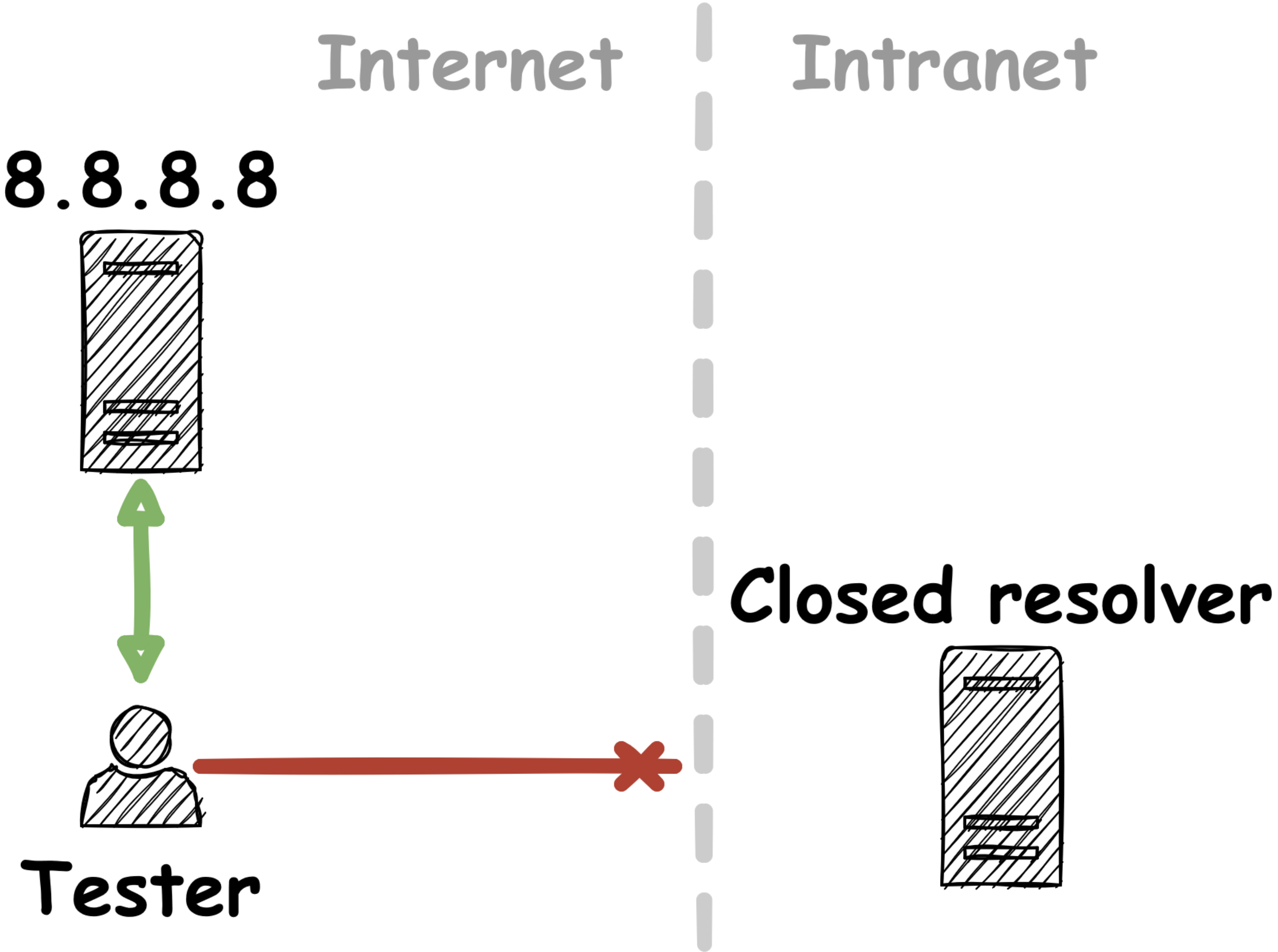
The DNS Iceberg? – Analyzing Web Applications



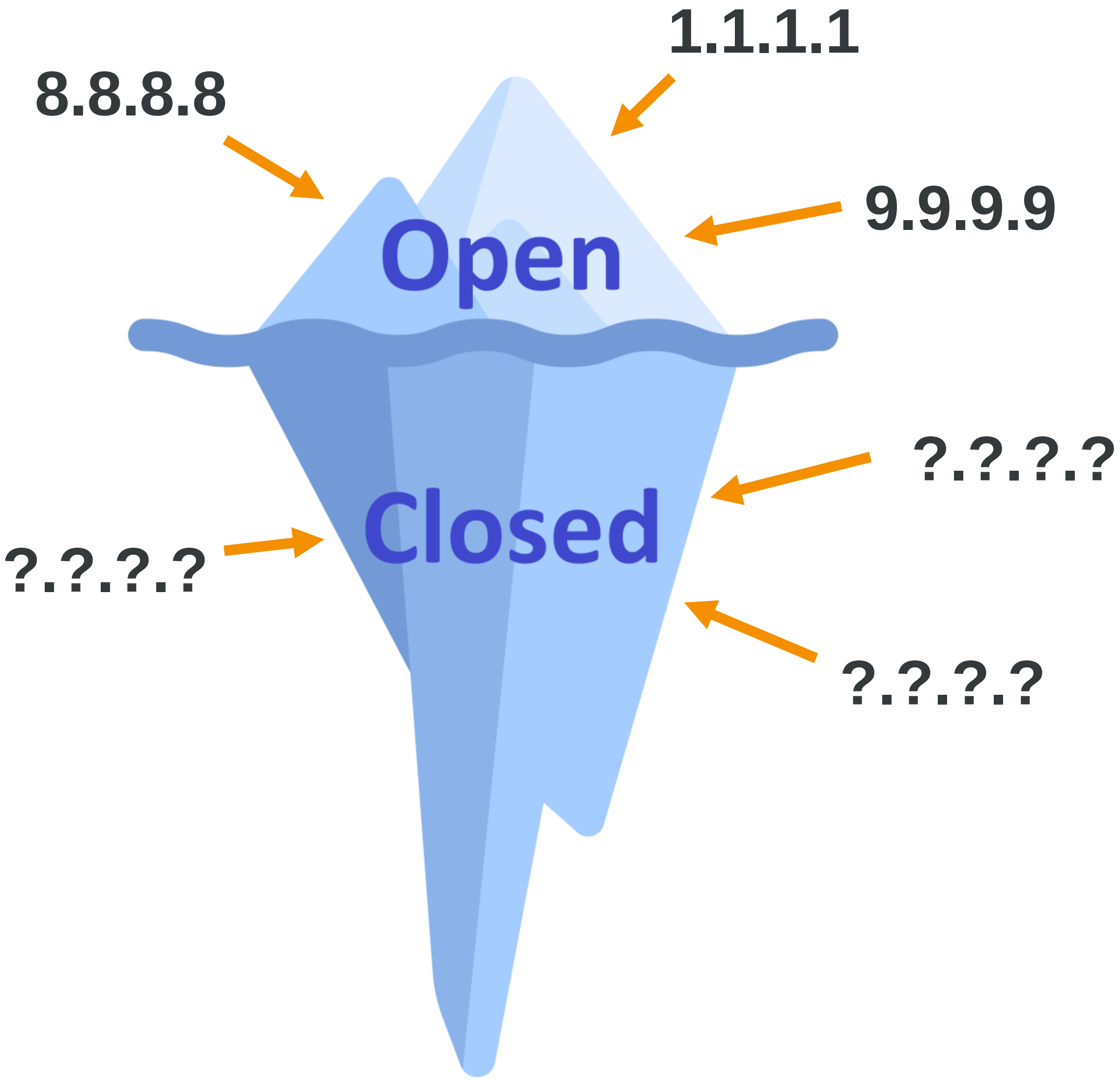
2 out of 146 DNS Resolvers vulnerable

Now receiving „gmail.com“

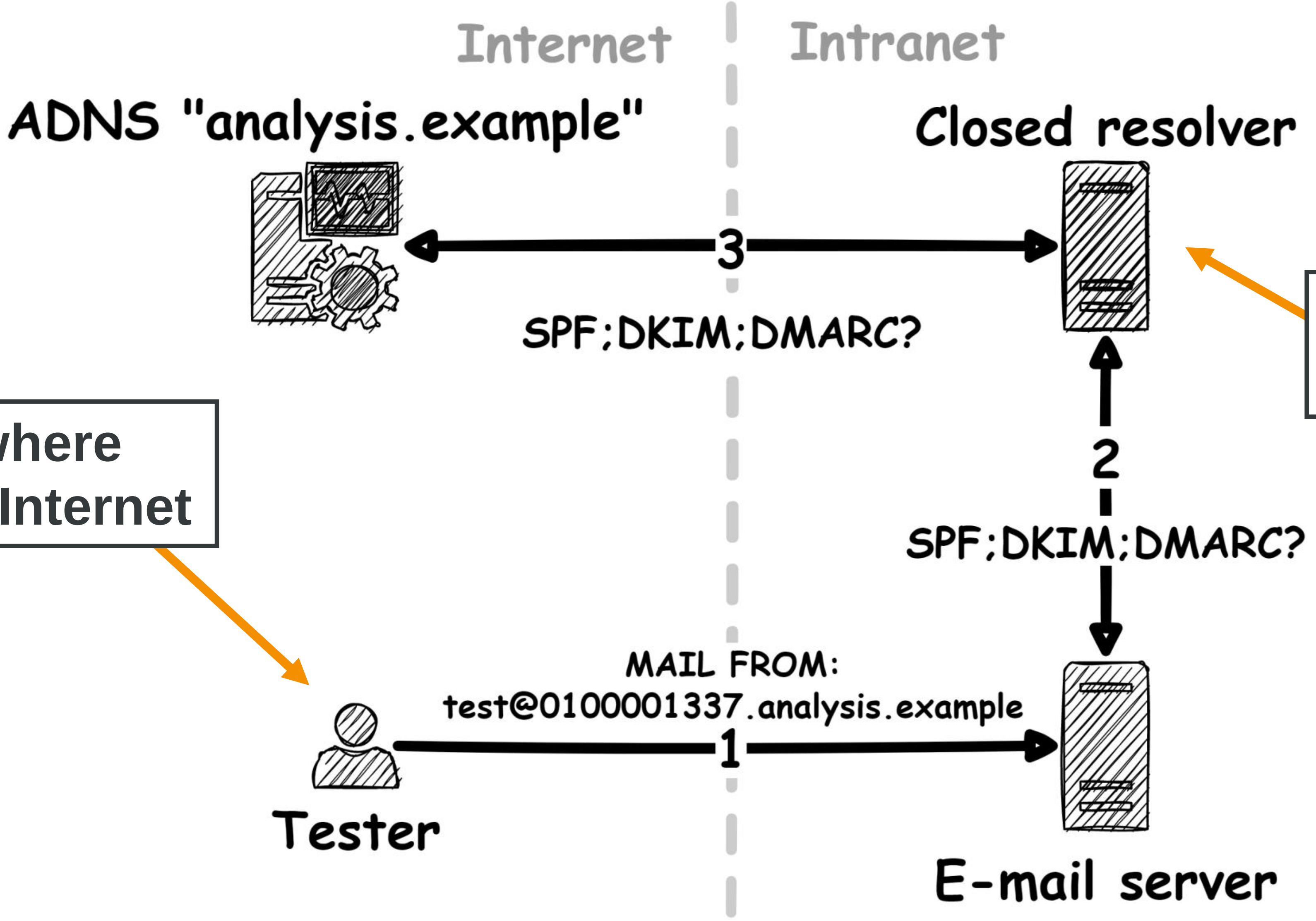
The DNS Iceberg? – Open and Closed Resolvers



The DNS Iceberg? – The DNS Iceberg



Melting the DNS Iceberg! – Reaching Closed Resolvers Method

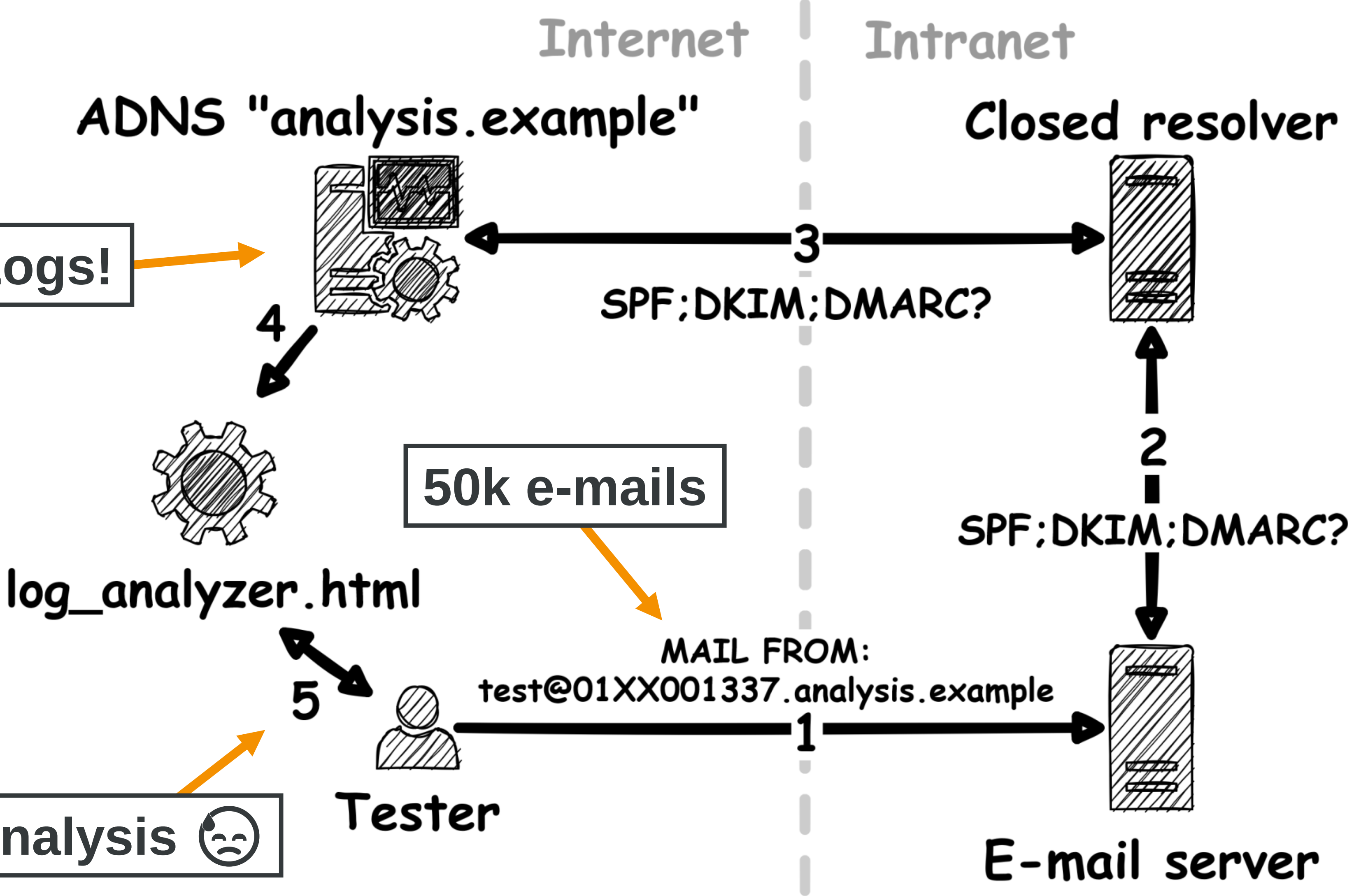


Somewhere internally

Somewhere on the Internet

Scheffler, Sarah, et al. "The unintended consequences of email spam prevention." International Conference on Passive and Active Network Measurement. Springer, Cham, 2018.

Melting the DNS Iceberg! – Testing Procedure

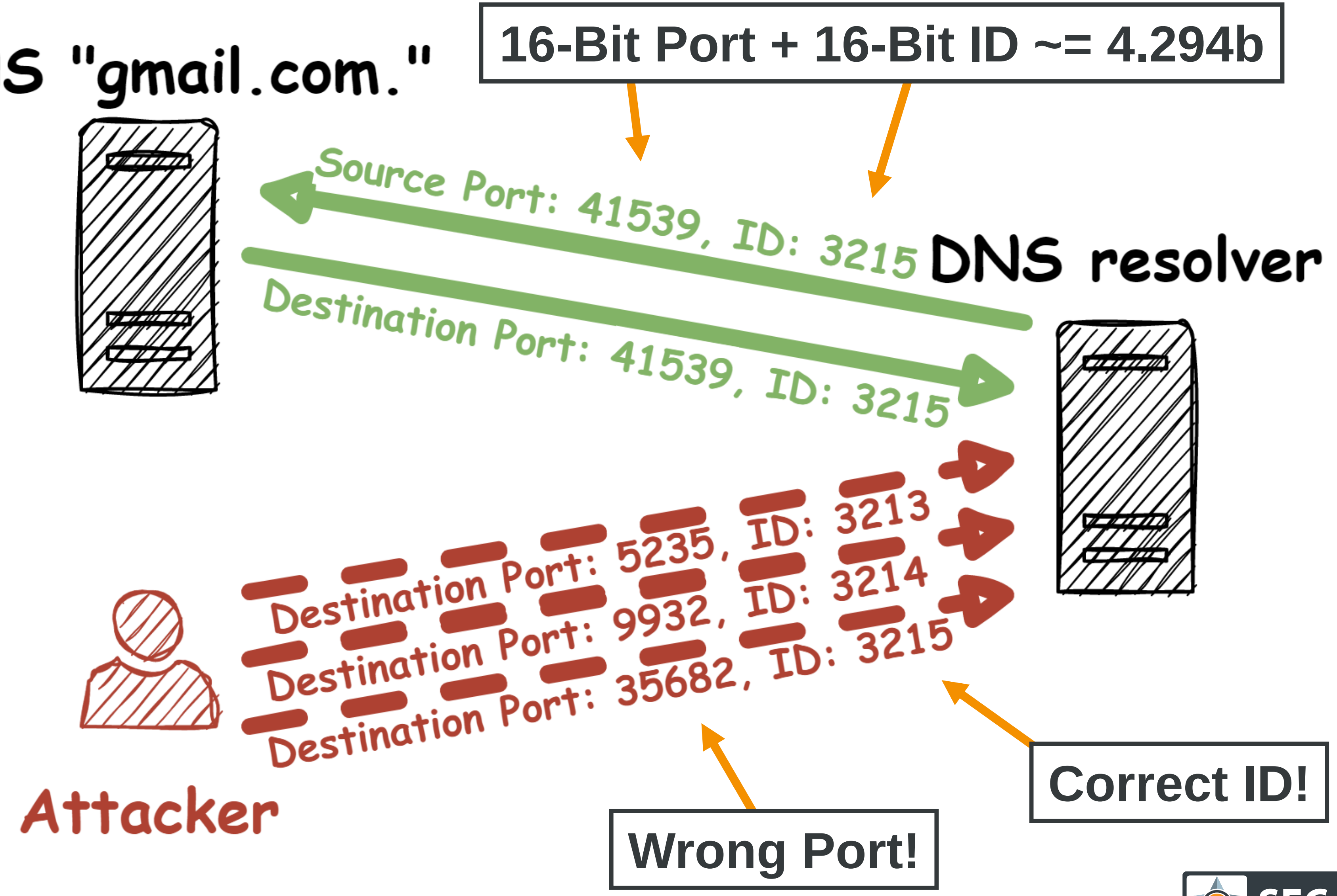


Logs!

50k e-mails

Manual Analysis 😓

Melting the DNS Iceberg! – A Kaminsky Detour (Post-Kaminsky)

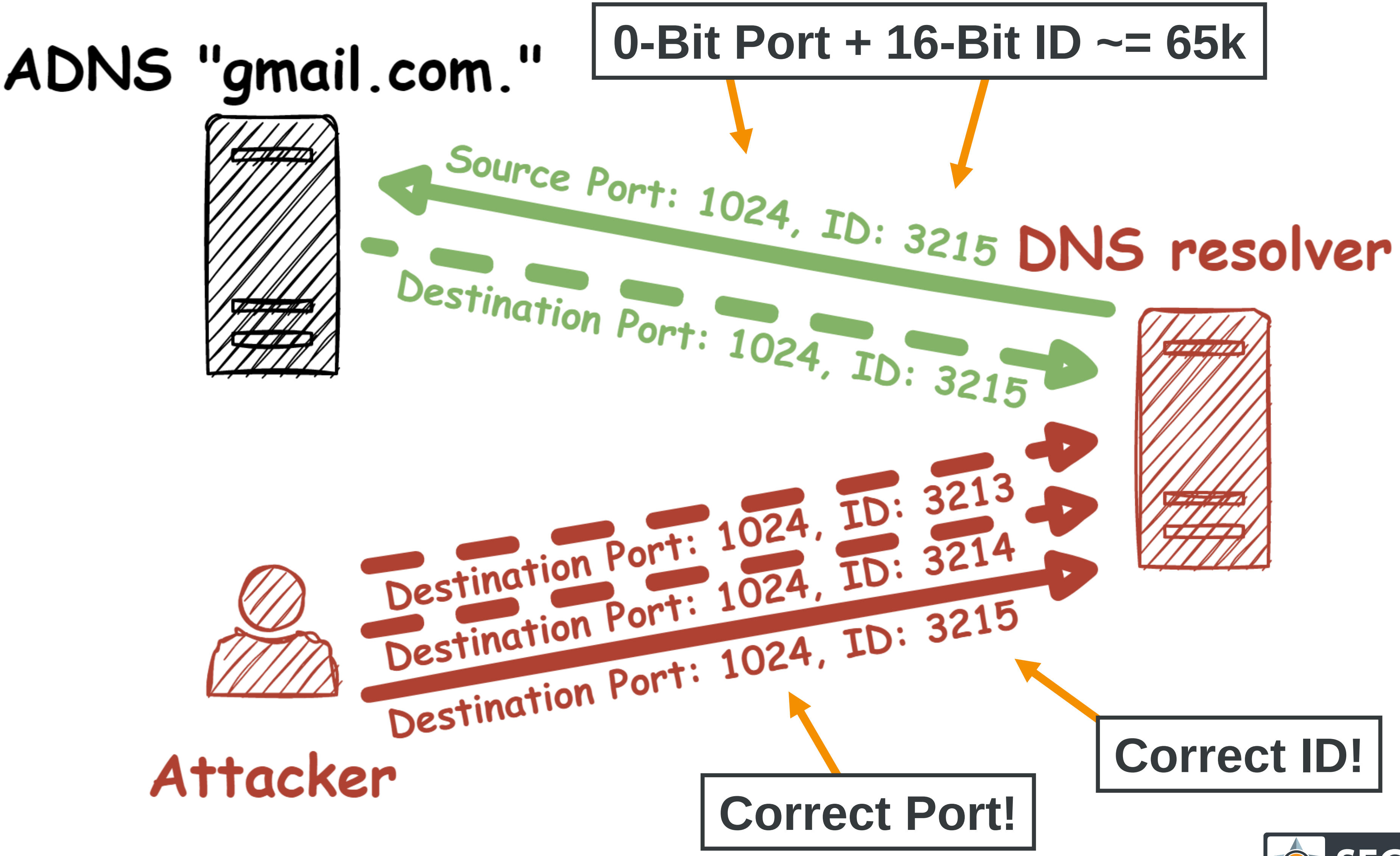

ADNS "gmail.com."
Source Port: 41539, ID: 3215
Destination Port: 41539, ID: 3215
DNS resolver
Destination Port: 5235, ID: 3213
Destination Port: 9932, ID: 3214
Destination Port: 35682, ID: 3215
Attacker

16-Bit Port + 16-Bit ID ~= 4.294b

Correct ID!

Wrong Port!

Melting the DNS Iceberg! – A Kaminsky Detour (Pre-Kaminsky)

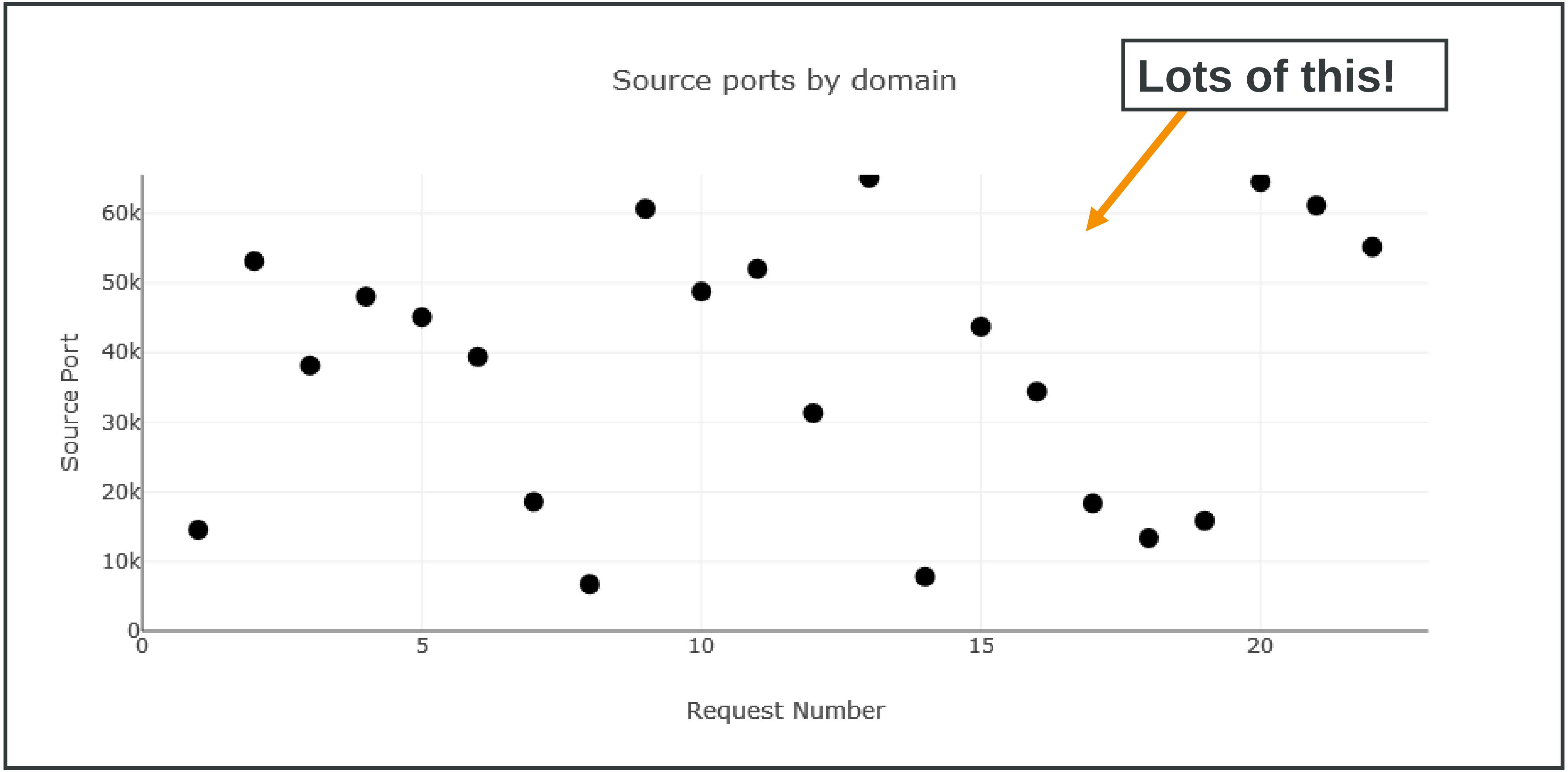

ADNS "gmail.com."
Source Port: 1024, ID: 3215
DNS resolver
Destination Port: 1024, ID: 3215
Destination Port: 1024, ID: 3213
Destination Port: 1024, ID: 3214
Destination Port: 1024, ID: 3215
Attacker

0-Bit Port + 16-Bit ID ~= 65k

Correct ID!

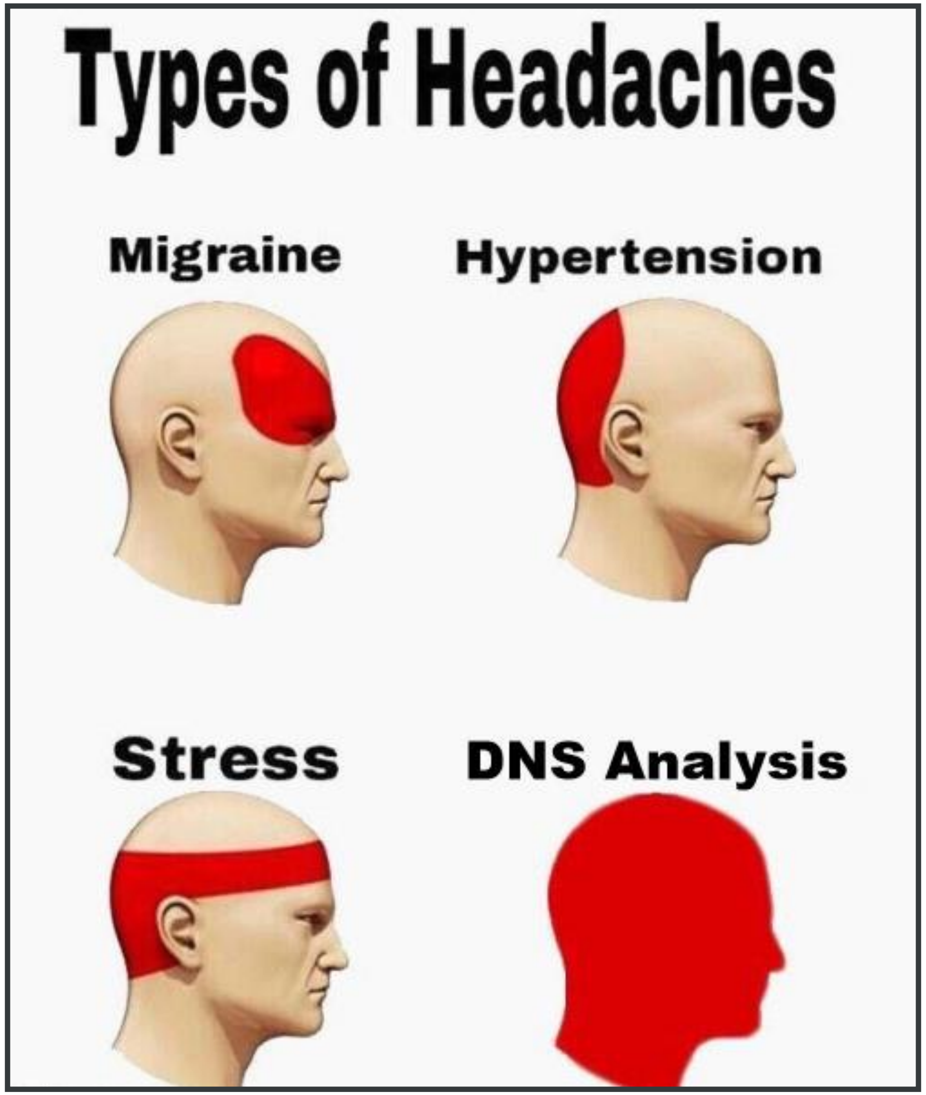
Correct Port!

Melting the DNS Iceberg! – log_analyzer.html

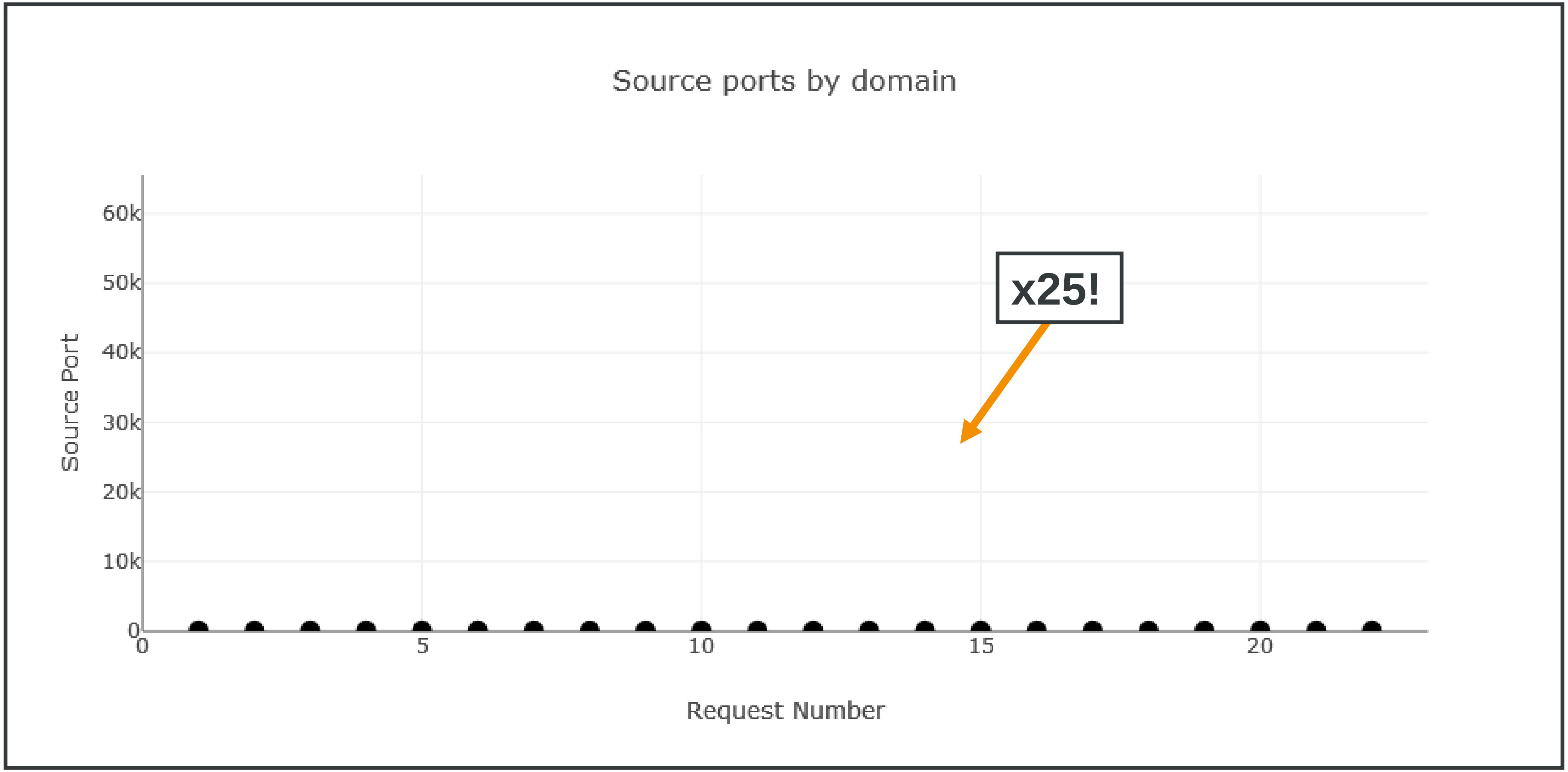


Lots of this!

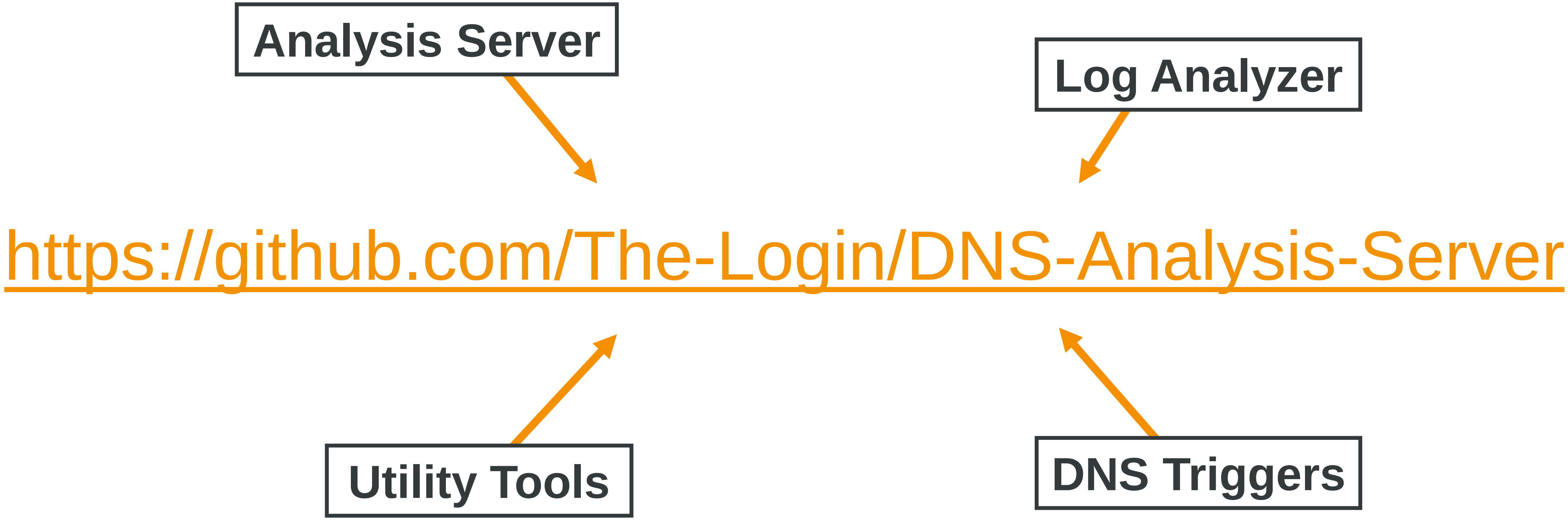
Melting the DNS Iceberg! – log_analyzer.html



Melting the DNS Iceberg! – log_analyzer.html



Melting the DNS Iceberg! – Tooling!



Analysis Server

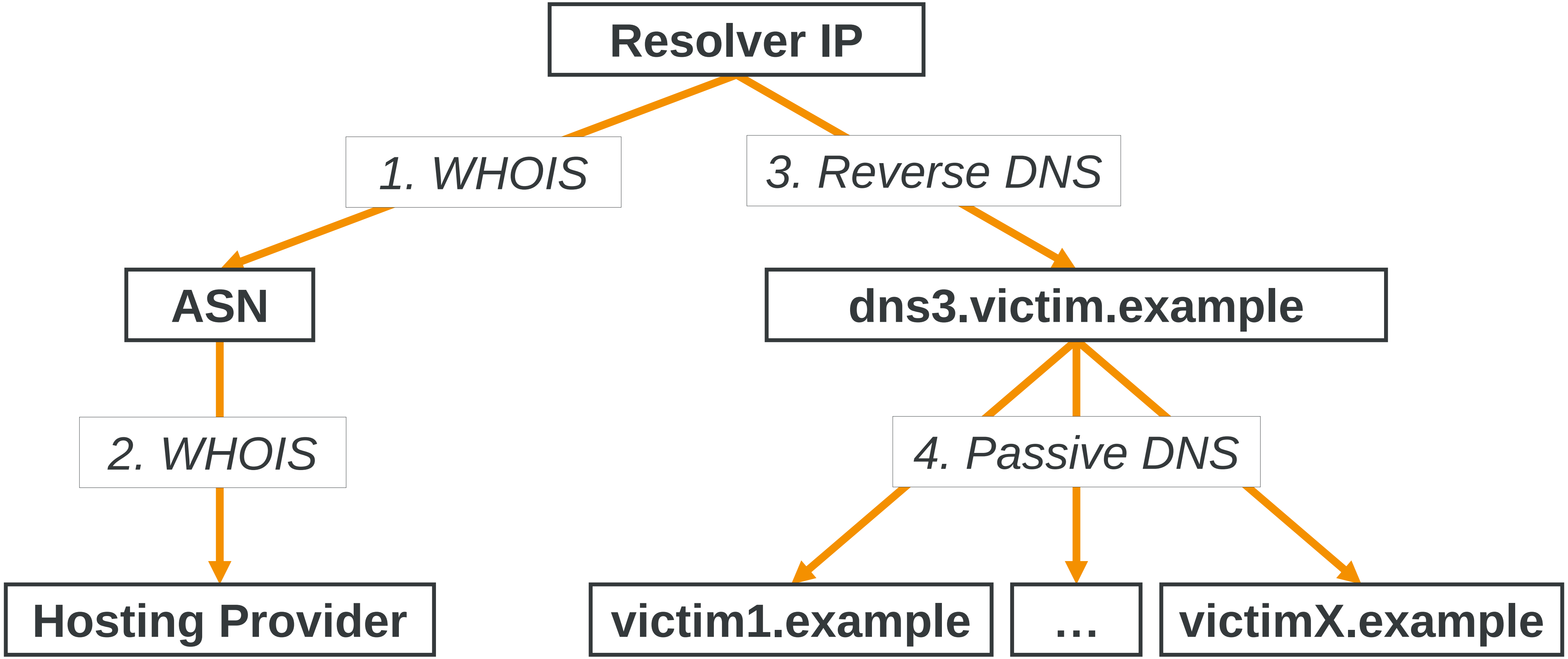
Log Analyzer

https://github.com/The-Login/DNS-Analysis-Server

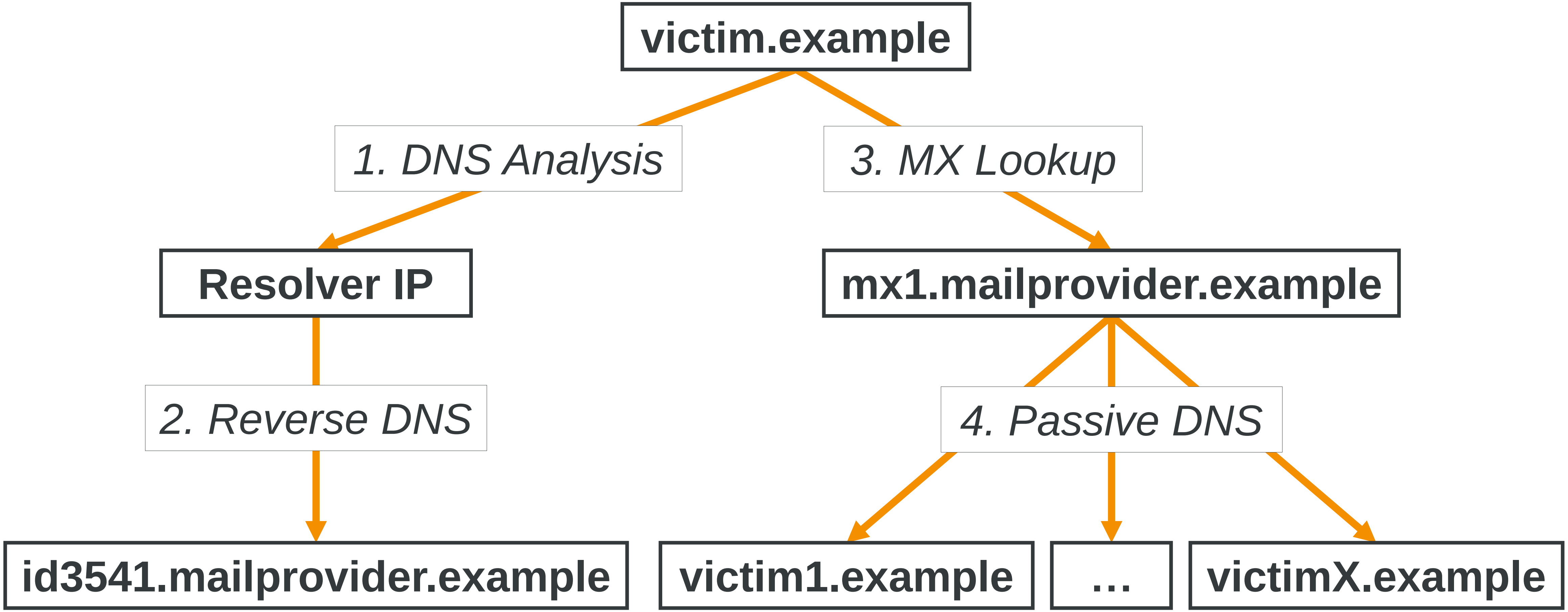
Utility Tools

DNS Triggers

Melting the DNS Iceberg! – Going down the Rabbit Hole #1



Melting the DNS Iceberg! – Going down the Rabbit Hole #2



The Bottom of the Iceberg – The (in)security of closed DNS Resolvers

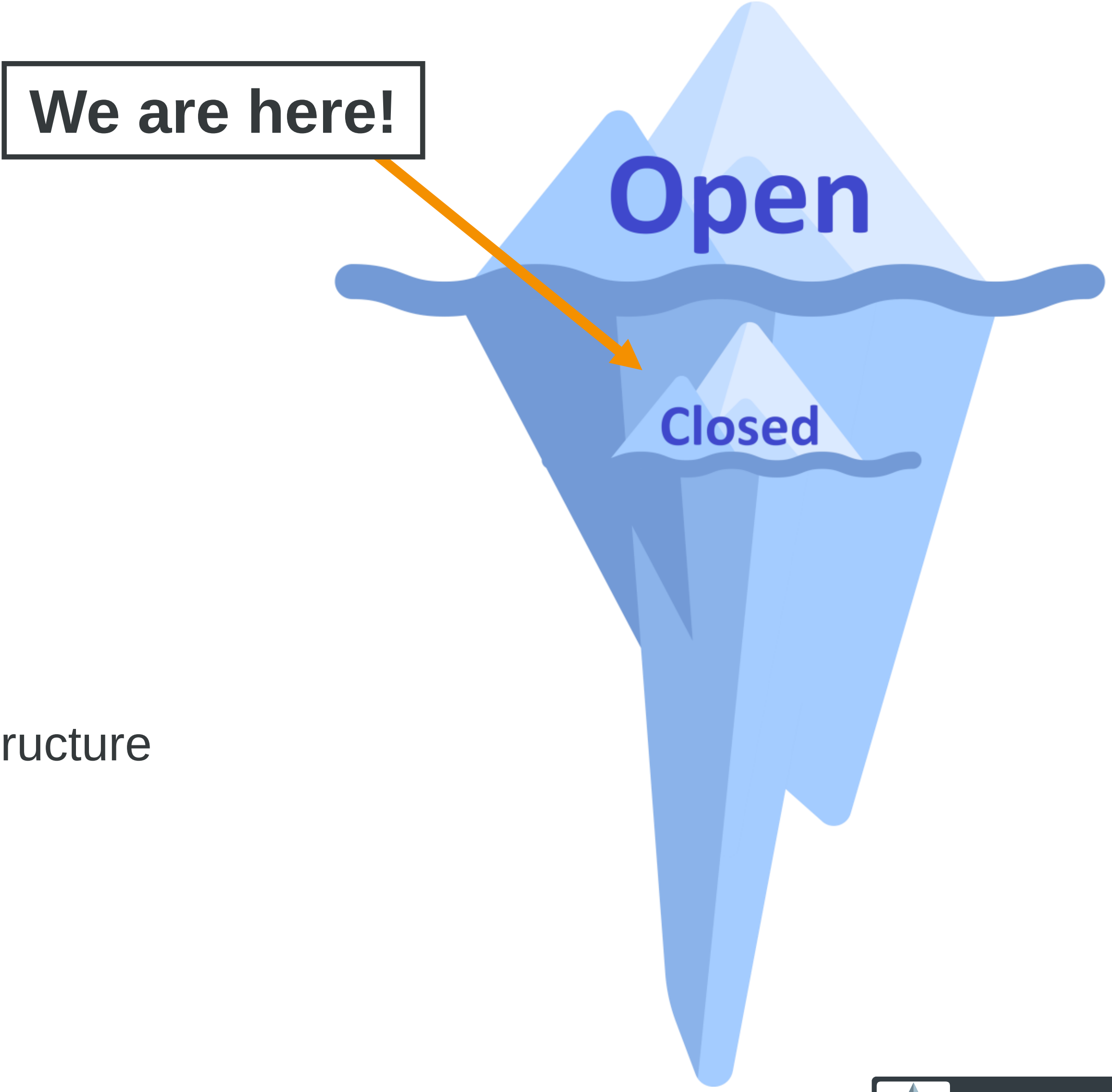
- **Initial Set:** 50k domains

- **Analyzed Set:** 7k domains
  - Open Resolvers: ~35%
  - Closed Resolvers: ~65%

- **Vulnerable Resolvers (Kaminsky):** 25
  - Open Resolvers: 2
  - Closed Resolvers: 23

- **Vulnerable Domains:** 1000+

- **Affected:** Websites and external Infrastructure
  - Corporate Infrastructure
  - Government Services
  - Political Campaigns
  - Small-Business Websites
  - …

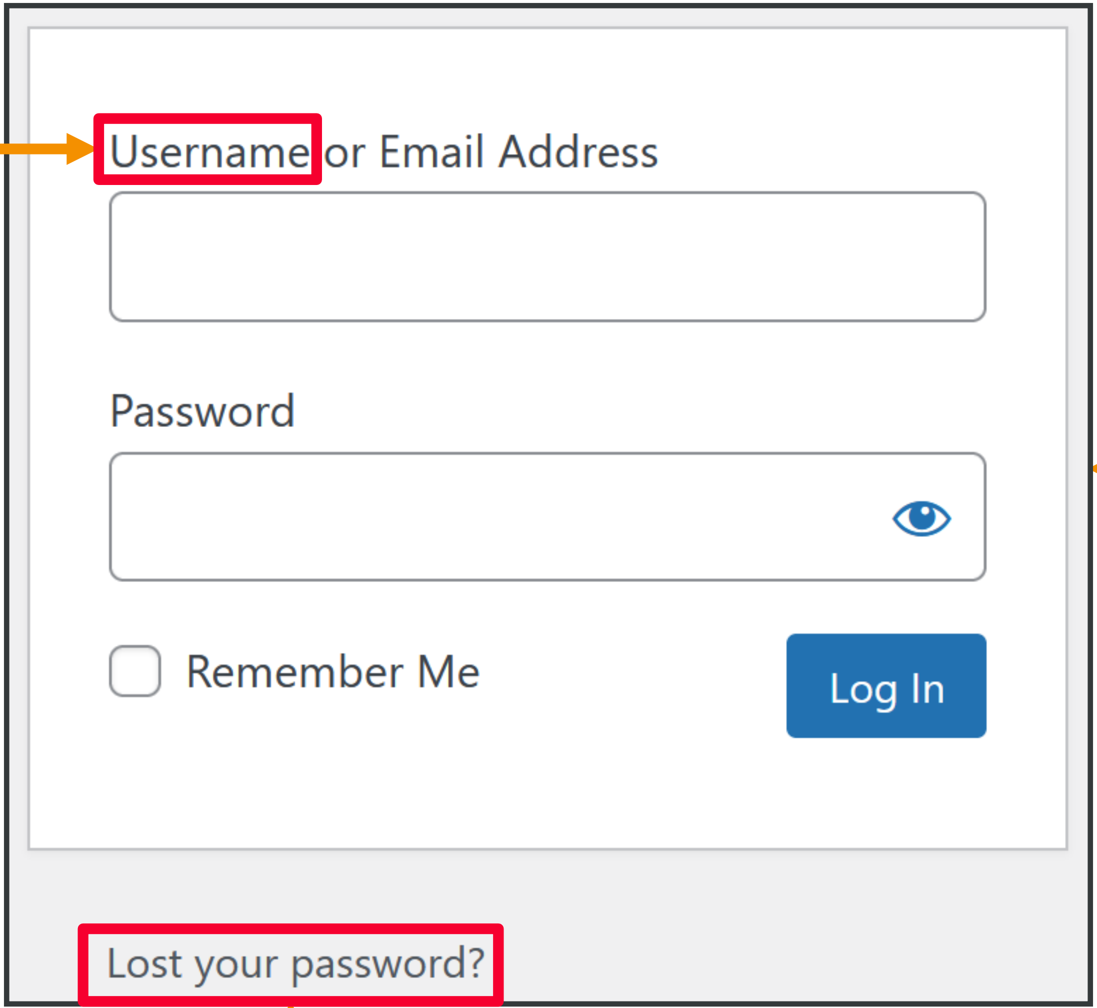


The Bottom of the Iceberg – The (in)security of closed DNS Resolvers

The Bottom of the Iceberg – Now what?

The Bottom of the Iceberg – Leveraging DNS

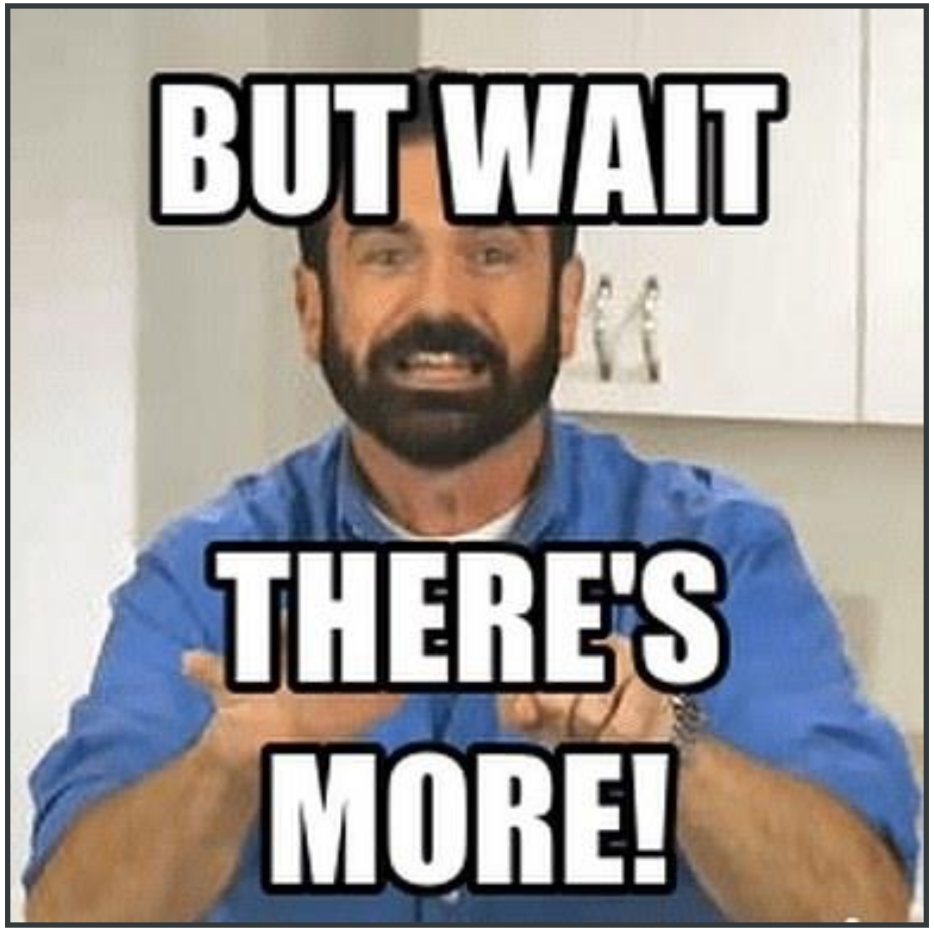
"admin"



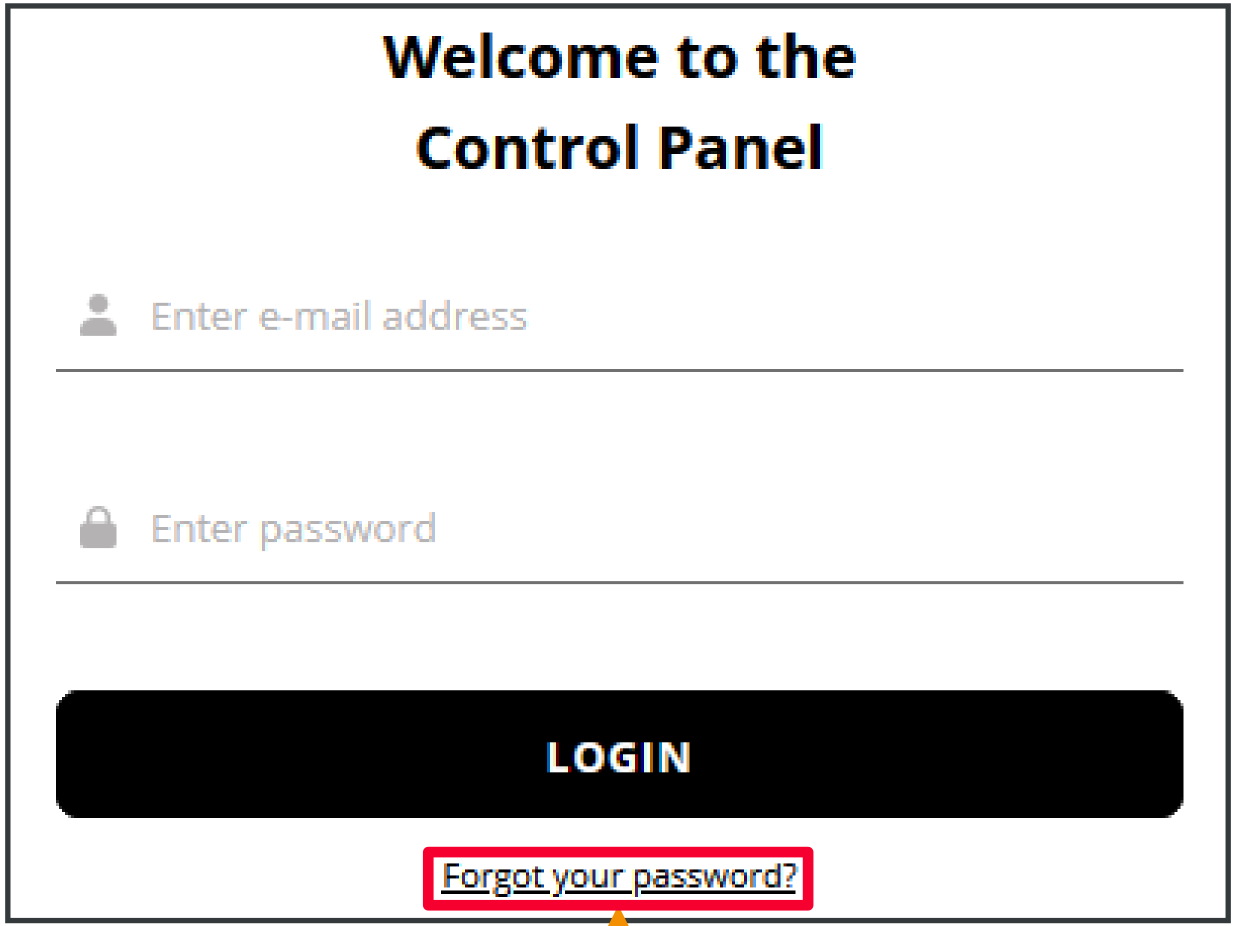
Fully patched?
No problem!

Let‘s reset!

The Bottom of the Iceberg – Leveraging DNS



The Bottom of the Iceberg – Leveraging DNS

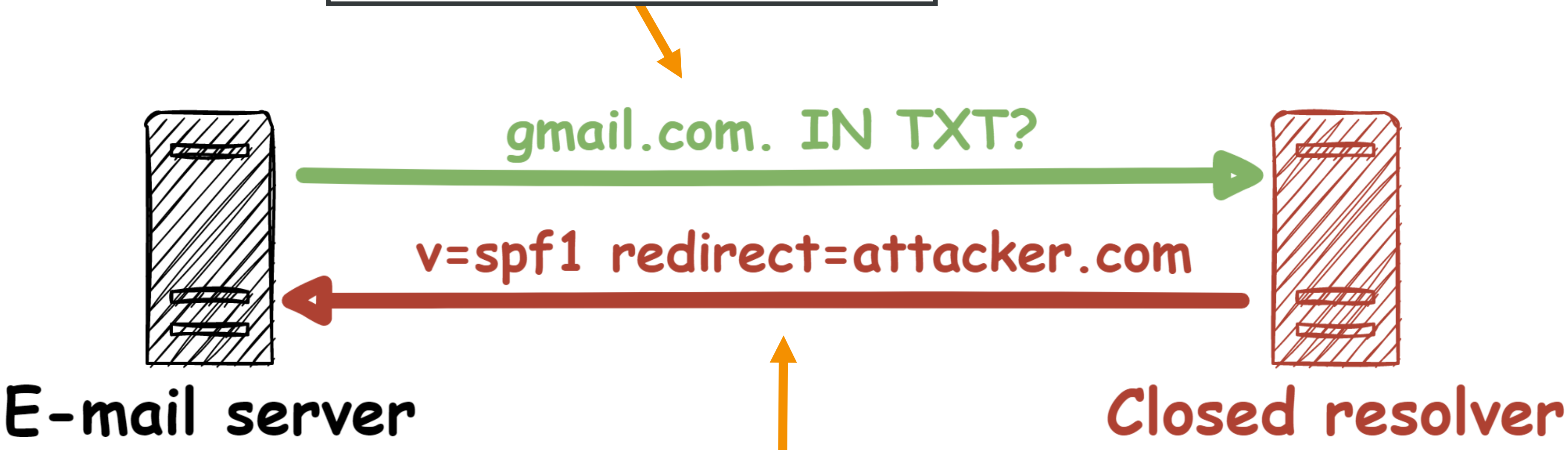


Welcome to the Control Panel

Let‘s reset them all!

The Bottom of the Iceberg – Leveraging DNS

"Give me the SPF record for gmail.com"



"Get it from attacker.com"

Conclusion – What‘s next?

- **Many more** DNS Triggers
- **Many more** DNS Attack Vectors
- **Many more** DNS Icebergs
- **Many more** Bug Bounties
- **Get creative!**