Dangling DNS Records for Cloud Resources:

Detection, Impact & Mitigation

Rich Infante
richard.infante@quinnipiac.edu

Vulnerability

- Some cloud resources use a shared pool of IP addresses
- Admins enter these IPs and hosts into DNS
- Upon resource termination, DNS records remain
- Attackers or other customers may receive these addresses from the provider

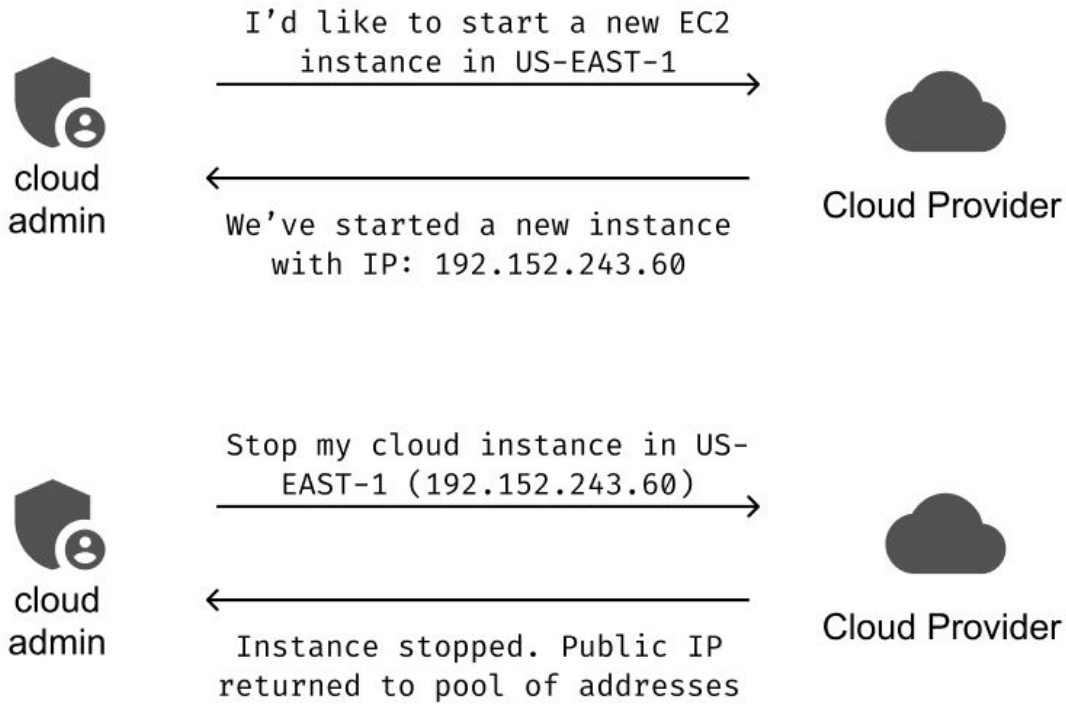
Threat

- Repeatedly create instances and listen for traffic
- Listen for traffic directed at instance
- If DNS Records exist, attackers can get a TLS Certificate
  - Unencrypted SNI allows domain name discovery
  - Launch convincing phishing attacks

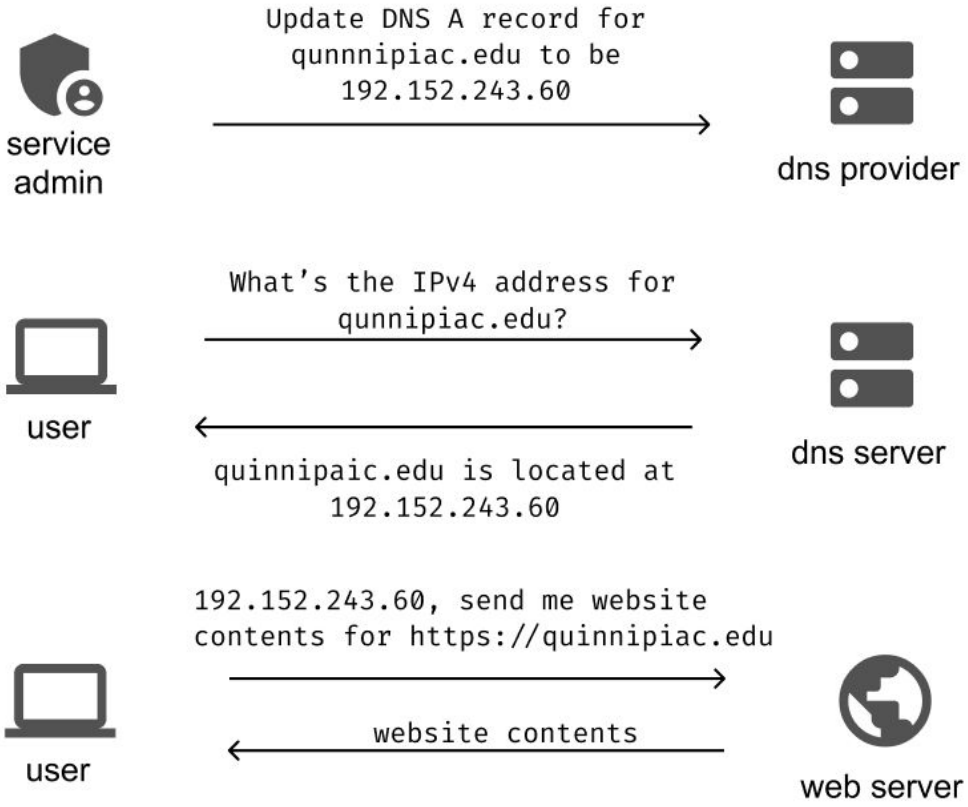
Threat (cont.)

- Spread malware
- Compromise websites (malicious JS)
- Credential stealing

Cloud Instance Lifecycle

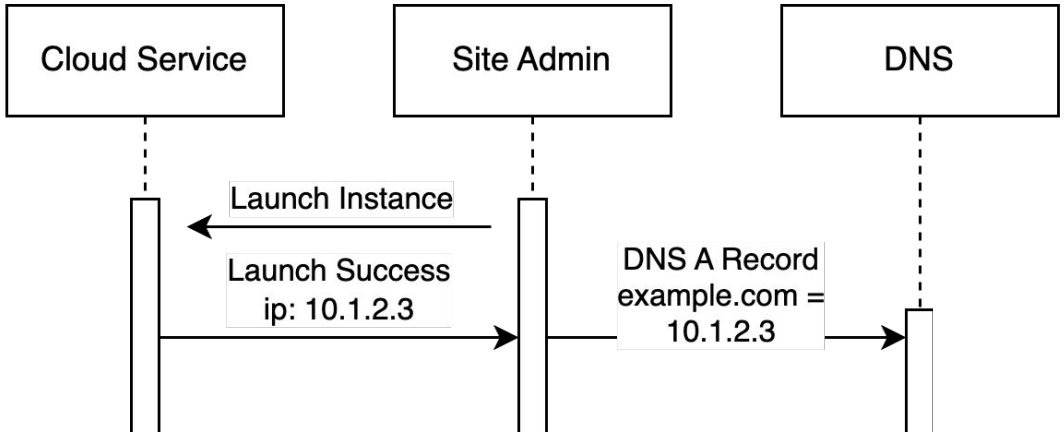


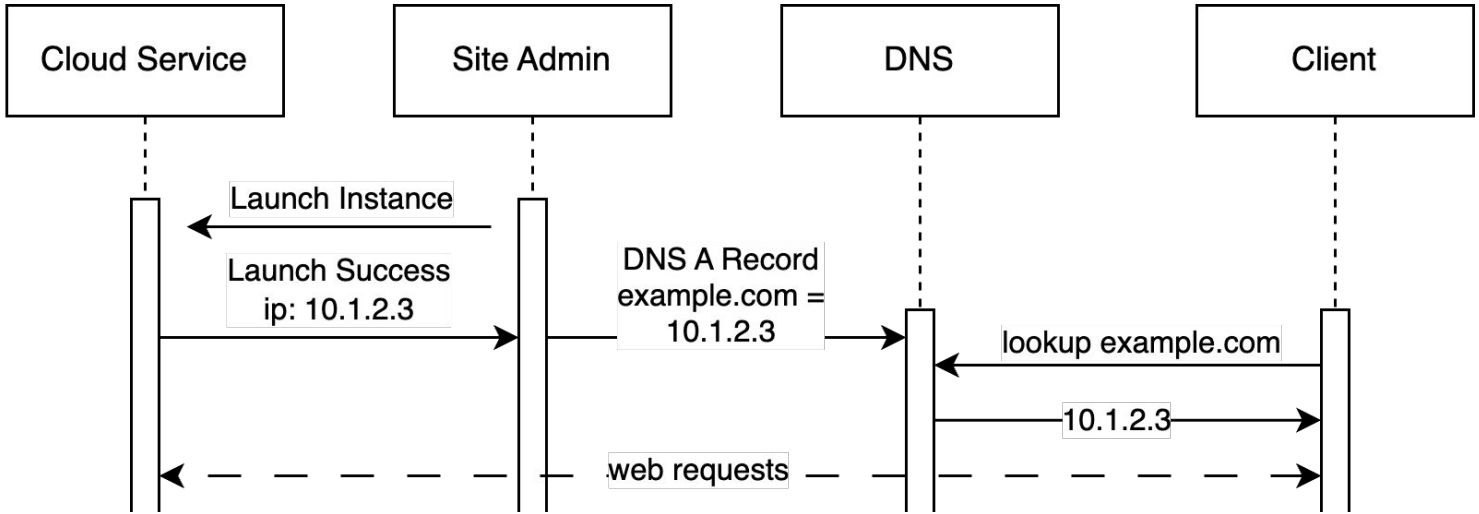
DNS Lookup Process

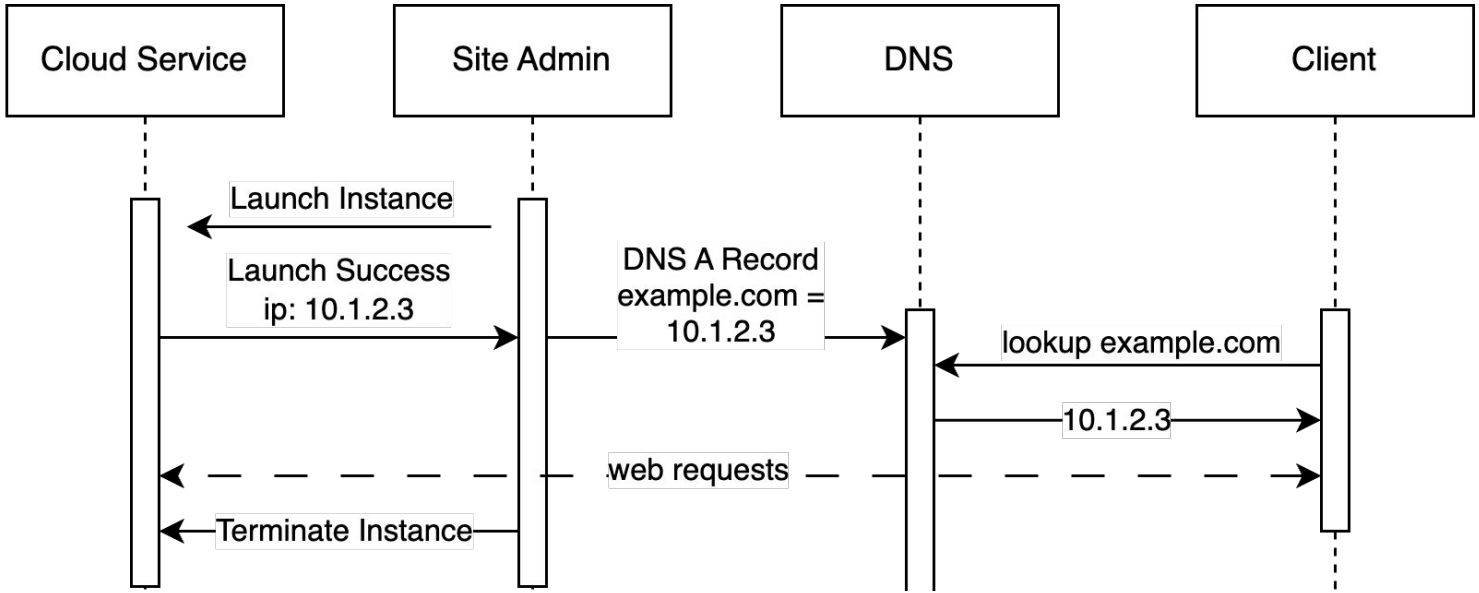


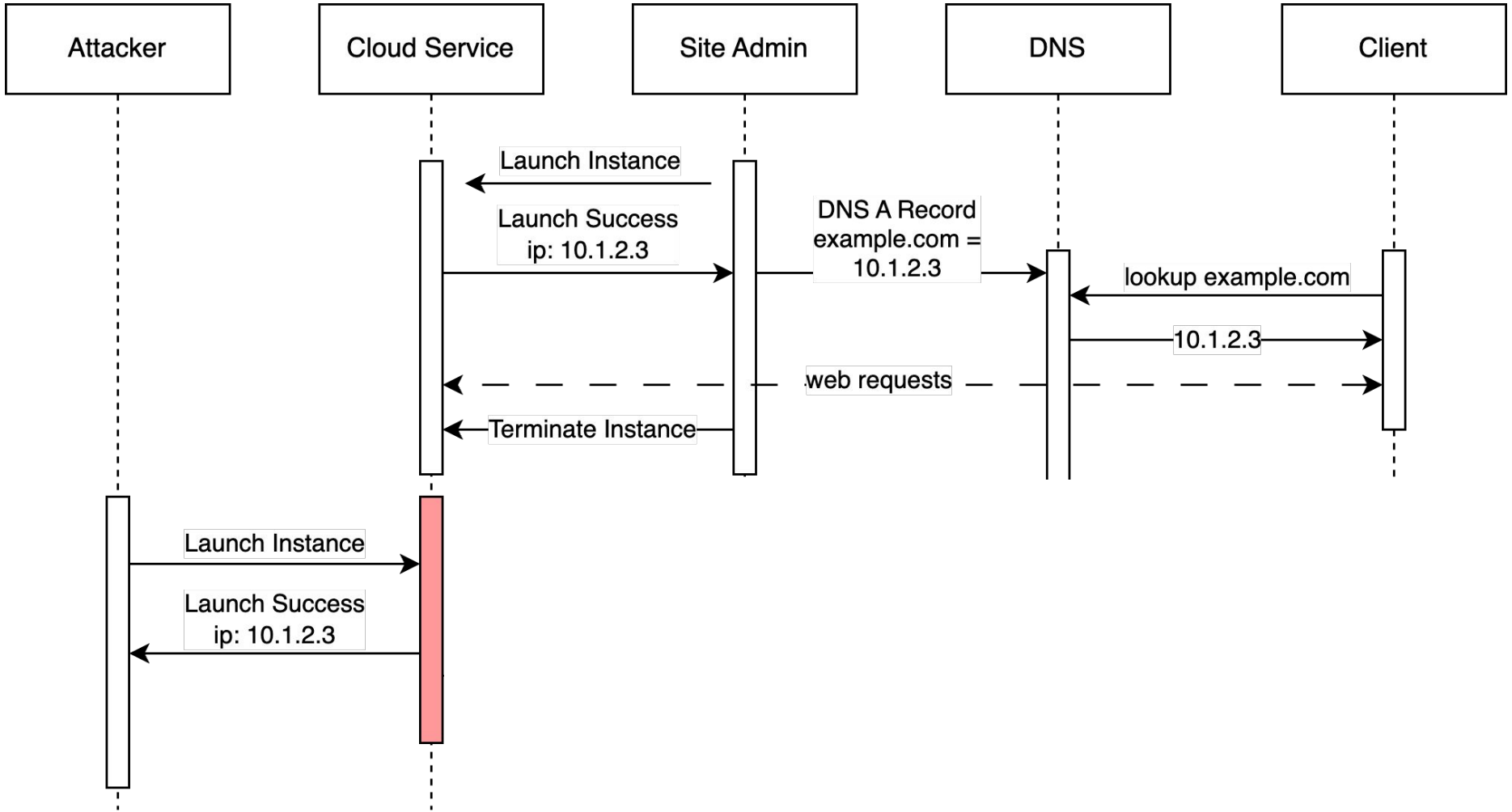
Attack

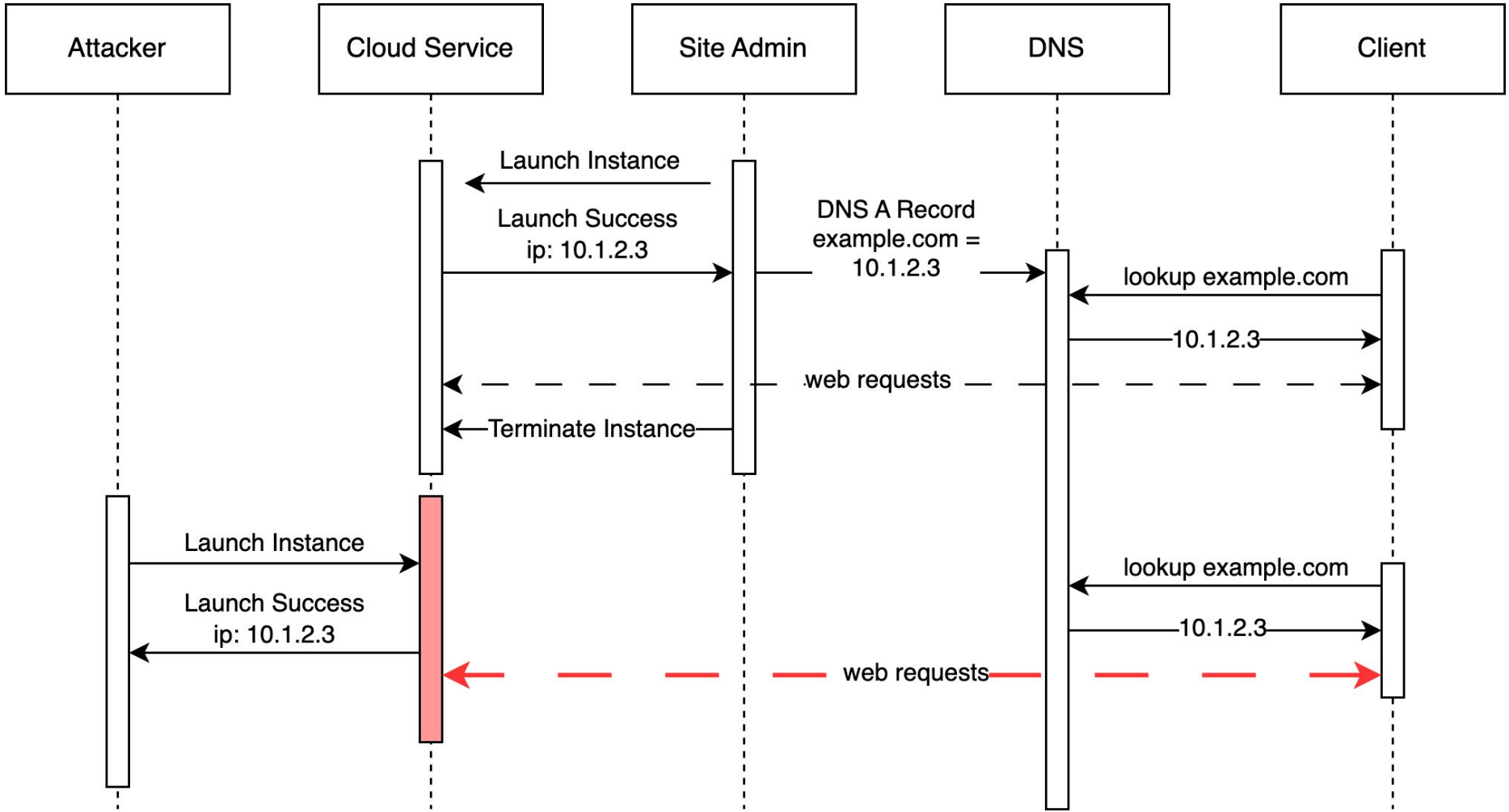
- Admin sets up a cloud instance and DNS
- Admin deprovisions it
- Attacker obtains old IP address
- Attacker receives traffic for original domain


Cloud Service
Site Admin
DNS
Launch Instance
Launch Success
ip: 10.1.2.3
DNS A Record
example.com =
10.1.2.3


Cloud Service
Site Admin
DNS
Client
Launch Instance
Launch Success
ip: 10.1.2.3
DNS A Record
example.com =
10.1.2.3
lookup example.com
10.1.2.3
web requests


Cloud Service
Site Admin
DNS
Client
Launch Instance
Launch Success
ip: 10.1.2.3
DNS A Record
example.com =
10.1.2.3
lookup example.com
10.1.2.3
web requests
Terminate Instance

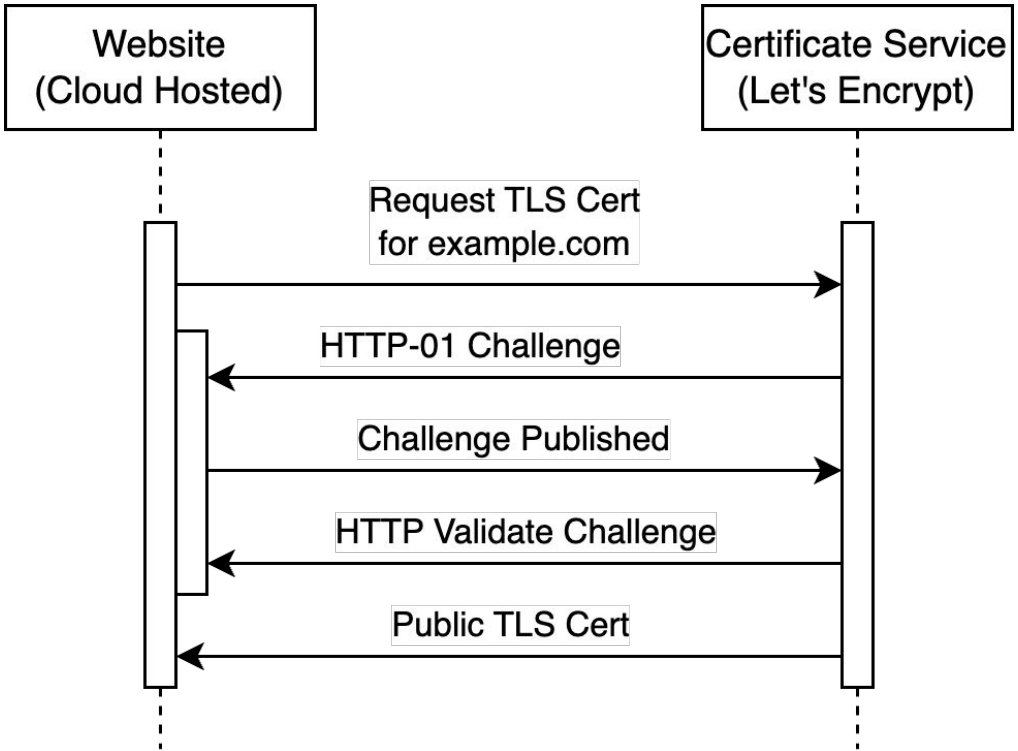

Attacker
Cloud Service
Site Admin
DNS
Client
Launch Instance
Launch Success
ip: 10.1.2.3
DNS A Record
example.com =
10.1.2.3
lookup example.com
10.1.2.3
web requests
Terminate Instance
Launch Instance
Launch Success
ip: 10.1.2.3


Attacker
Cloud Service
Site Admin
DNS
Client
Launch Instance
Launch Success
ip: 10.1.2.3
DNS A Record
example.com =
10.1.2.3
lookup example.com
10.1.2.3
web requests
Terminate Instance
Launch Instance
Launch Success
ip: 10.1.2.3
lookup example.com
10.1.2.3
web requests

Server Name Indication

- Extension in TLS Client Hello Packet
- SNI can contain plaintext hostname
- Attacker can extract this easily

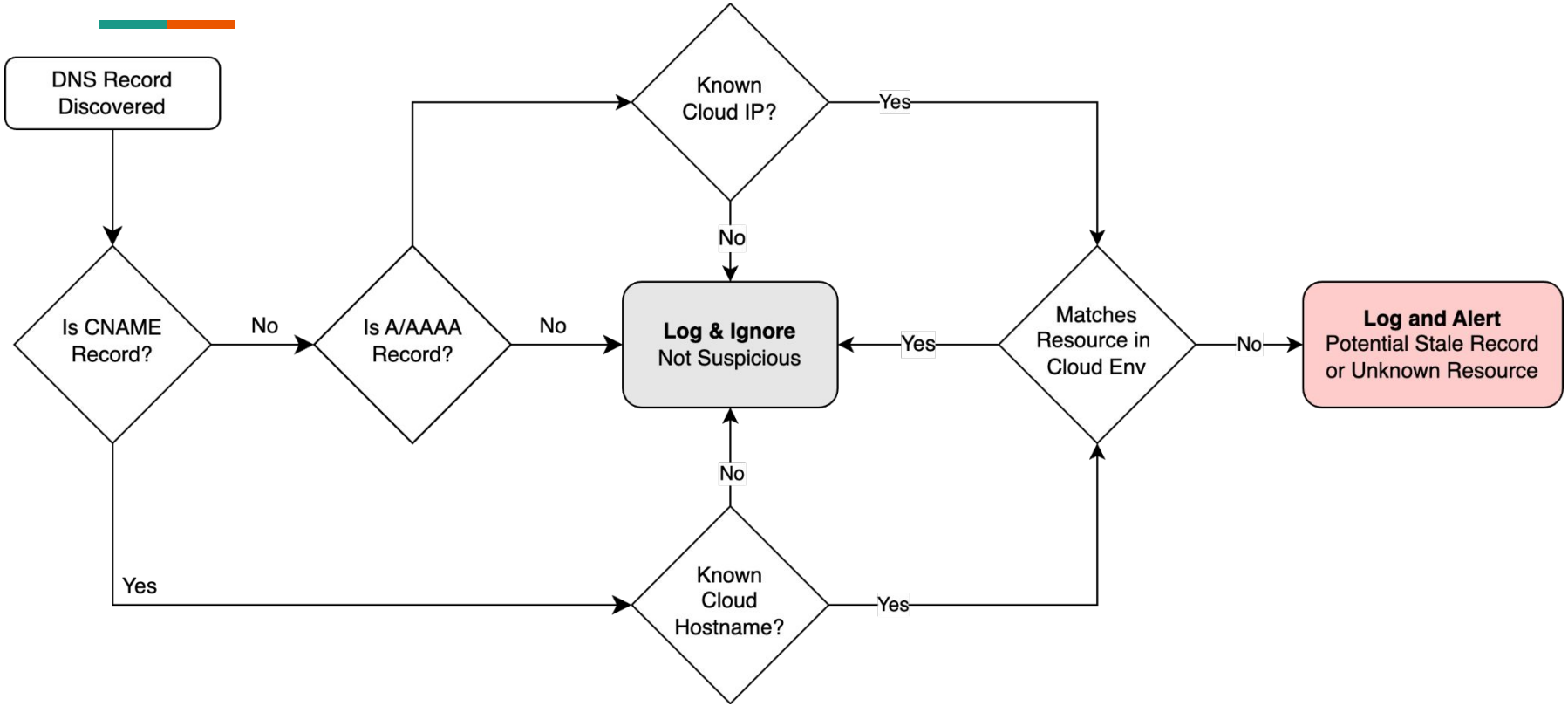
SSL Certificates via ACME Protocol



Methodology

- Enumerate all IP addresses and hostnames in cloud account
- Enumerate DNS records
- Perform classification on DNS records
- Match DNS records to cloud resources
- Alert on records for cloud resources not present in our account

Implementation - Resource Matching



Impact

- Data breaches
- Ransomware attack
- Proprietary information stolen
- Impact: Moderate to High

Likelihood

- Vulnerability information is public
- Not easy to target a specific org
- If threat event occurs, impact is high
- Rated: Moderate

Risk

- Risk: Moderate
- (Impact: Moderate * Likelihood: Moderate)

Live Demo

Mitigations & Conclusion

- Audit DNS configuration regularly
- Use Infrastructure-as-code to automate management
- Deploy CAA record to limit issuance of certificates
- Monitor Certificate logs for your domain
- Use cloud provider “BYOIP” instead of public pool

Questions?

Thank You

Sources

Digicert (n.d.). *What is DNS and how does it work?* Retrieved April 12, 2023, from https://www.digicert.com/faq/dns/what-is-dns

Pauley, E. (2022). Measuring and Mitigating the Risk of IP Reuse on Public Clouds. *43rd IEEE Symposium on Security and Privacy*. https://arxiv.org/pdf/2204.05122.pdf

Let's Encrypt (n.d.). *Letsencrypt Challenge Types*. Letsencrypt. Retrieved April 12, 2023, from https://letsencrypt.org/docs/challenge-types/

Amazon (n.d.). *Routing Traffic to EC2 Instances*. AWS Documentation. Retrieved April 12, 2023, from https://docs.aws.amazon.com/Route53/latest/DeveloperGuide/routing-to-ec2-instance.html

Terraform (n.d.). *Terraform Command: Validate*. Hashicorp Terraform. Retrieved April 12, 2023, from https://developer.hashicorp.com/terraform/cli/commands/validate

0xffsec Handbook (n.d.). *Subdomain Enumeration*. Retrieved April 12, 2023, from https://0xffsec.com/handbook/information-gathering/subdomain-enumeration/

Number Resources (n.d.). *Number resources*. IANA. Retrieved April 27, 2023, from https://www.iana.org/numbers