DNS Under Attack
The Miscreant's Offensive Playbook

Fast, Intelligent and Secure at the Edge

Moving beyond the simple & obvious DNS attacks to protect your business, your customers, and the Internet.

Version 1.3

Akamai
Experience the Edge

Agenda

Understanding our Miscreant Threat

Miscreant's "Attacking DNS" Playbook

DNS Security Wake Up Call

Understanding our Miscreant Threat

Reality of Today's Miscreant Threat

"[T]he malware that was used would have gotten past 90 percent of the Net defenses that are out there today in private industry and [would have been] likely to challenge even state government,"

Joe Demarest, Assistant Director - US FBI's Investigations Cyberdivision."

What this is really saying is that when there is a will, there is always a way to violate a system.

The Reality: Protecting DNS is Critical to Security

- 34% increase in DNS attacks
- 45% had websites compromised
- 27% experienced business downtime
- 63% suffered application downtime
- Shift from volumetric to low-signal attacks (phishing, malware, etc.)

Article: DNS Attacks Grow More Frequent and Costly
InfoSecurity, June 2019

"With an average cost of $1m per attack and a constant rise in frequency, organizations just cannot afford to ignore DNS security and need to implement it as an integral part of the strategic functional area of their security posture to protect their data and services."

- Romain Fouchereau
Research Manager, European Security
IDC

Our Traditional View of the World

The Internet is not organized based on countries. It is a group of "Autonomous System Networks" (ASNs) all interconnected in a Global Network.

The Reality of the Internet - No Borders!

How does a government enforce the rule of law where the Internet's risk are all trans-national? *We have an International Justice Problem that is not going to be solved in this decade!*

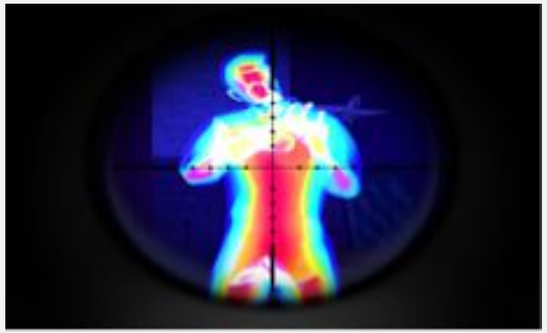
Work on the Right Security Problem

The Good Guys are the Big Part of the Security Problem! Geek out on the "miscreant widgets" forgetting there are always people behind every attack.

This is Nice to Know

The AK-47 was used to rob the bank is = to the phishing was used to get into the bank.

Who we need to Target



The people who robbed the bank were tracked via the forensic evidence with a trail that lead to arrest.

Why skull & cross bones? It is only a matter of time before miscreant mischief will lead to death as a factor of "collateral damage"

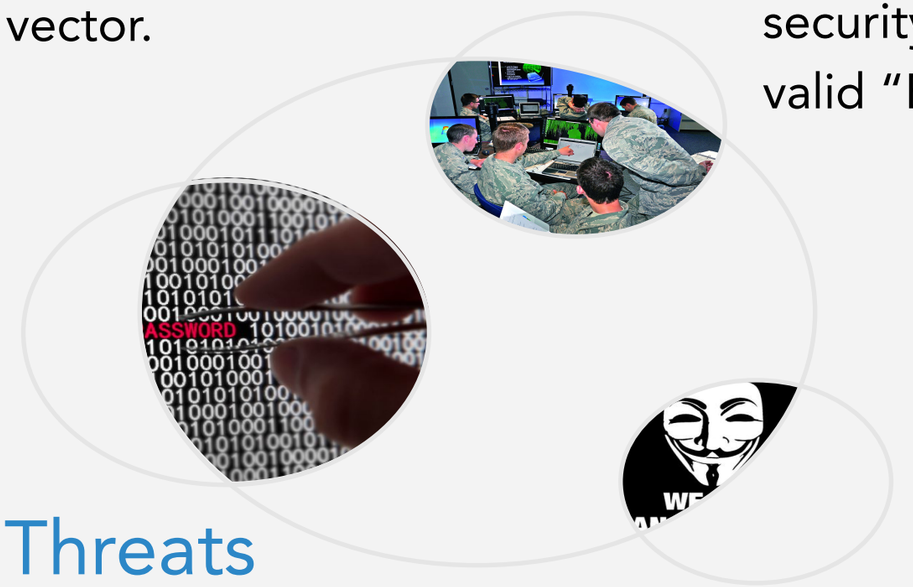
Miscreant Threat Vectors have Evolved

Corporate Threats (New!)

The dialog between US & China will accelerate the corporate on corporate threat vector.

Nation State Threats

Post-Snowden, the secret world of nation state security is now all in the open. Your network is a valid "Battle Space" for any Cyber-War.



Cyber-Criminal Threats

Cyber-Crime is an International Legal problem that has no short term resolution. There will always be someplace in the world that is a harbor for cyber-criminal activity.

Political, Patriotic, Protestors (P3)

There is always going to be someone, somewhere, who is upset with society - with the ability to make their anxiety know through any network - anywhere.

Threat Vectors: Who are the Miscreants?

Corporate / Corporate-on-Corporate Threats

The dialog between US & China will accelerate these

Nation State Threats – Now all in the open

Your network is a valid “battle space” for any cyber-war

Cyber-Criminal Threats

International legal problem with no short-term resolution

Political, Patriotic, Protestors (P3)

Always someone, somewhere, who is upset with society

Miscreant Threats are a Force of Nature

Think of the current and future security threats as a force of of the environment we live in. This is not new to human society. We have to live with the issues of nature all the time.

Like a hurricane, it is not a matter of if, but when. Even worse, you can be in a zone where the hurricane, tornado, flood, earthquake, and blizzard are all a major risk.

Forces of Nature cannot be stopped! The Only thing you can do is mitigate the risk through your design, preparation, and investment.

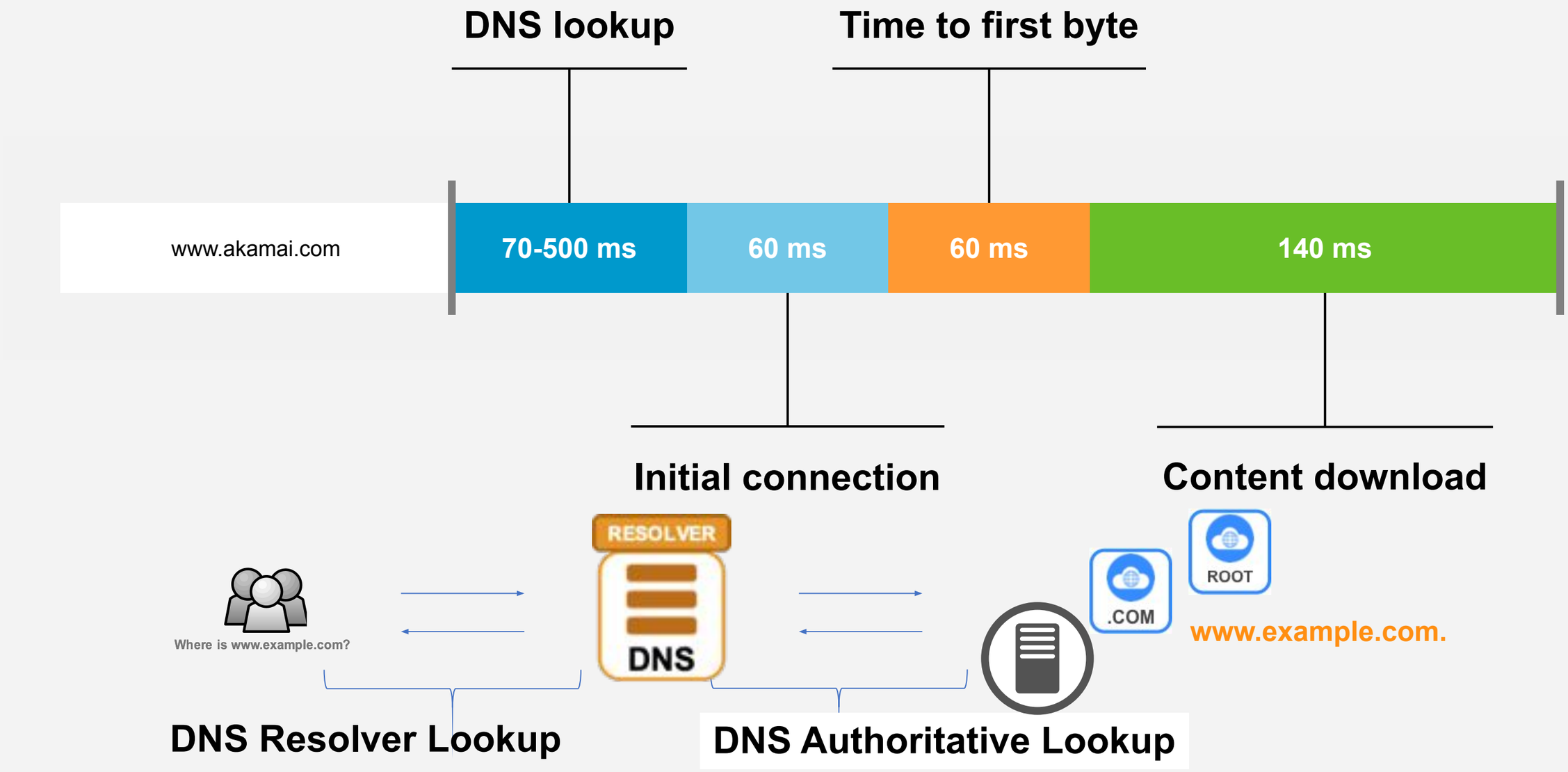
7 Habits of Highly Effective Cyber Criminals

1. Don’t Get Caught
2. Don’t work too hard
3. Follow the money
4. If you cannot take out the target, move the attack to a coupled dependency of the target
5. Always build cross jurisdictional attack vectors
6. Attack people who will not prosecute
7. Stay below the pain threshold

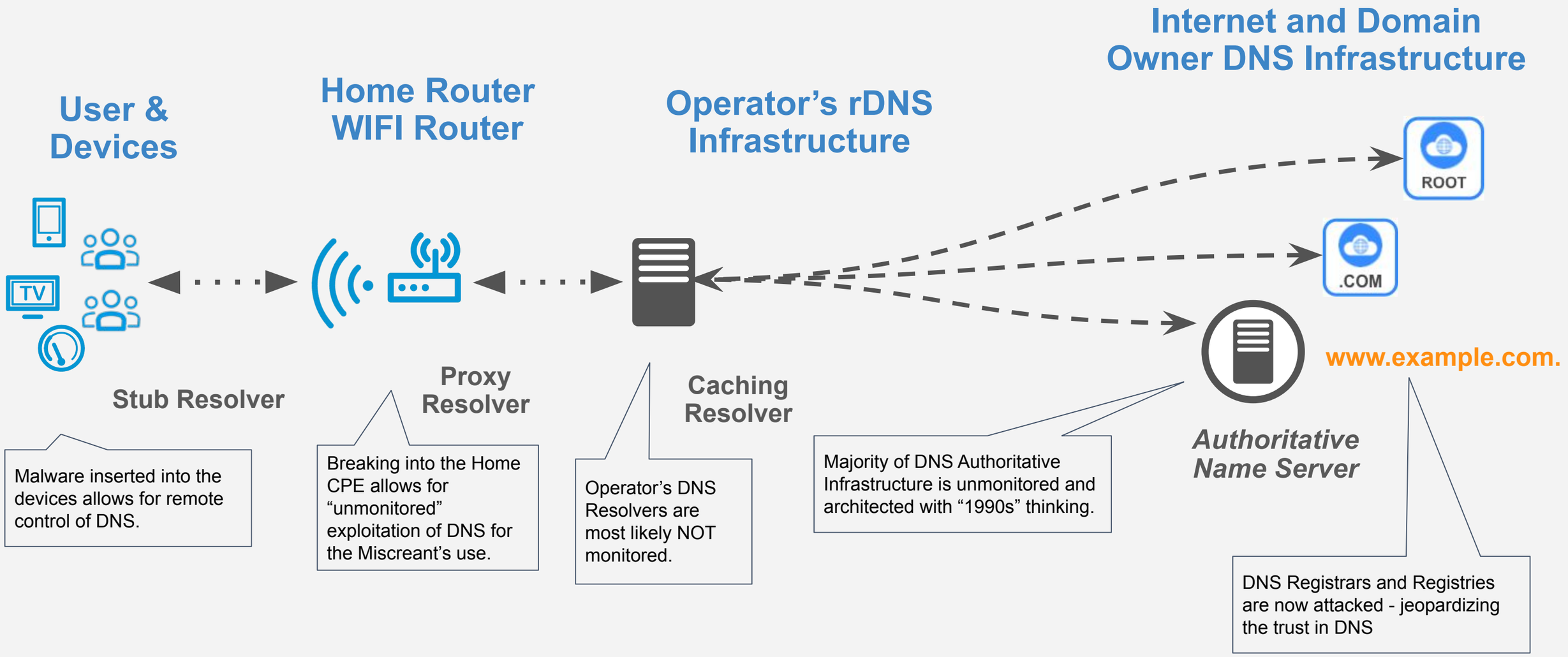
Too many miscreants work too hard to achieve their goals - not exploring the easier means to achieve their objectives.

(See the Blog & Presentations on 7 Habits of Highly Effective Cybercriminals)

DNS is Critical to Everything on the Internet



Domain Name Service (DNS) is the Miscreant's Toolkit



Miscreants “Attacking DNS” Playbook

Miscreants DNS Attack Playbook

I'm going to DoS the target

I'm going to use DNS to Collect Intel

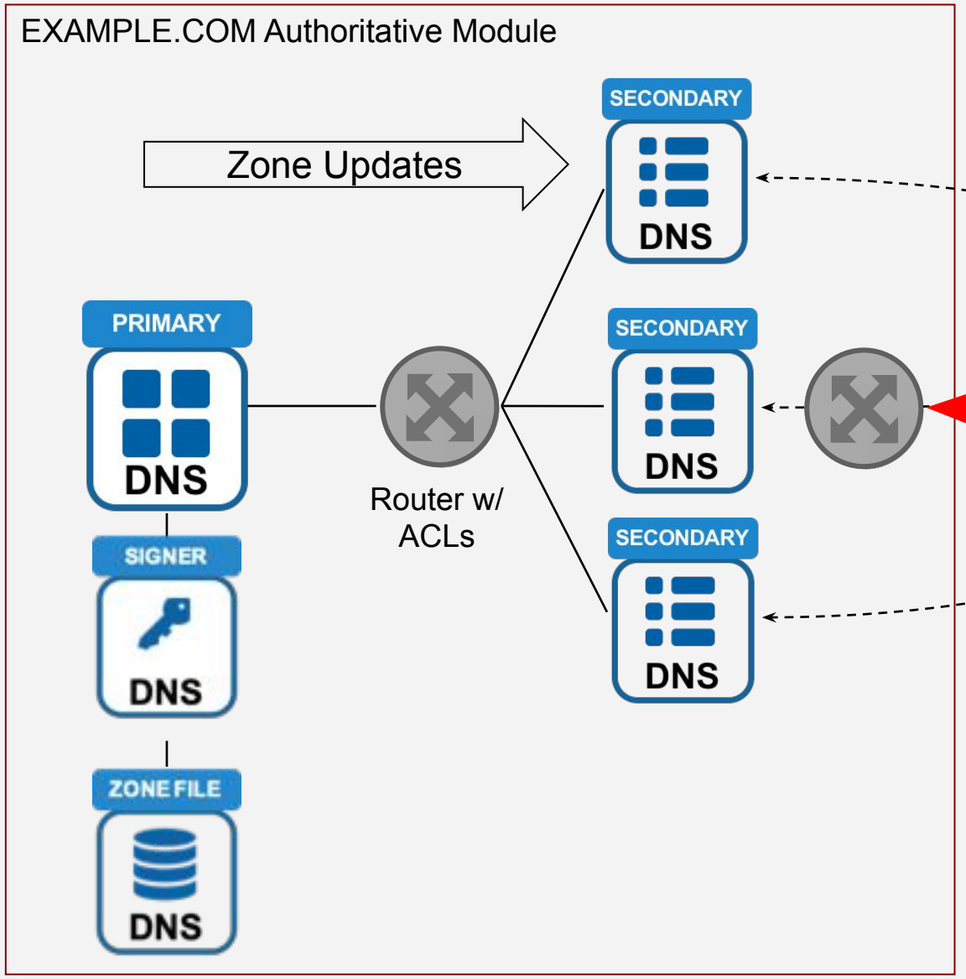
I'm going break into the Target's Admin

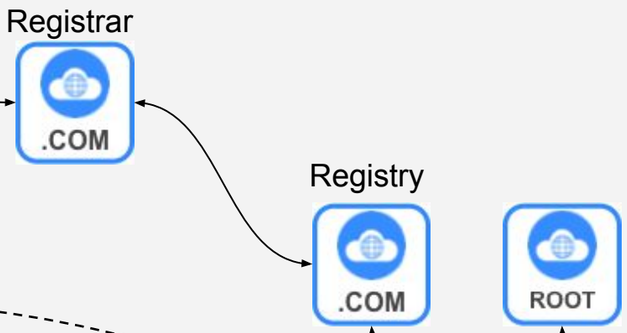
I'll use stealth 'Man in the Middle'

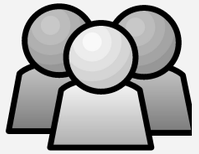
For many organizations, DNS is an "afterthought." It is neglective, not monitored, and delegated to teams who do not have the skills. This makes is ideal for Miscreants to abuse for their gain.

Example #1 - Attack the DNS Underbelly

Administrators who Managed the Domain Name for an Organization

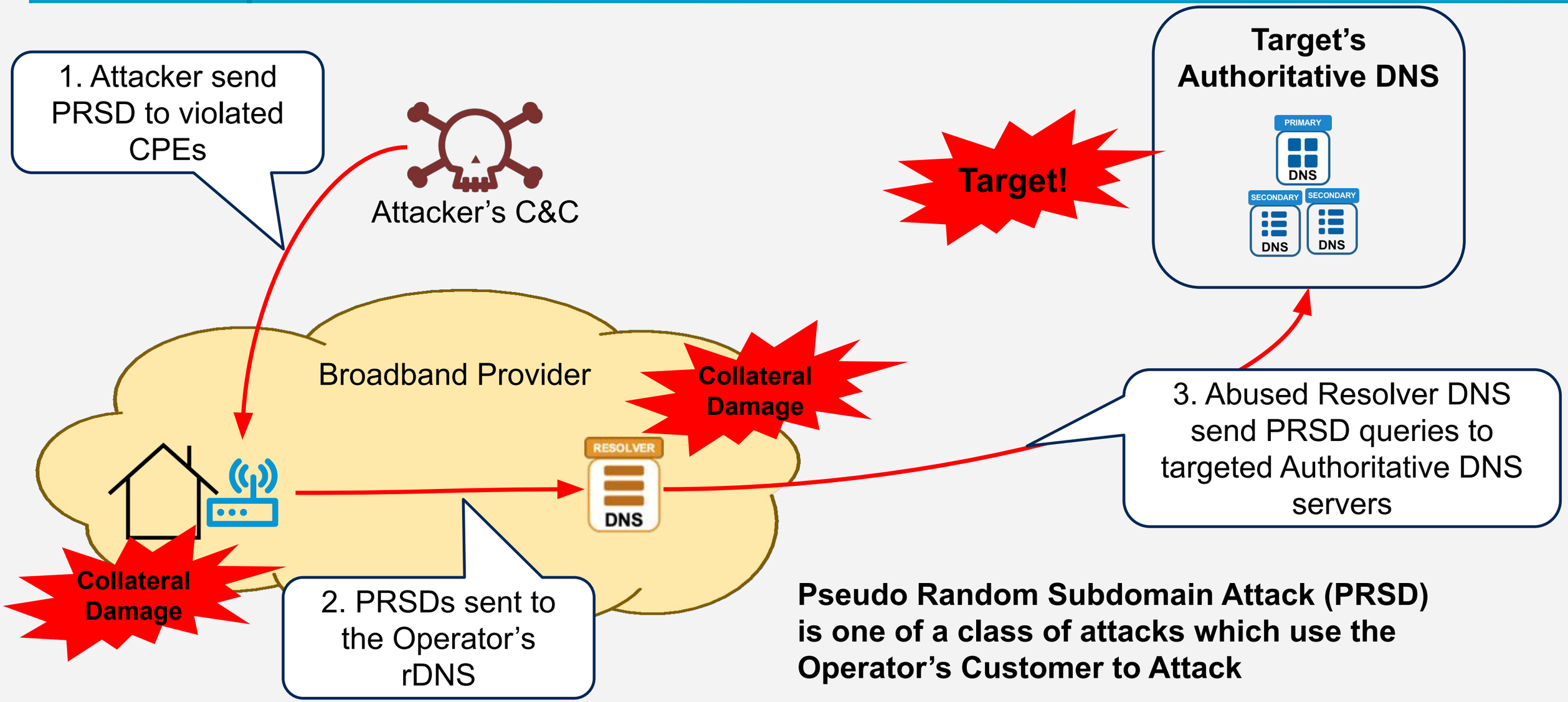






DOS Attack the Routers which Support the few public facing DNS servers.

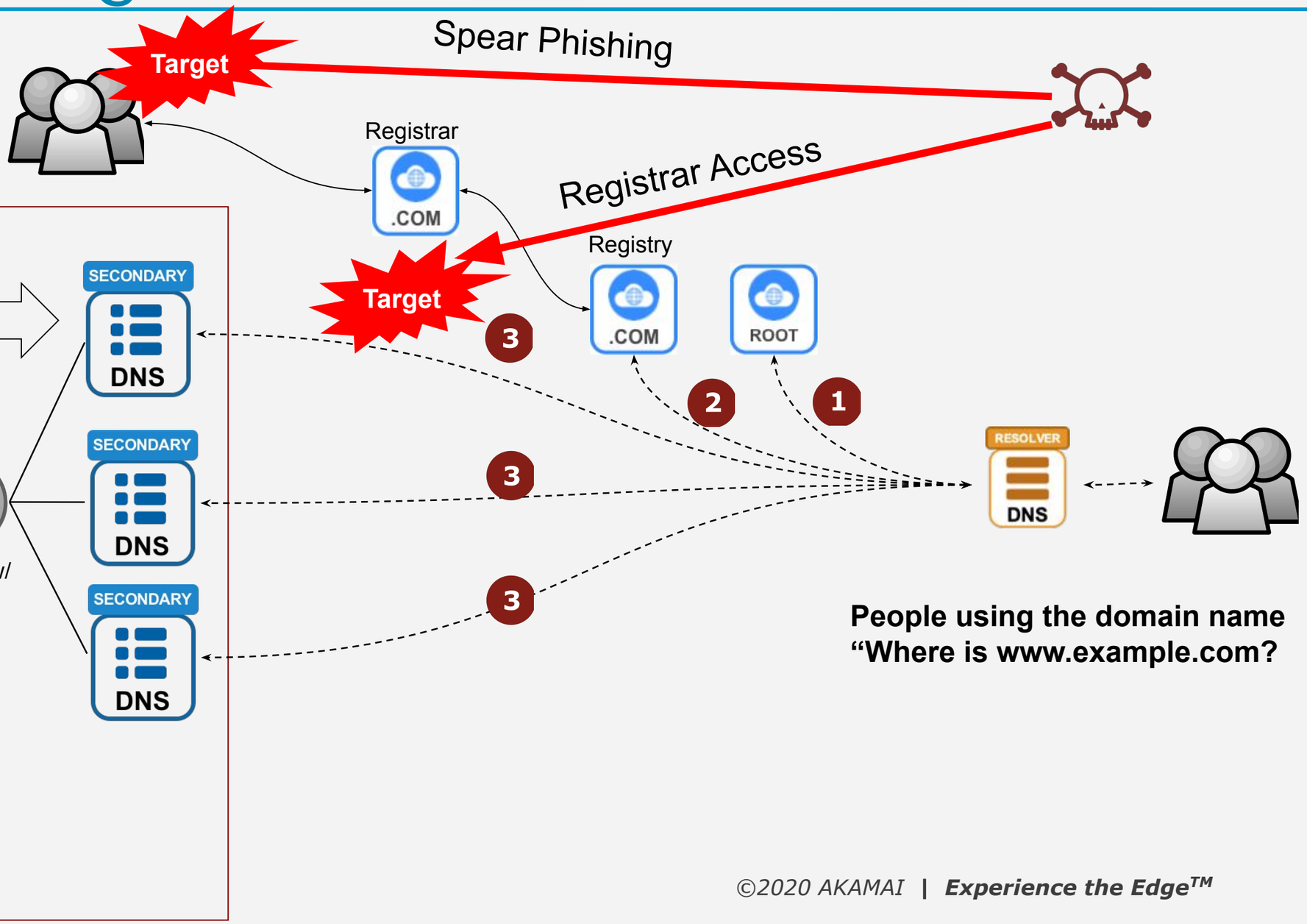
Example #2 - Use Customer to Attack



Pseudo Random Subdomain Attack (PRSD) is one of a class of attacks which use the Operator's Customer to Attack

Example #3 - Registrar Control

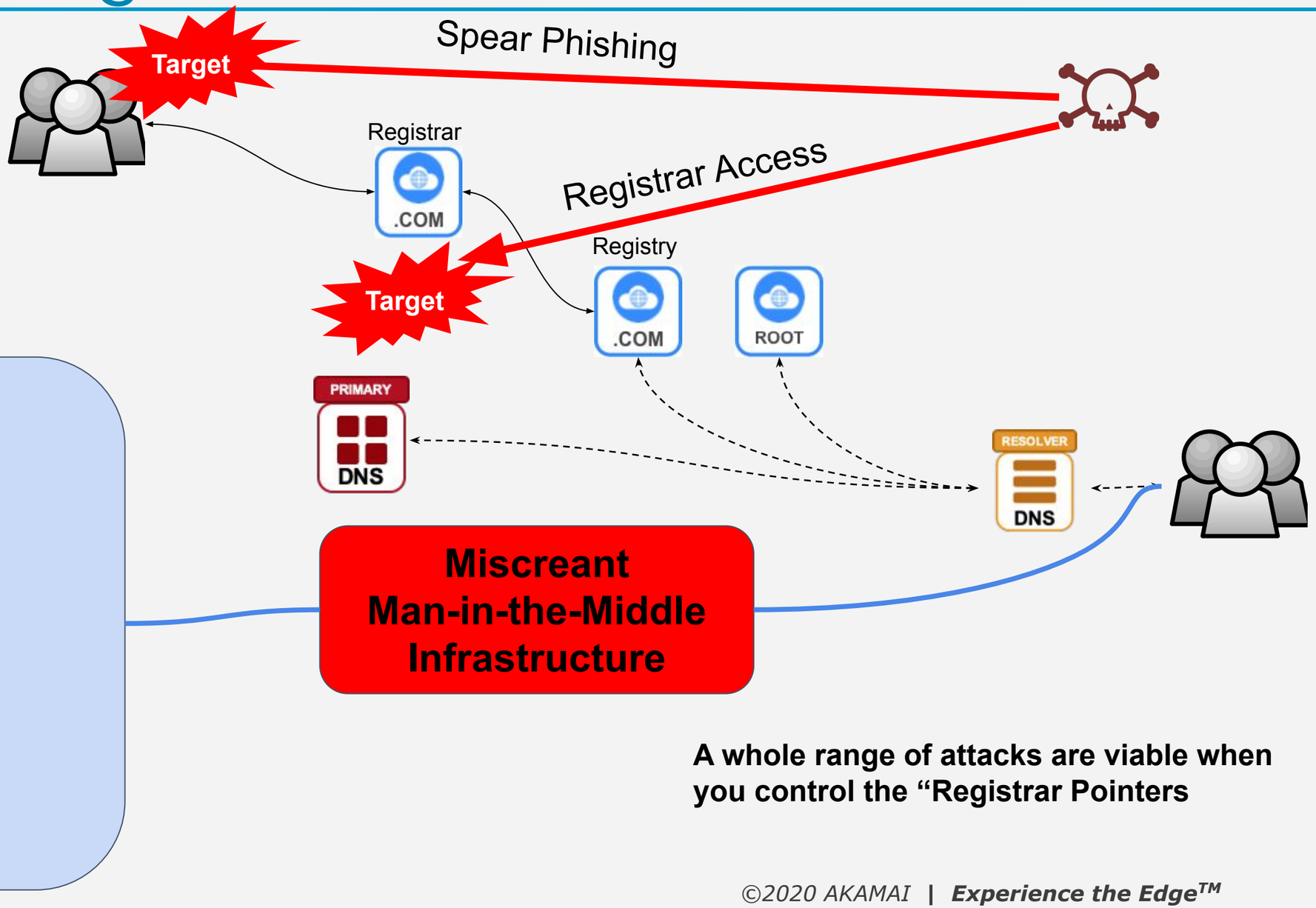
Administrators who manage the domain name for an organization.



People using the domain name "Where is www.example.com?

Example #3 - Registrar Control

Administrators who manage the domain name for an organization.

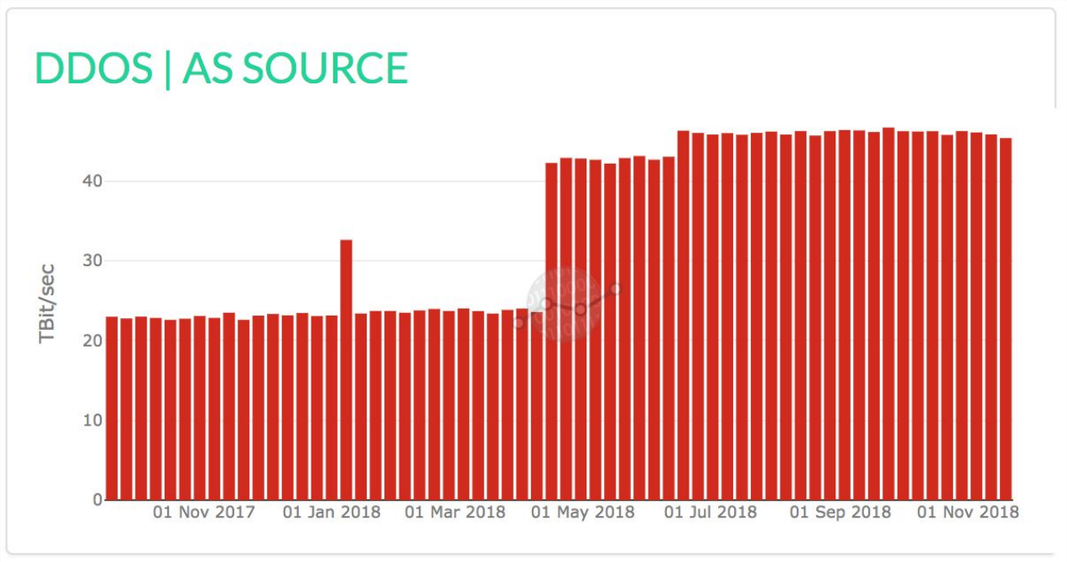


A whole range of attacks are viable when you control the "Registrar Pointers

Obvious & Overlooked Attack Vectors

Too much focus on the easy "reflection" attacks is distracting from the other attack vectors (like DNS).

- We know who, what, and where reflection amplifiers reside.
- There are efforts for Internet Security Hygiene. Once that happens - the miscreants shift their activities.



Source: https://stats.cybergreen.net/

DNS Threat will Target the Resolver

DDOS Volumetric Attack

DDOS Reflections

Collateral Malware Saturation

DDOS State Attack

DNS Poison

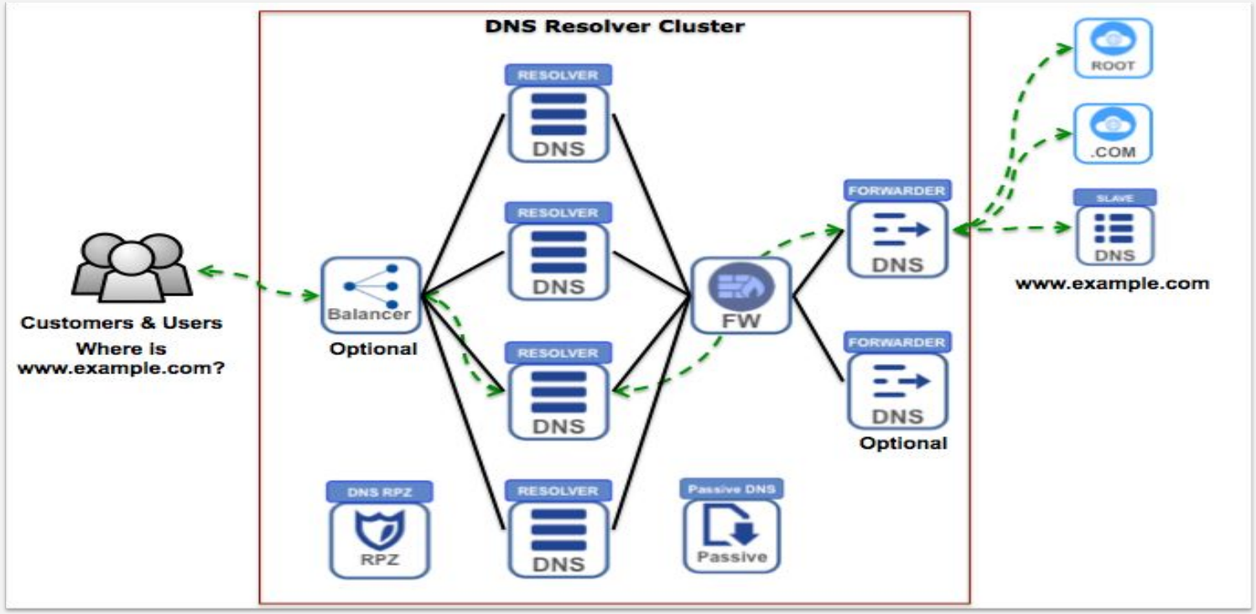
Penetration Attacks

Internal Spoofing

CPE Reflection DDOS

Inside Threats

Outside Threats



DDOS Volumetric Attack

DDOS Reflections

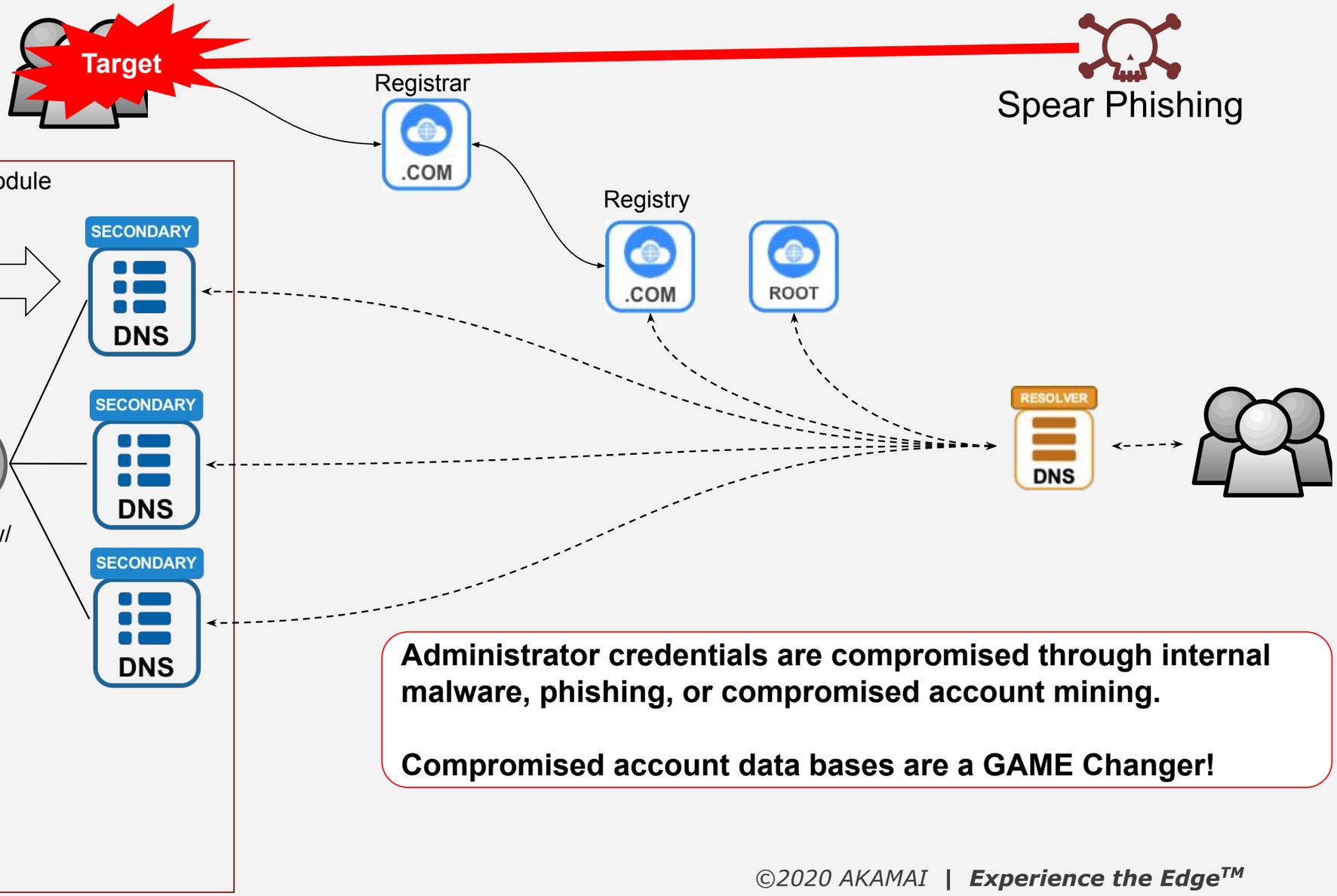
DNS Poison

DDOS State Attack

Penetration Attacks

Account Compromise

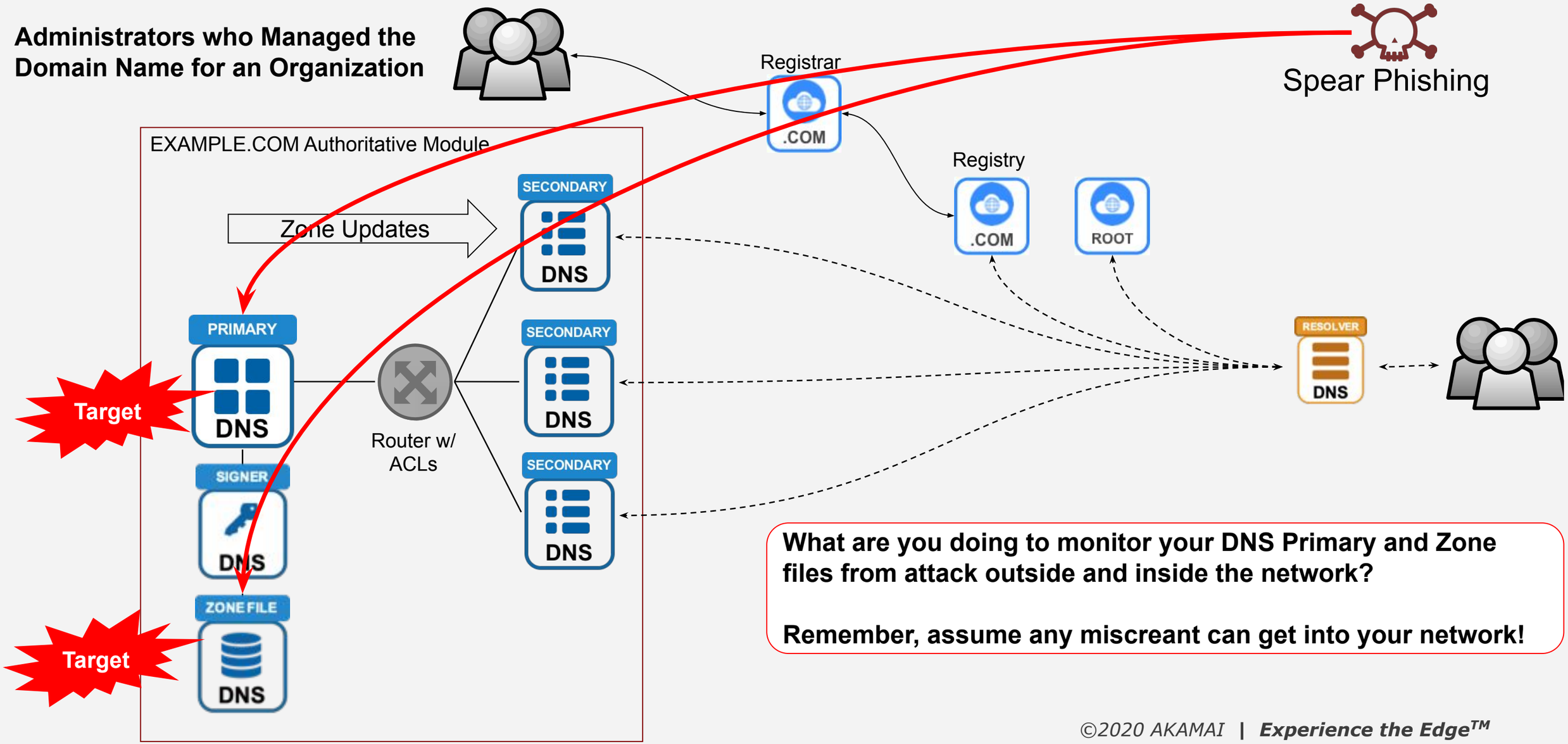
Administrators who Managed the Domain Name for an Organization



Administrator credentials are compromised through internal malware, phishing, or compromised account mining.

Compromised account data bases are a GAME Changer!

Host Compromise

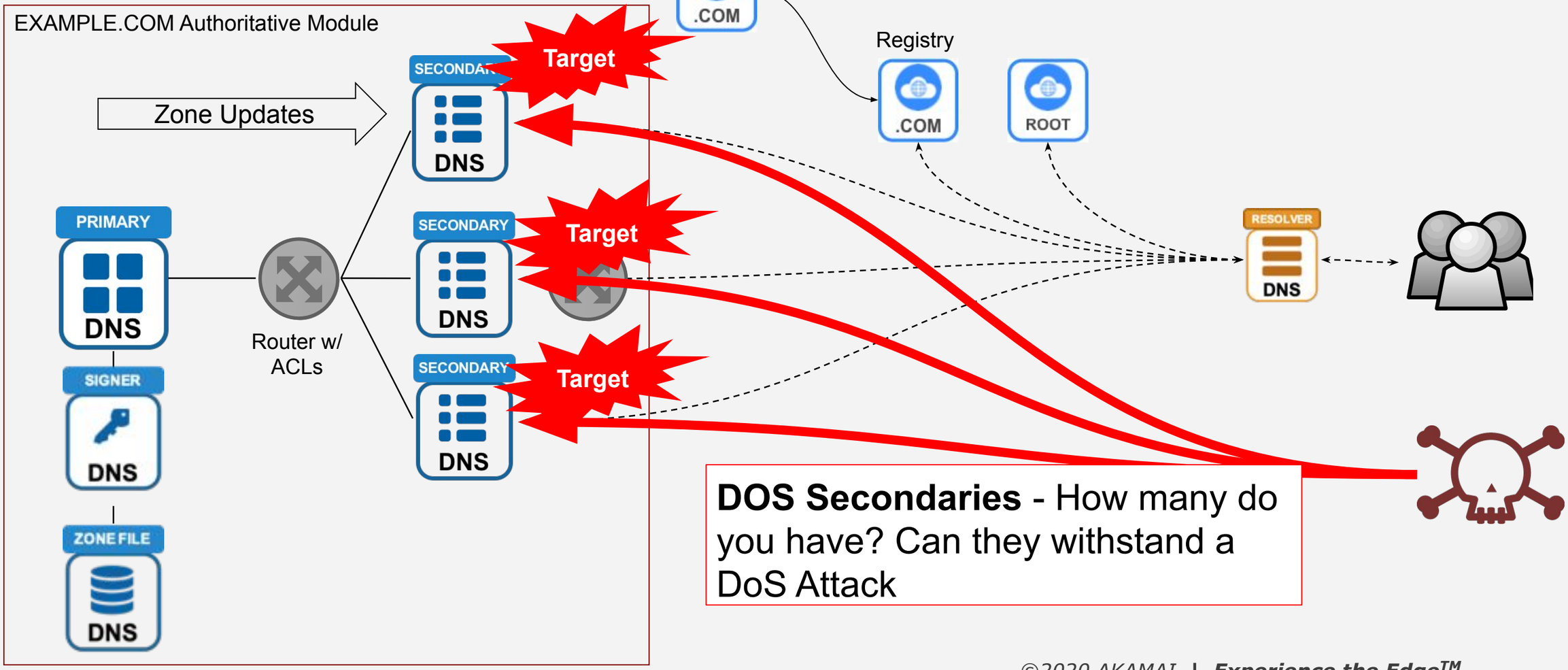


What are you doing to monitor your DNS Primary and Zone files from attack outside and inside the network?

Remember, assume any miscreant can get into your network!

DoS the Externally Visible

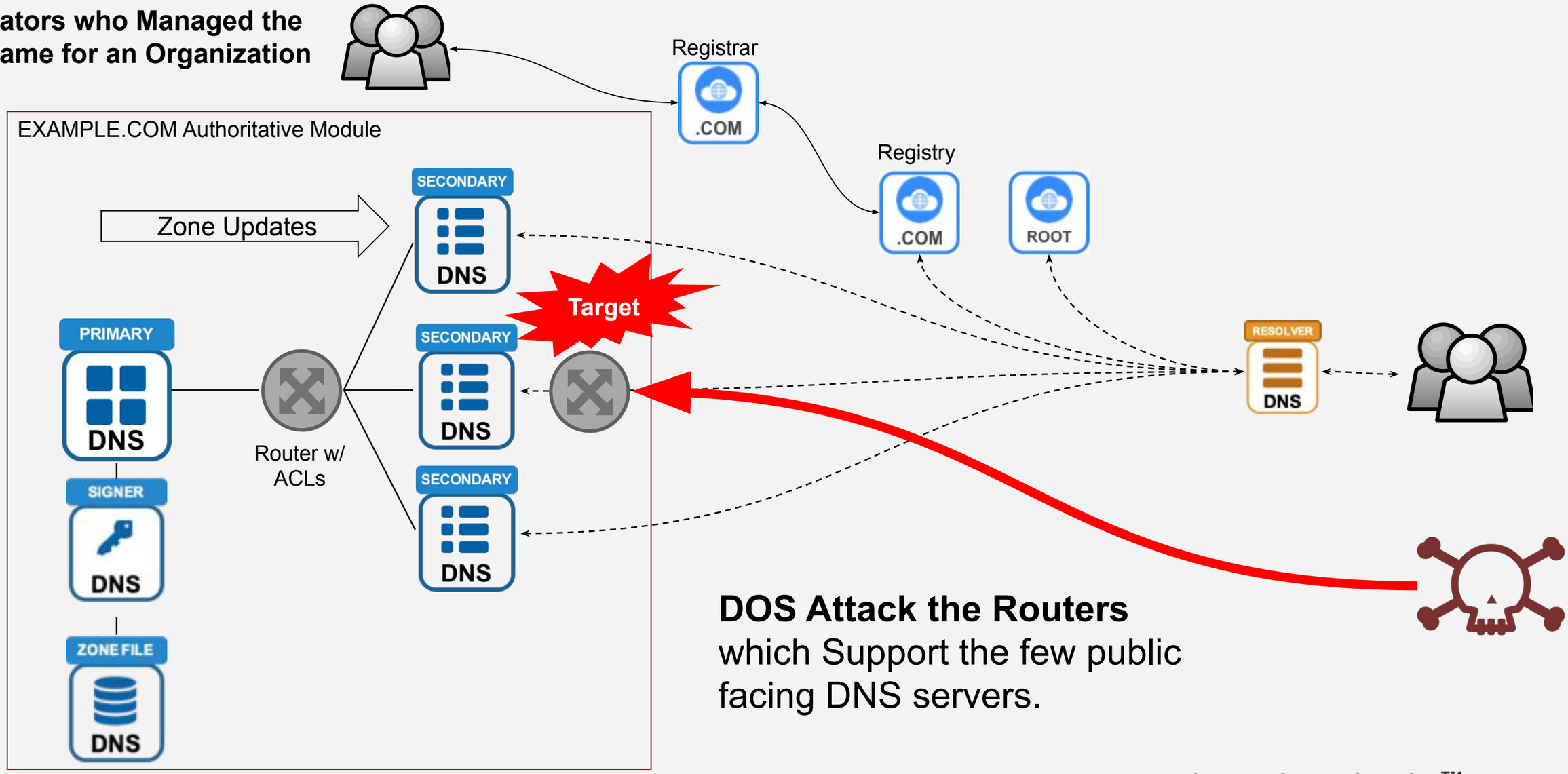
Administrators who Managed the Domain Name for an Organization



DOS Secondaries - How many do you have? Can they withstand a DoS Attack

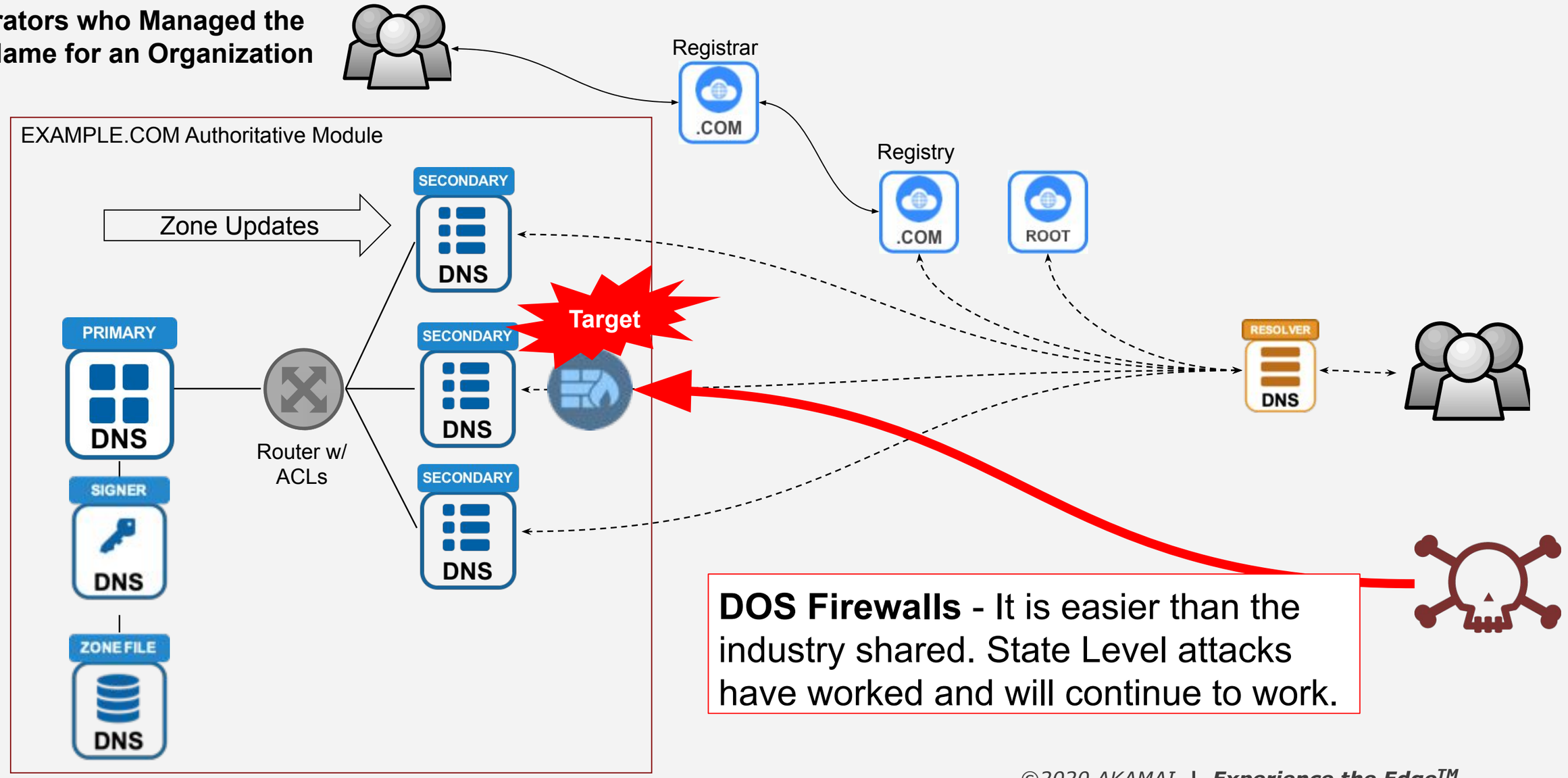
DoS the Supporting Router

Administrators who Managed the Domain Name for an Organization



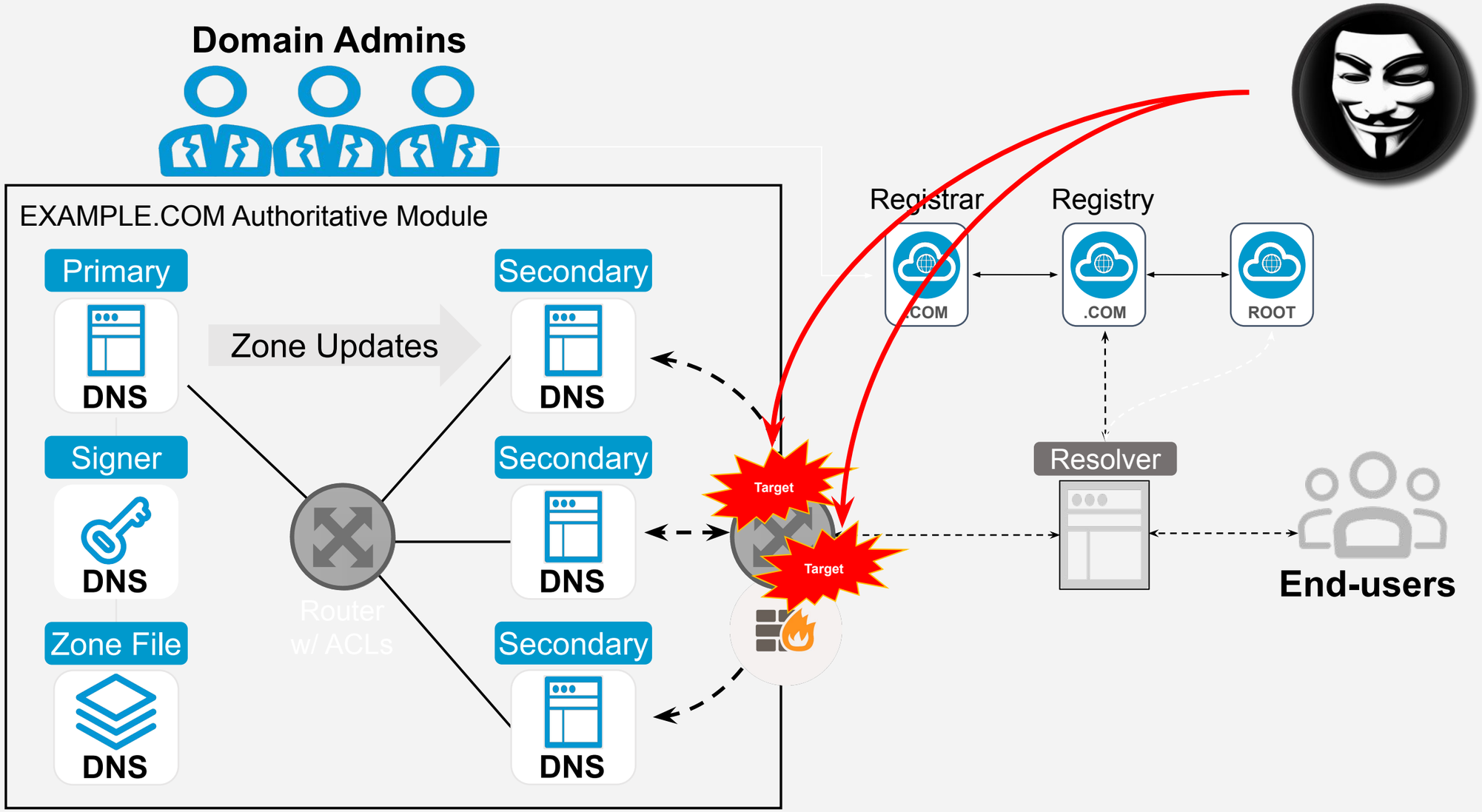
DOS Attack the Routers
which Support the few public facing DNS servers.

DoS the "Protective" Firewall / Load Balancer



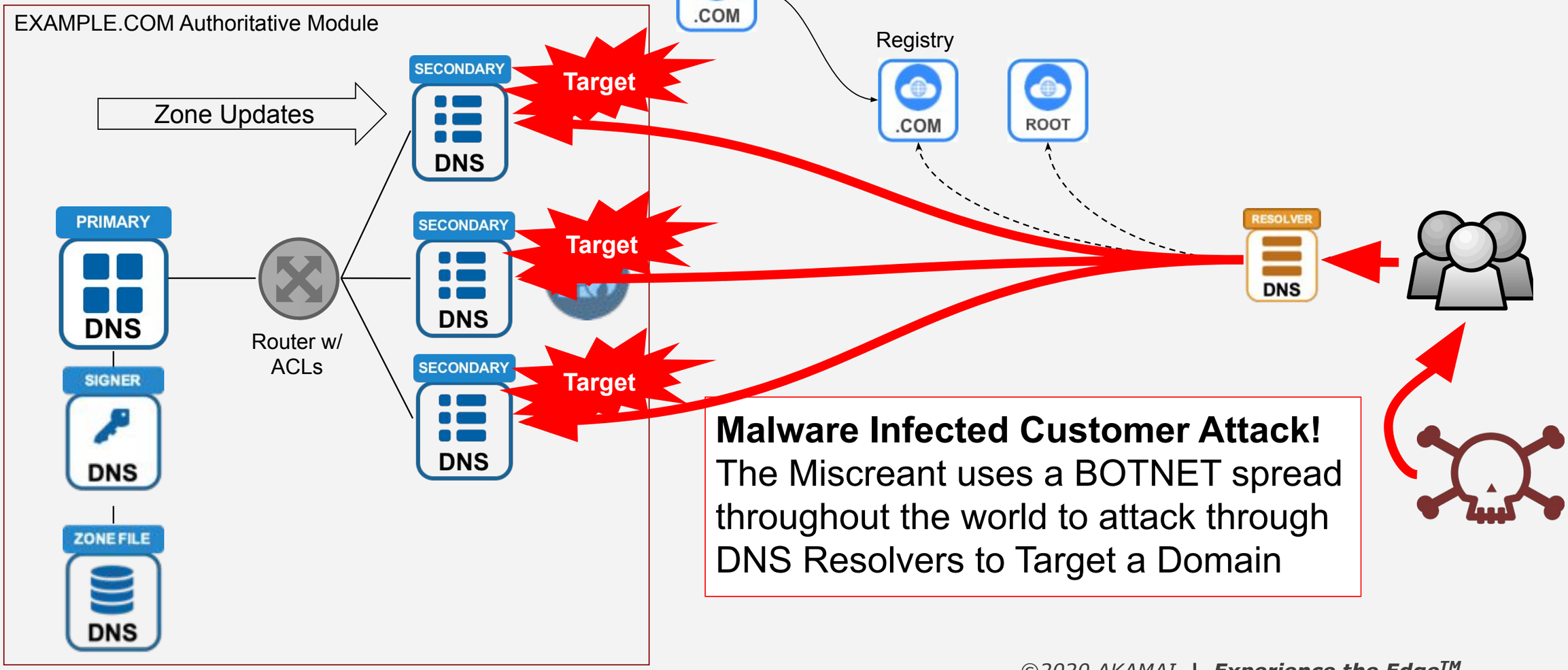
DOS Firewalls - It is easier than the industry shared. State Level attacks have worked and will continue to work.

DoS the Supporting Router and/or Firewall



Customer DoS DNS

Administrators who Managed the Domain Name for an Organization



Malware Infected Customer Attack!
The Miscreant uses a BOTNET spread throughout the world to attack through DNS Resolvers to Target a Domain

DoS DNS Registry

Administrators who Managed the Domain Name for an Organization

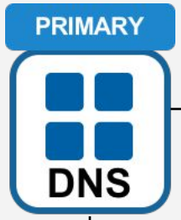
Registrar

EPP

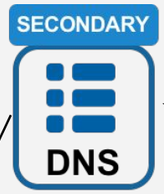
Registry

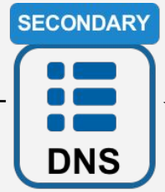
EXAMPLE.COM Authoritative Module

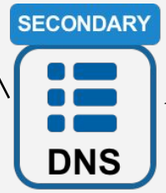
Zone Updates

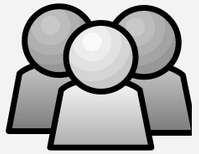


Router w/ ACLs



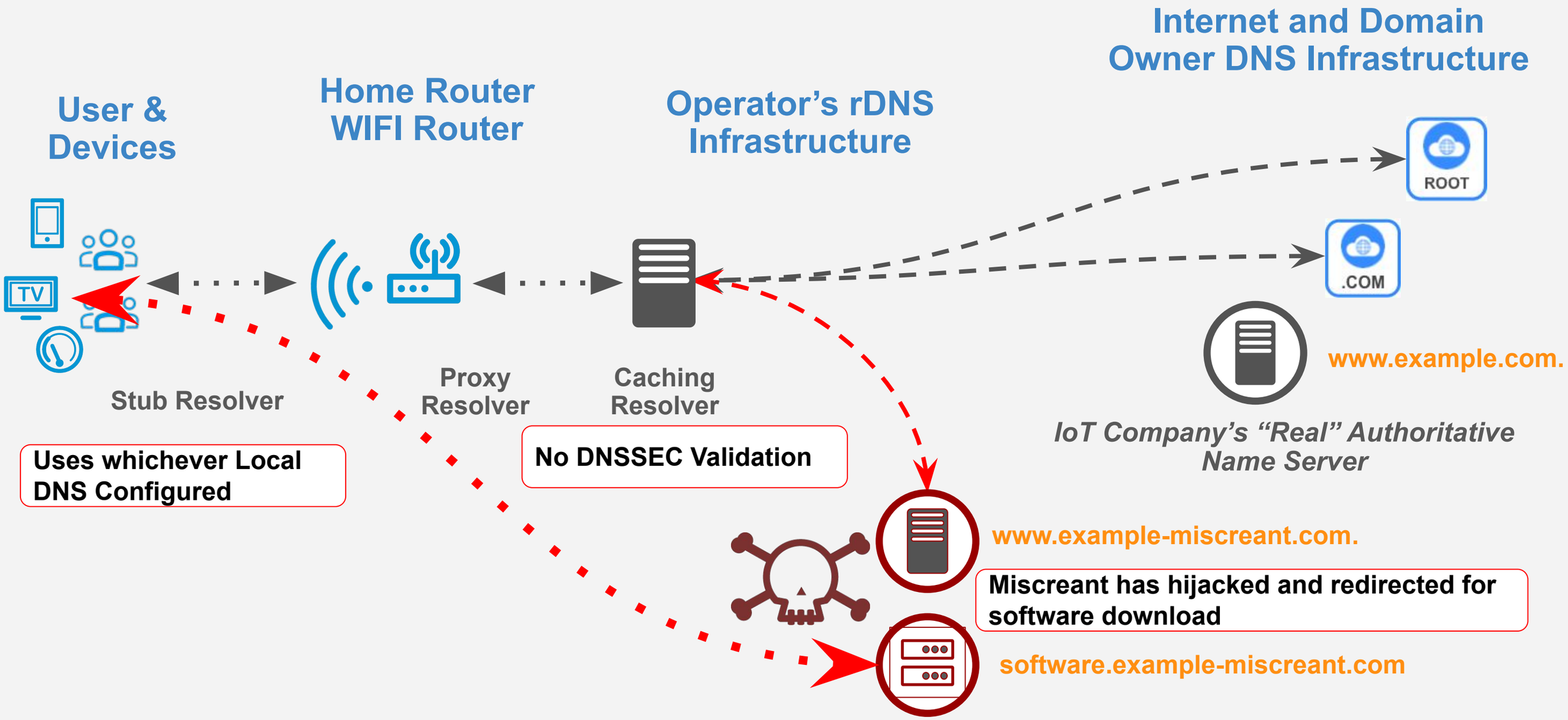






Target EPP on the DNS Registry. Ask your DNS Registry what they do to protect against these attacks?

IoT Domain Account Compromised

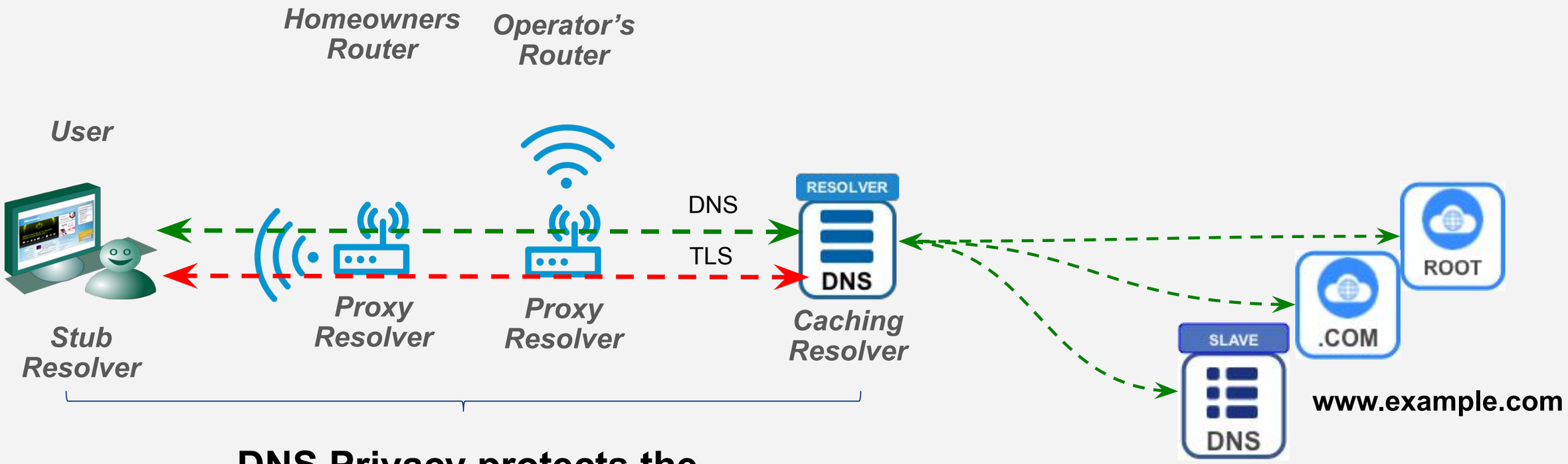


Our Future DNS Security Risk?

DNS over HTTPS and DNS over TLS will add some security while opening additional security risk.

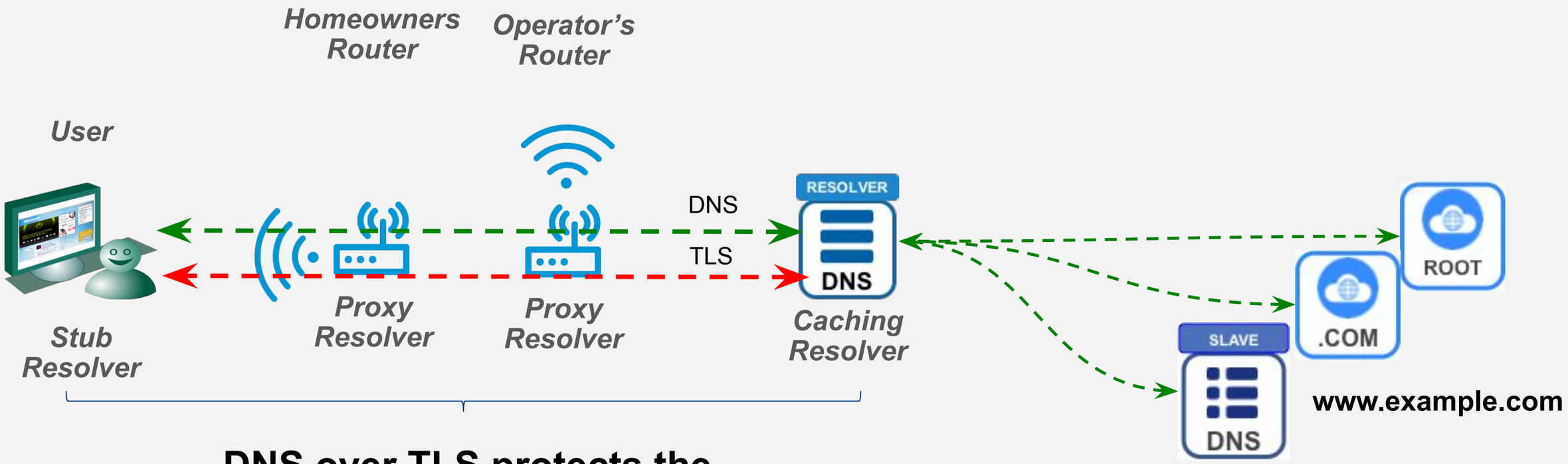
4G/5G are both open to DNS attacks that are known and unknown.

DNS Privacy (IETF)



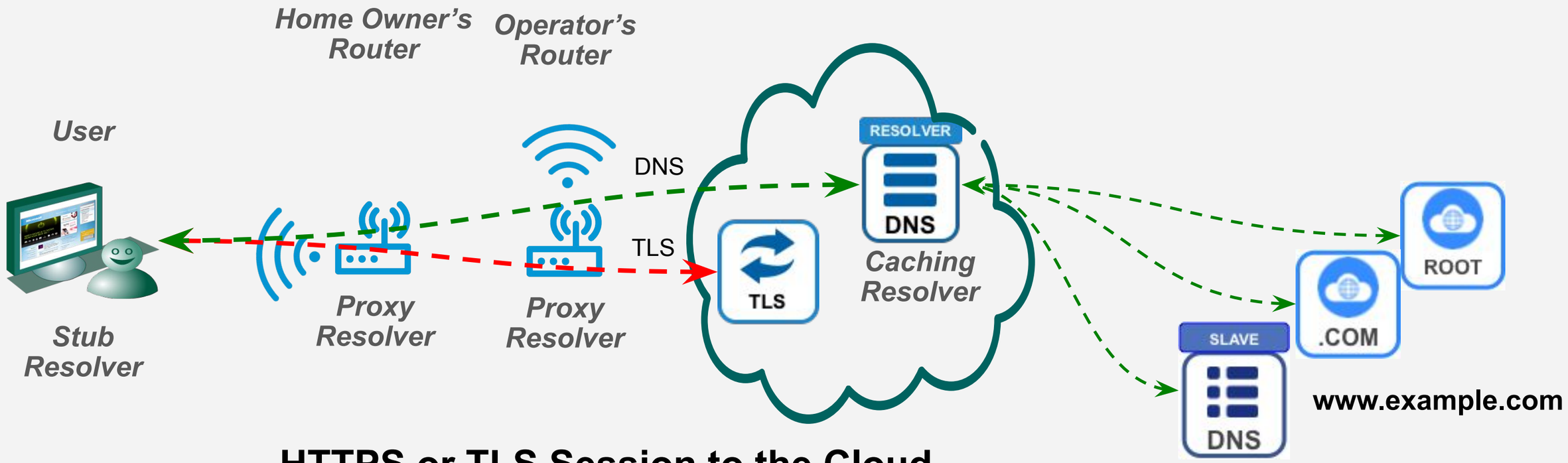
DNS Privacy protects the communications from the DNS Stub to the DNS Resolvers

DNS over TLS (DoT)



DNS over TLS protects the communications from the DNS Stub to the DNS Resolvers

DNS over HTTPS/TLS (IETF DoH WG)

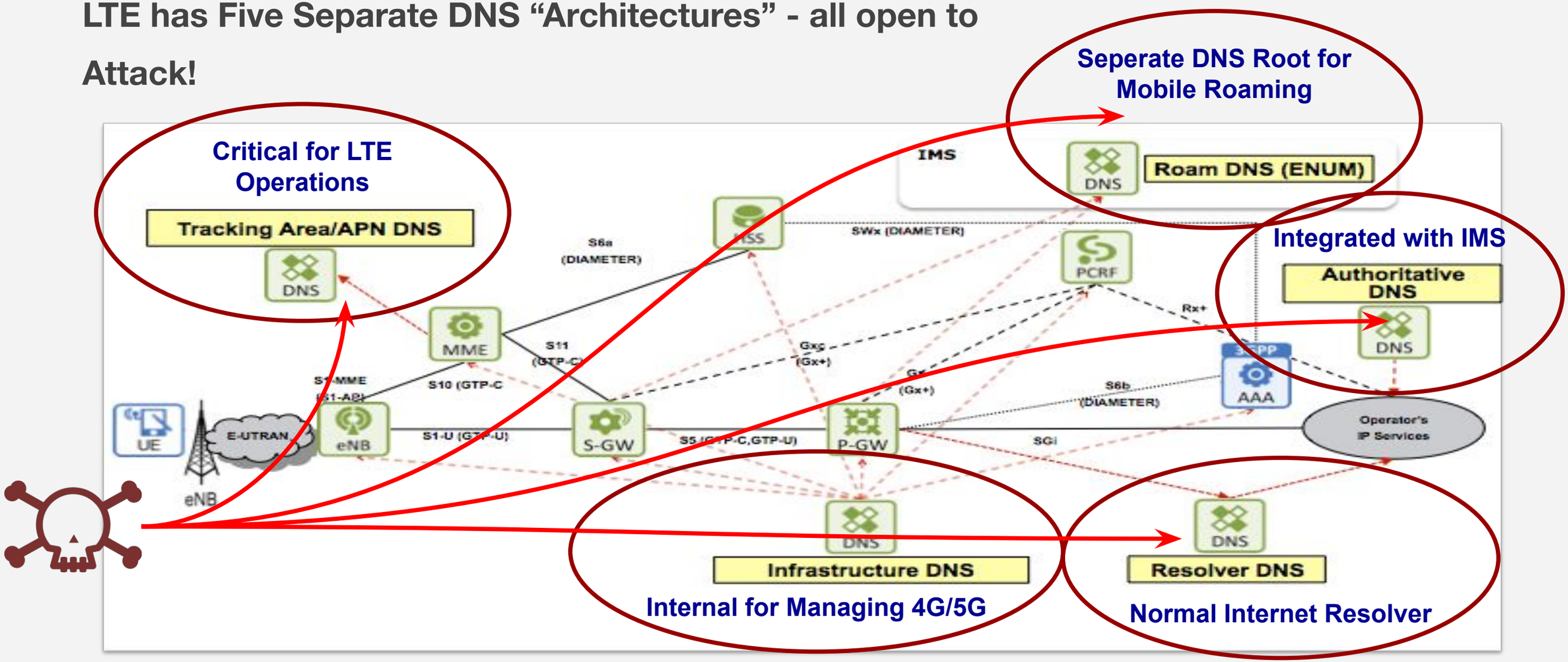


HTTPS or TLS Session to the Cloud

All DNS Queries for the Application to the rDNS in the Cloud

4G/5G's two Separate DNS Elements

LTE has Five Separate DNS "Architectures" - all open to Attack!



DNS Security Wake Up Call

Wake Up - DNS Attacked Evolution

18 FEB 19 **A Deep Dive on the Recent Widespread DNS Hijacking Attacks**

State-sponsored hackers in DNS hijacking campaign targeting government networks - Cisco Talos

Espionage campaign has compromised the websites of more than 40 organisations over the past two years

Global DNS Hijacking Campaign: DNS Record Manipulation at Scale

January 09, 2019 | by Muks Hirani, Sarah Jones, Ben Read

ANDY GREENBERG SECURITY 04.17.19 11:01 AM

CYBERSPIES HIJACKED THE INTERNET DOMAINS OF ENTIRE COUNTRIES

PayPal, Netflix, Gmail, and Uber Users among Targets in New Wave of DNS Hijacking Attacks

by Mihai Vasilescu on April 20, 2019

Industry Wake Up

We didn't have good "security action" list needed to help organizations perform a security review.

The guidance from ICANN and other organizations was confusing and not actionable.

It did not cover the gaps.

Two Critical DNS Actions

Protect your Domain Name!

- What happens when the Criminal and Political Threat Vectors start using techniques which are highlighted in the security blogs?
- Spending a day doing a domain name security review can save you from months of security headaches.

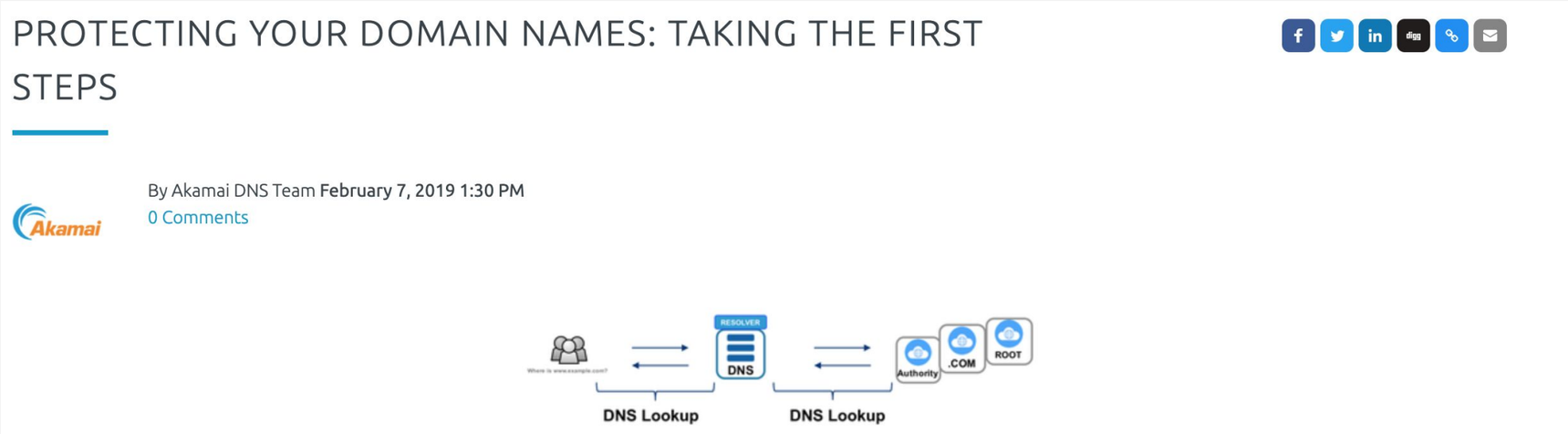
Turn your DNS Resolver into a Security Tool

- Checking all DNS transactions through your DNS Resolver is one of the most cost effective ways to add security resilience.
- It supplements all other security tools
- Resiliency against malware, botnet C&Cs, detecting threat actors, data exfiltration, phishing and other vectors are all part of turning your DNS Resolver into a security tool.

New Domain Security Checklist for Everyone

Peer reviewed guide by a combine team via Akamai to have a quick guide to help organizations review their security practices that is part of securing their domain.

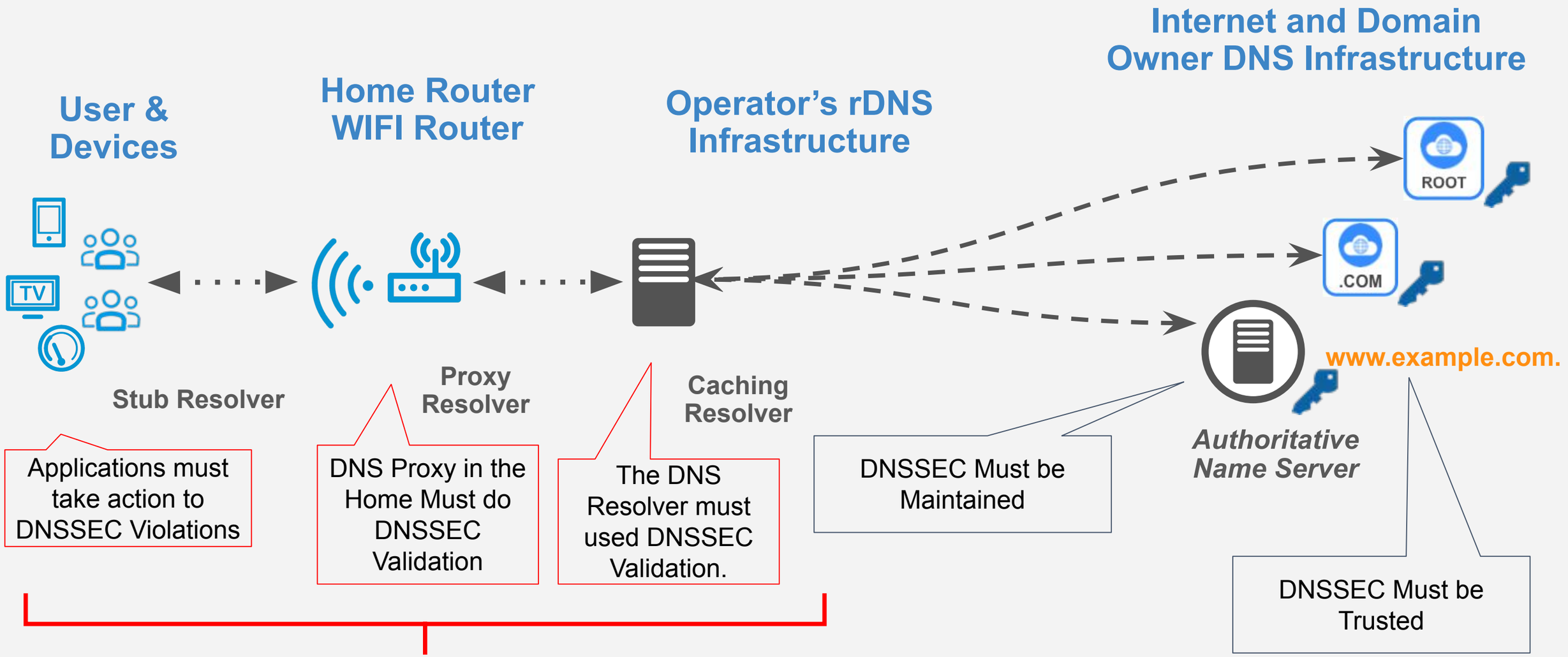
https://blogs.akamai.com/2019/02/protecting-your-domain-names-taking-the-first-steps.html



First Step to Securing your Domain?

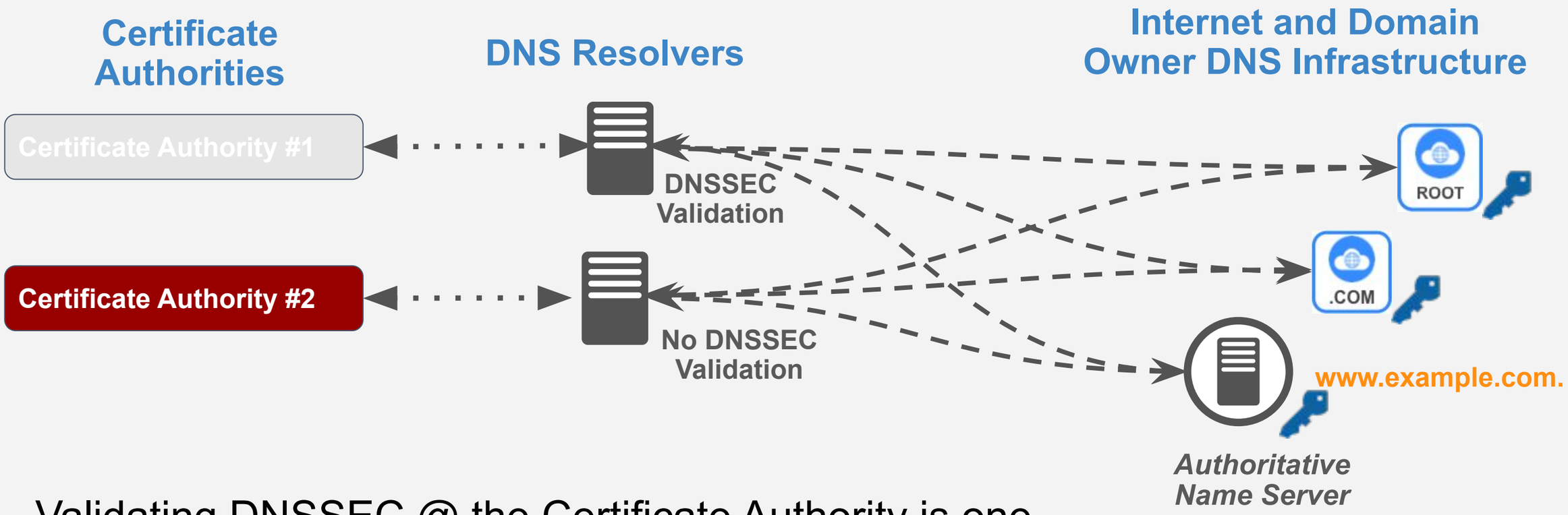
- ❑ Review Access to Domain Name Registrars
- ❑ Review DNS Roles and Responsibilities
- ❑ Employee Transitions
- ❑ Update all Registration Information
- ❑ Use Roles for Domain Registration Information
- ❑ Don't Use Personal Email Addresses
- ❑ Protect against Phishing Attacks
- ❑ Credential Updates - Change the Passwords
- ❑ Two-Factor Authentication (2FA) for Registrar Accounts
- ❑ Understand Registrar Security Policies, Tools, and Processes
- ❑ Review the Privacy Registration Options
- ❑ Review and Maintain Records in your Zone
- ❑ Name Server and Zone File Best Practices
- ❑ DNS Zone File Revision Control
- ❑ Is your Domain Locked at the Registrar?
- ❑ Hope for the best; plan for the worst

Why is DNSSEC Missing from the First Round?



What is missing in large parts of the Internet!

Other tools Must Validate DNSSEC



Validating DNSSEC @ the Certificate Authority is one way to add Security Resiliency to the Architecture.

Next Step and Questions

Articles Exploring DNS Security

- Protecting Your Domain Names - Taking First Steps
- Architecting DNS for DDoS Durability and Resiliency
- Global Traffic Management for Cloud Data Centers and CDNs
- Traffic Management for Peace of Mind
- Fast DNS Secondary Implementation: Order or Operations for NS Zone and Registrar Records
- When "Customers" Attack DNS
- Deployment Diversity for DNS Resiliency

Akamai

Experience the Edge