CHECK POINT

Hacking DNS

Understanding DNS Security

Hubert Ralph Bonnell | Security Engineer, Check Point Software

July 2023

YOU DESERVE THE BEST SECURITY

Agenda

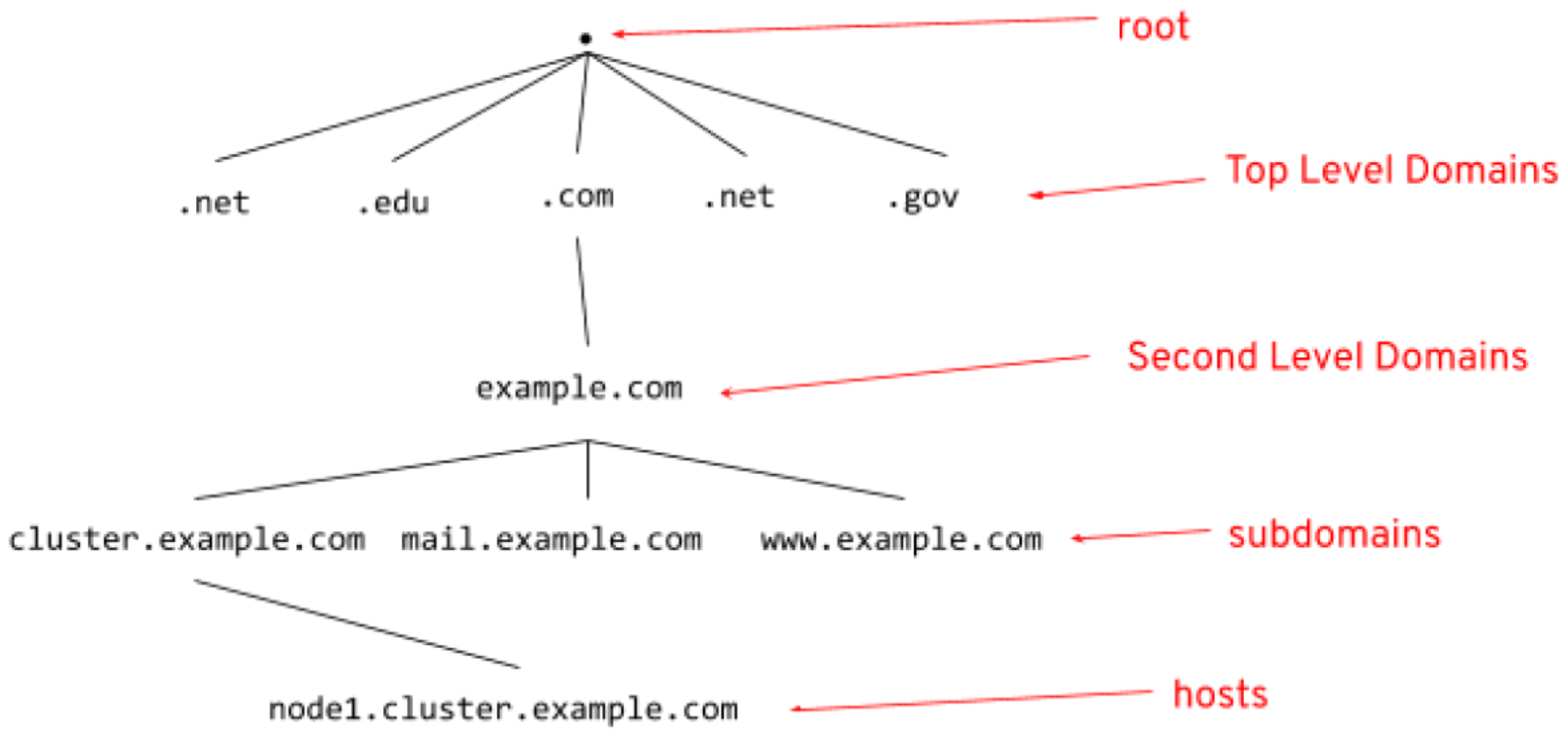
- DNS 101
- DNS Attacks
- DNS Best Practices

DNS 101

DNS 101

- Client Initiates a DNS Lookup on Protocol UDP, Port 53
- DNS Server Types
  - Recursive Resolver
  - Root Nameserver
  - TLD (Top Level Domain) Nameserver
  - Authoritative Nameserver
- BIND (Berkeley Internet Name Domain) Software, version 9
- DNS is defined by the IETF in RFCs 1034 and 1035
  - Published in 1987, updating older ones from 1983, introduced in RFC 805, 1982

DNS 101

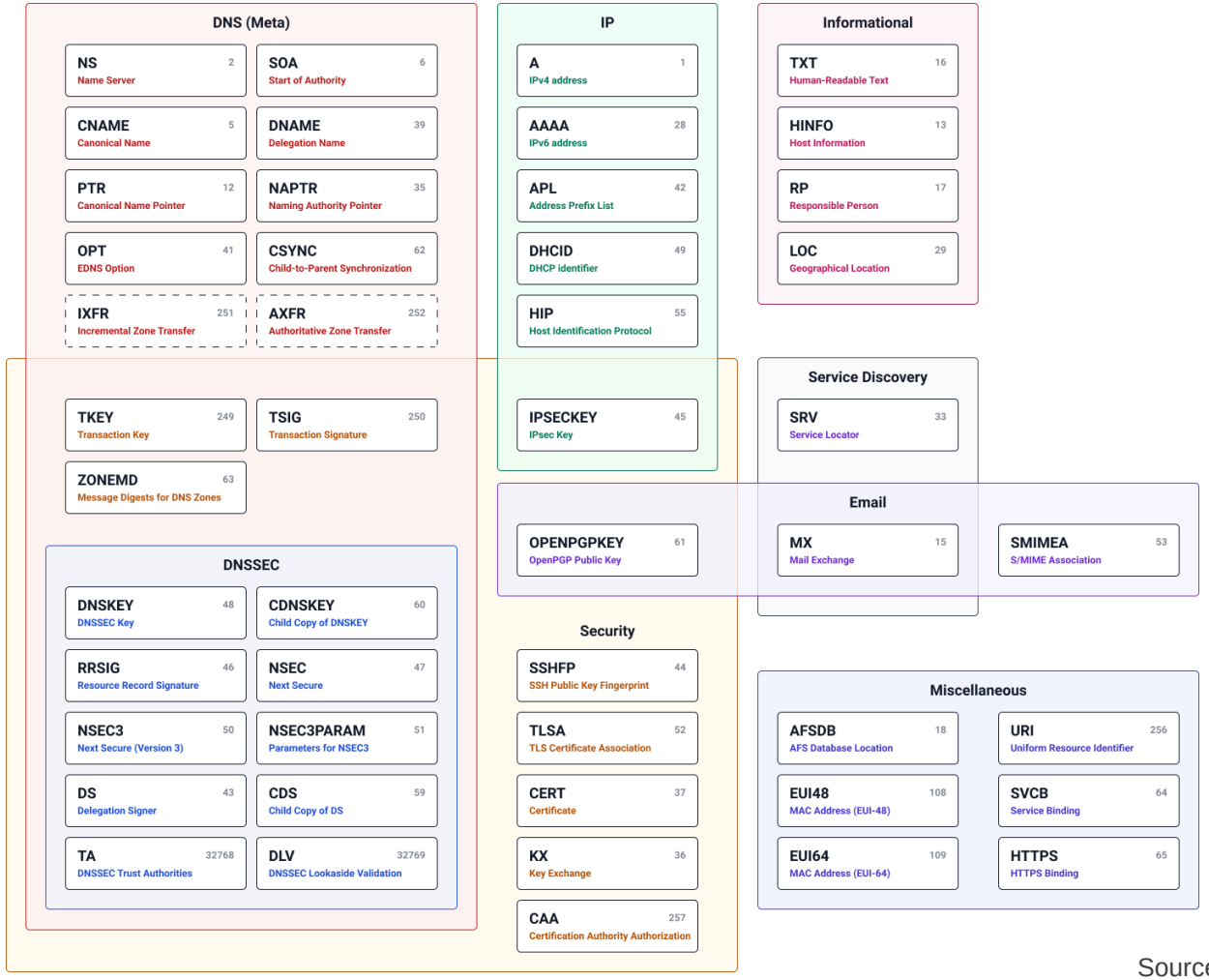


DNS 101

- DNS components
  - Domain namespace
  - Name Servers
    - Zone files
    - Master and Slave Servers
  - Resolvers
- Types of DNS Queries
  - Recursive Query
  - Iterative Query
  - Non-Recursive Query

- Common Record Types
  - **A** — IPv4 address
  - **AAAA** — IPv6 address
  - **CNAME** — Canonical name
  - **MX** — Mail exchange
  - **NS** — Name server
  - **TXT** — Human-readable text
  - **SOA** — Start of authority
  - **PTR** — IP Address of a Domain

DNS 101



Source: https://www.nslookup.io/learning/dns-record-types/

DNS 101

- Time to Live (TTL)
  - Zone File Header (Example)
  - $ORIGIN example.com. ; This marks the beginning of the file
    $TTL 86400 ; TTL is 24 hours , it could also be 1d or 1h
    example.com IN SOA ns1.example.com. webmaster.example.com. (
    2023052201 ; serial number of this zone file
    2d ; refresh time for slave
    5h ; retry time for slave
    2w ; expiration time for slave
    1h ; maximum caching time
)
- Caching
  - Browser Caching
  - Operating System Caching
  - Recursive Resolver Caching

DNS Lookups

- Tools
  - Windows: **nslookup**

```
C:\Users\myusername>nslookup
Default Server:  UnKnown
Address:  127.0.0.1

> ralphbonnell.com
Server:  UnKnown
Address:  127.0.0.1

Non-authoritative answer:
Name:    ralphbonnell.com
Address:  44.206.122.150
```

DNS Lookups

- Tools
  - Linux or MacOS: **dig**

```
myusername@mydebianbox:~$ dig ralphbonnell.com
; <<>> DiG 9.16.37-Debian <<>> ralphbonnell.com
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 45134
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1
;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 1232
;; QUESTION SECTION:
;ralphbonnell.com.              IN      A
;; ANSWER SECTION:
ralphbonnell.com.       84457   IN      A       44.206.122.150
;; Query time: 3 msec
;; SERVER: 10.250.240.3#53(10.250.240.3)
;; WHEN: Sun May 21 20:33:23 PDT 2023
;; MSG SIZE  rcvd: 61
```

DNS Lookups

- Tools
  - **whois**

WHOIS search results

- Domain Name: CHECKPOINT.COM
- Registry Domain ID: 68307_DOMAIN_COM-VRSN
- Registrar WHOIS Server: whois.domainthenet.com
- Registrar URL: http://www.DomainTheNet.com
- Updated Date: 2023-02-28T04:32:14Z
- Creation Date: 1994-03-29T05:00:00Z
- Registry Expiry Date: 2024-03-30T04:00:00Z
- Registrar: Domain The Net Technologies Ltd.
- Registrar IANA ID: 10007
- Registrar Abuse Contact Email: abuse@dtnt.com
- Registrar Abuse Contact Phone: 972-3-7600500
- Domain Status: clientDeleteProhibited https://icann.org/epp#clientDeleteProhibited
- Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited

HACKING DNS

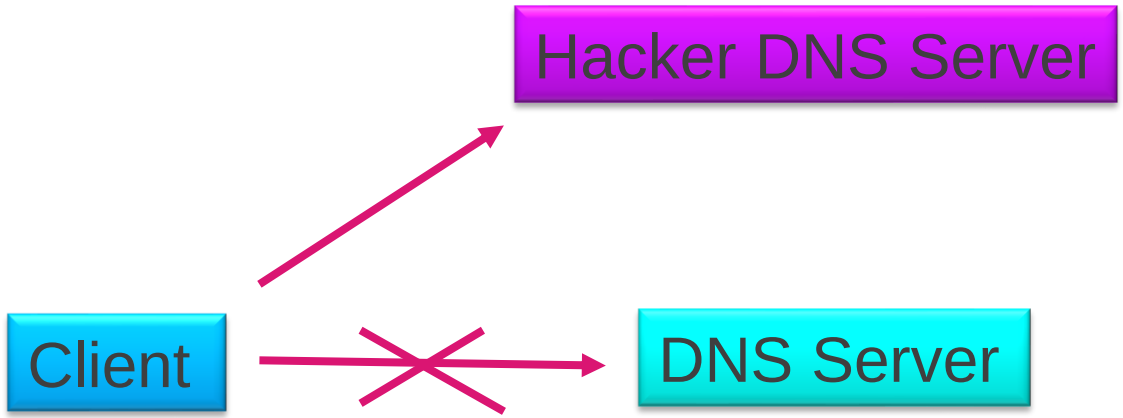
DNS ATTACKS

DNS Enumeration

- Banner Grabbing
- "any" record
  - dig ralphbonnell.com any
- Asynchronous Full Zone Transfer (AXFR)
- Reverse Lookups
  - Forward look-up resolved ralphbonnell.com to 44.206.122.150
  - dig 150.122.206.44.in-addr.arpa PTR
- IPv6
- Email to non-existing account

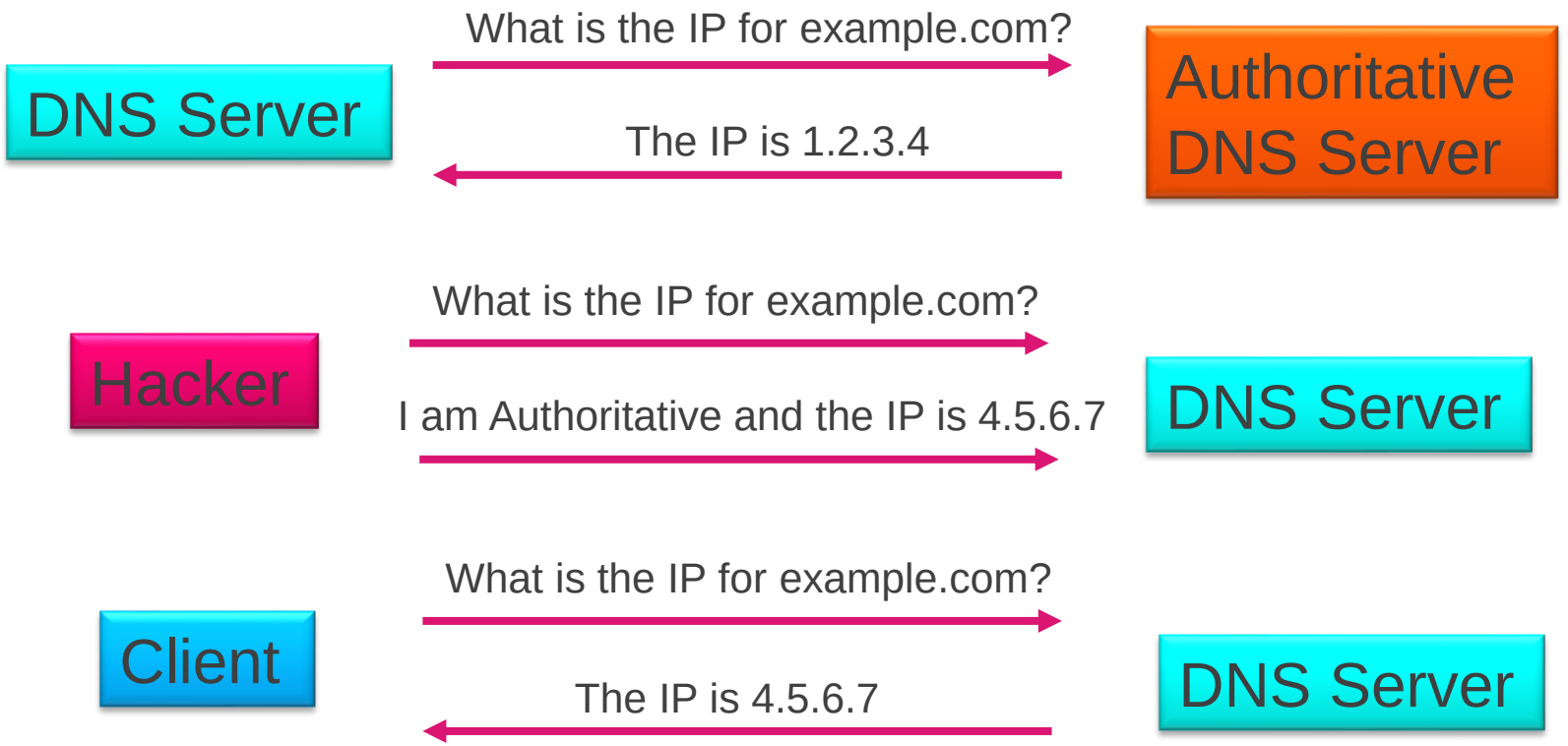
DNS Hijacking

- DNS Queries are redirected to a different domain name server
- Types of DNS Hijacking
  - Local DNS Redirect
  - DNS Settings on local Router or DHCP Server
  - MITM (Man In The Middle) Attack
  - Rouge DNS Servers
  - ISP Redirection
    - Advertising
    - Statistics / Analytics



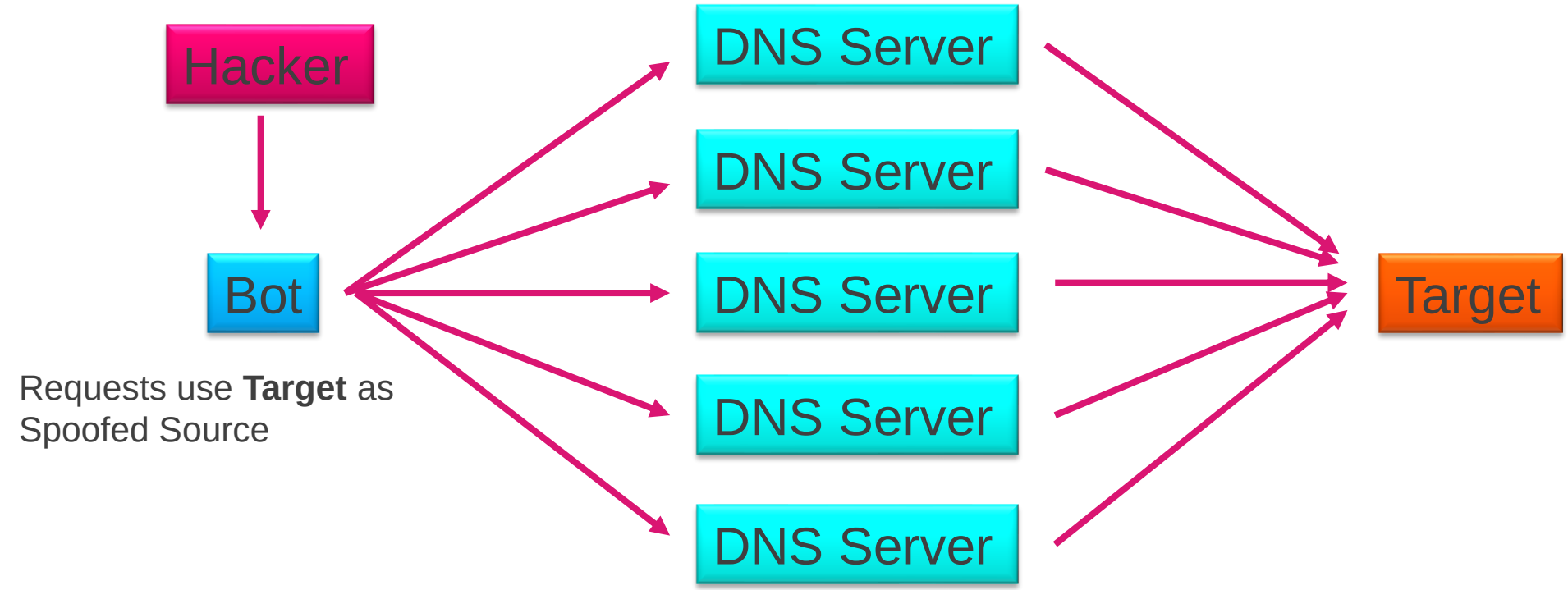
DNS Spoofing / Cache Poisoning

- Forged DNS data is introduced into the DNS Resolvers cache



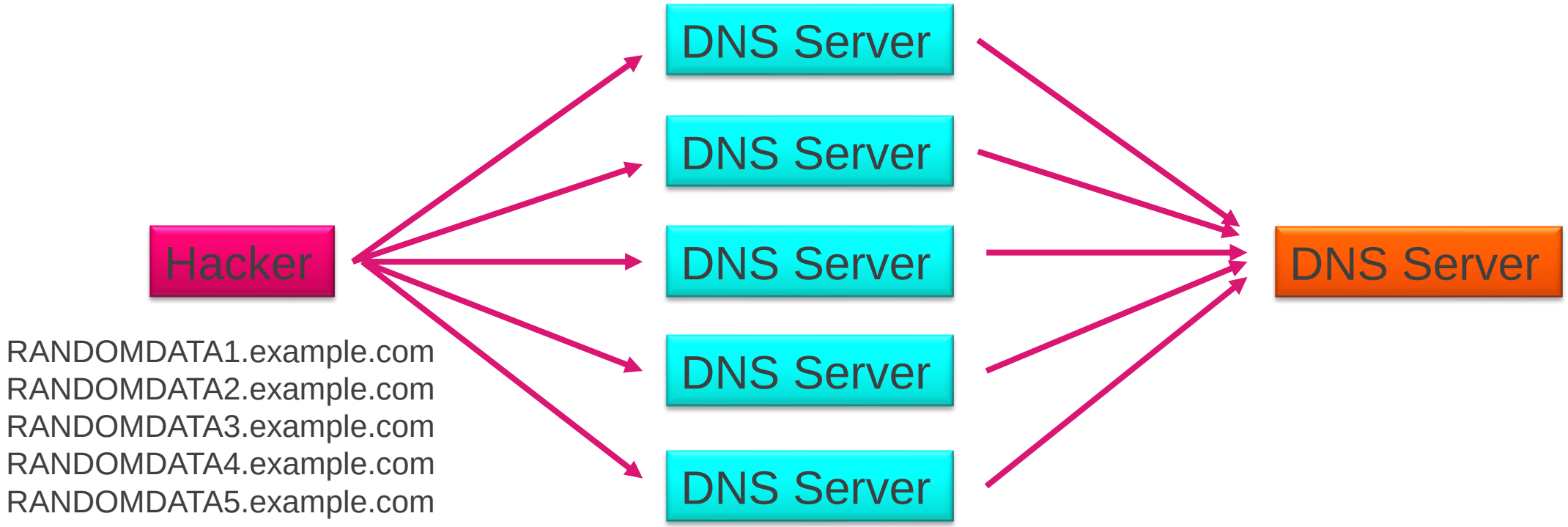
DNS Amplification

- DDoS (Distributed Denial of Service) attack using a spoofed source of the target service, a large amount of seemingly legitimate requests overwhelm a target when DNS replies to the requests



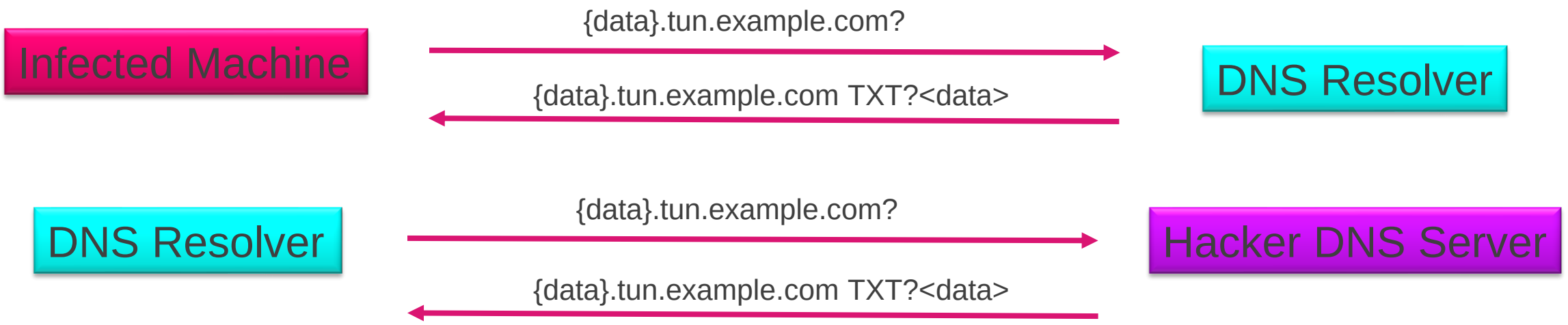
DNS NXDOMAIN / Random Subdomain Attack

- DNS queries flood a system with requests and cause a denial of service.
- DNS Queries are random strings as subdomains.



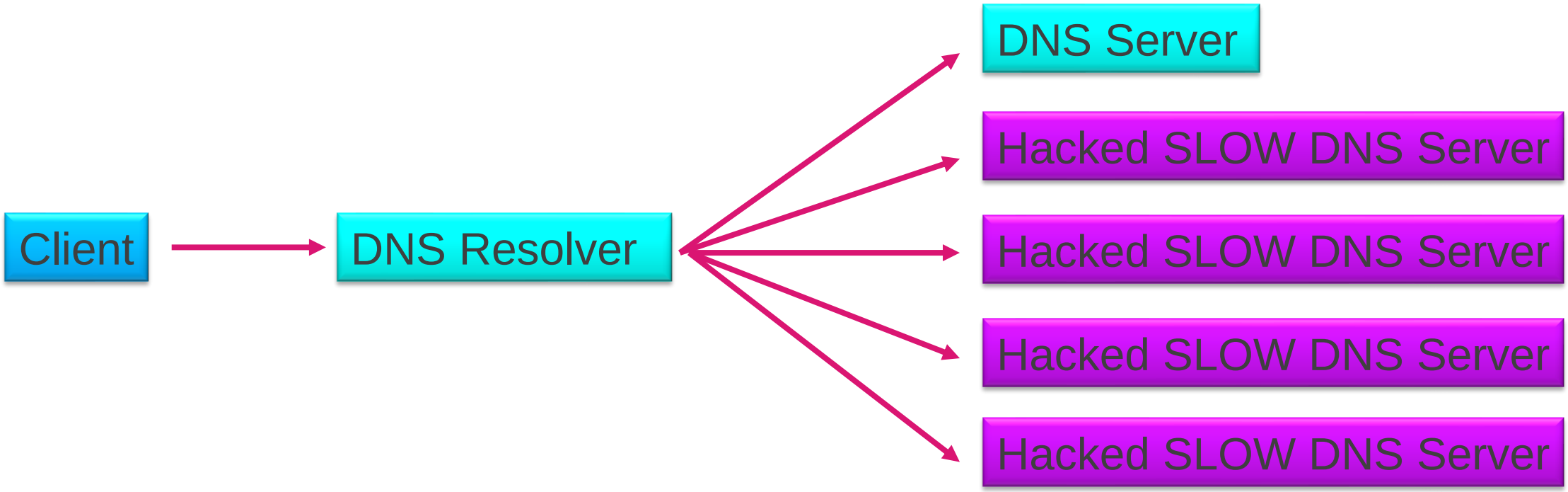
DNS Tunneling

- Application data is tunneled through DNS queries
- Can be used to tunnel command and control networks
- Bypasses firewall inspection
- Can bypass captive Wi-Fi portals (free Wi-Fi!)



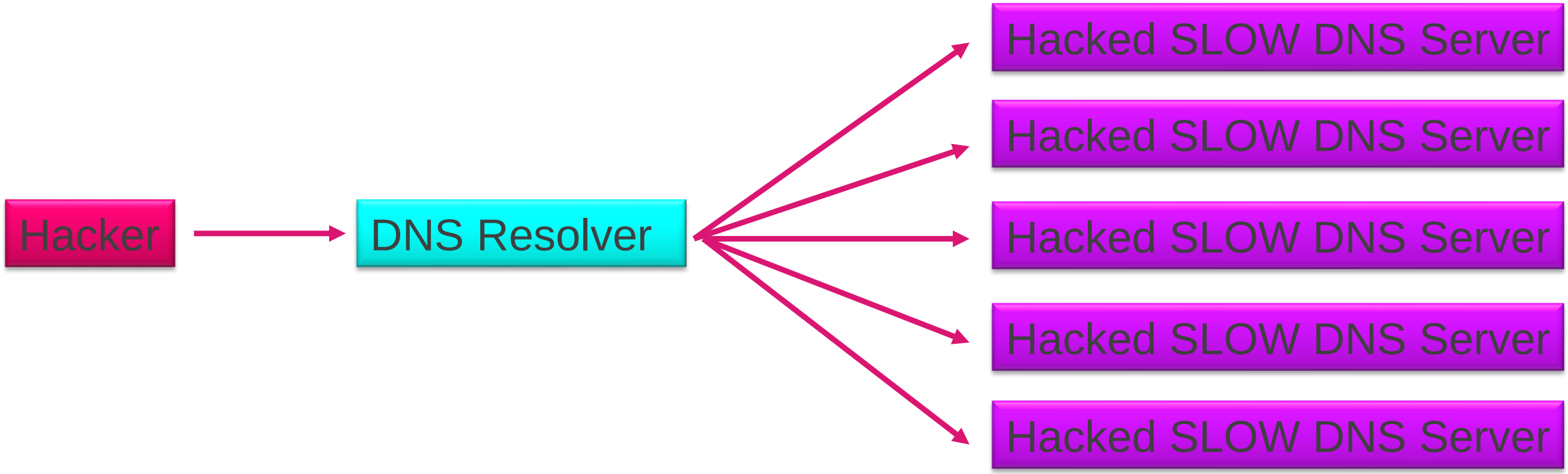
DNS Phantom Domain

- A malicious domain server is setup that responds very slowly (if at all)



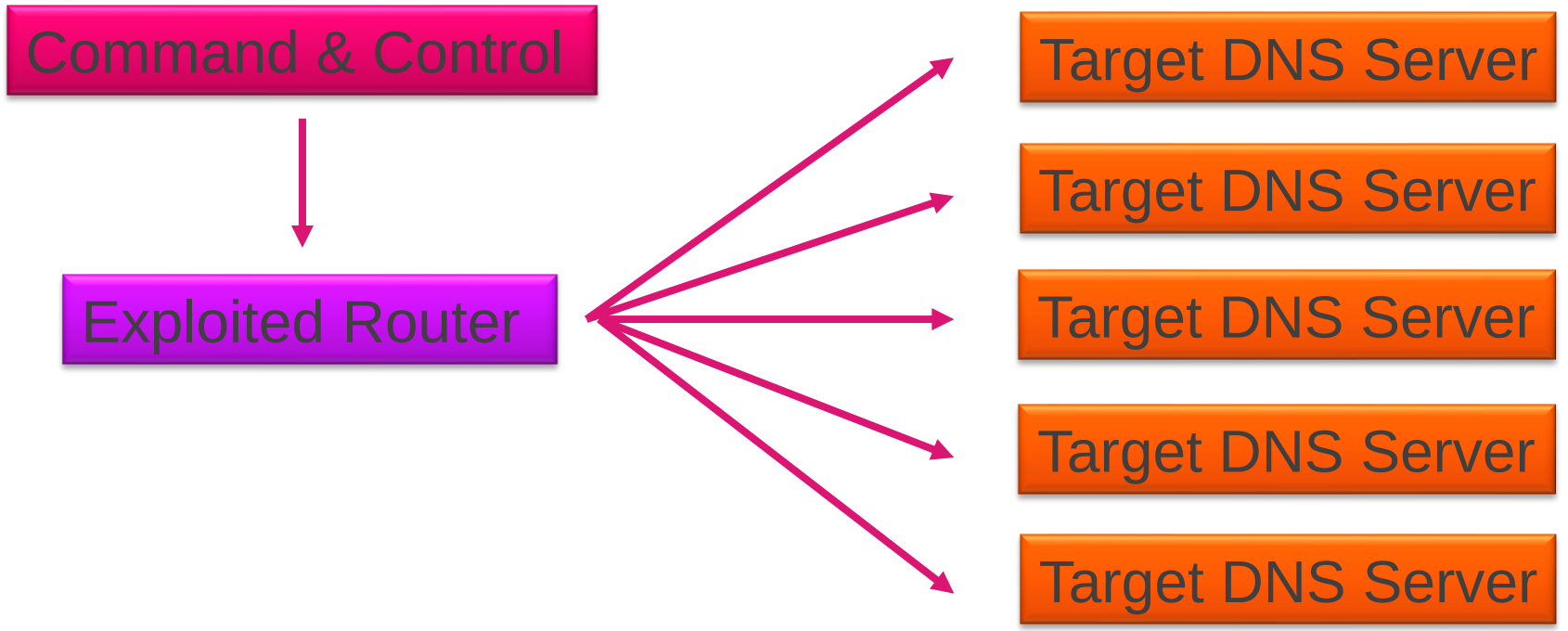
DNS Domain Lock-up

- Domains and Resolvers are setup to create TCP connections with other Resolvers, which reply with slow streams of random packets



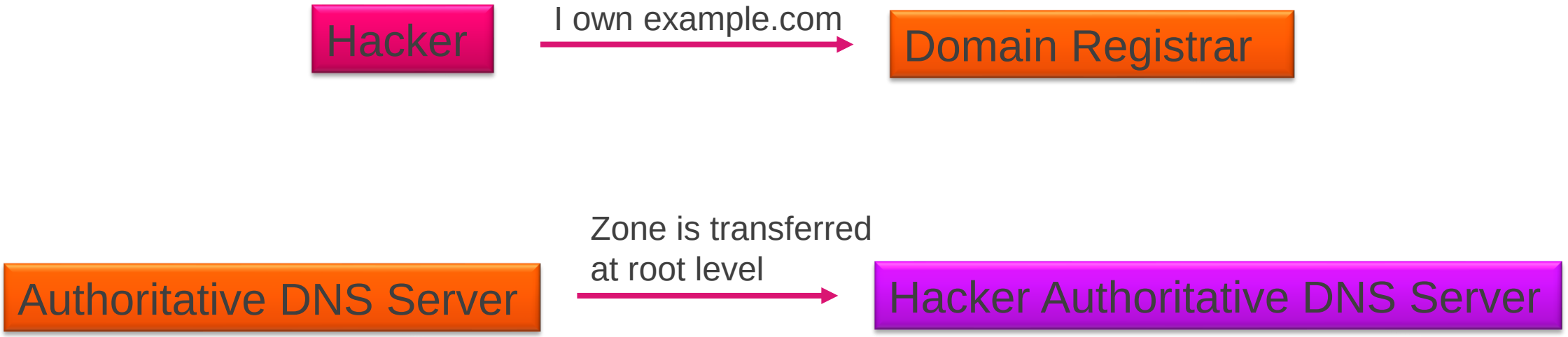
DNS Botnet-based CPE

- CPE (Customer Premise Equipment), such as a cable modem or internet router, is compromised and becomes part of a botnet



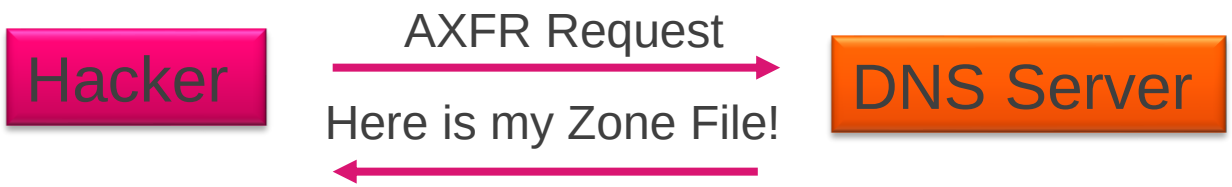
DNS Domain Registrar Take Over

- A malicious entity accesses the DNS registrar and Transfers the Domain



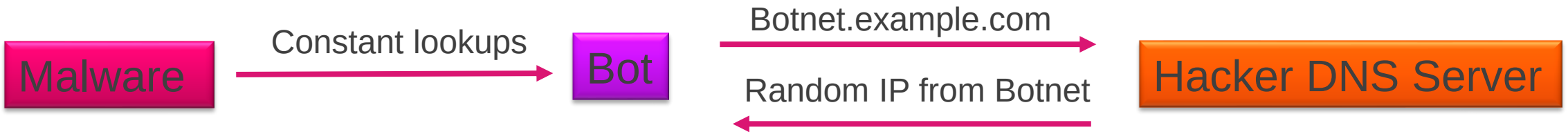
DNS Zone Transfers / Brute Forcing

- A DNS query type AXFR transfers the entire zone record to the requestor.



DNS Fast Flux

- DNS Evasion technique where attackers use botnets to hide malware and phishing activities from security scans using DNS queries to DNS resolvers that act as reverse proxies
- Uses a LOT of IP Addresses. Domain queries respond with a different IP address every few minutes. IP addresses come from compromised systems that are part of a botnet.
- Single-Flux Network
- Double-Flux Networks



DNS DGA (Domain Generation Algorithms)

- A script / algorithm that generates large amounts of new domain names for use with malware

DGA_RANDOMDATA_1.TIMEDATE_STAMP.example.com
DGA_RANDOMDATA_2.TIMEDATE_STAMP.example.com
DGA_RANDOMDATA_3.TIMEDATE_STAMP.example.com
DGA_RANDOMDATA_4.TIMEDATE_STAMP.example.com
DGA_RANDOMDATA_5.TIMEDATE_STAMP.example.com

DNS BEST PRACTICES

DNS Best Practice Recommendations

- Implement strong access controls
- Implement a ZTNA (Zero Trust Network Access) model
- Implement a Network Firewall
- Setup a VPN with MFA (Multi Factor Authentication)
- Patch regularly!

DNS Best Practice Recommendations

- Monitor for SSL Certificate changes
- http://www.whoismydns.com
- Use DNS Registry Lock
- Restrict Zone Transfers
- Review DNS Configuration periodically

DNS Best Practice Recommendations

- Implement DNSSEC
  - DNSSEC Implements a hierarchical digital signing policy throughout all layers of the DNS Infrastructure
- DNSSEC is defined by the IETF in RFCs 4033, 4034, and 4035
  - Published in 2005
- Implements new record types for the cryptographic keys

- DNS over TLS
- DNS over HTTPS

DNS Best Practice Recommendations

- DNS Behavioral Analytics / Threat Intelligence Solution
- A copy of all DNS traffic is sent to a Database Server
- Uses Big Data model
- Requires a lot of hardware resources
- Can detect:
  - Data Exfiltration
  - Botnets / Command and Control networks
  - Domain Generation Algorithms

DNS Best Practice Recommendations

- Network Firewall DNS Subscriptions
- Most solutions require DNS Queries go to a Cloud Service
- Usually involve Machine Learning algorithms
- Can detect:
  - Data Exfiltration
  - Botnets / Command and Control networks
  - Domain Generation Algorithms

DNS Best Practice Recommendations

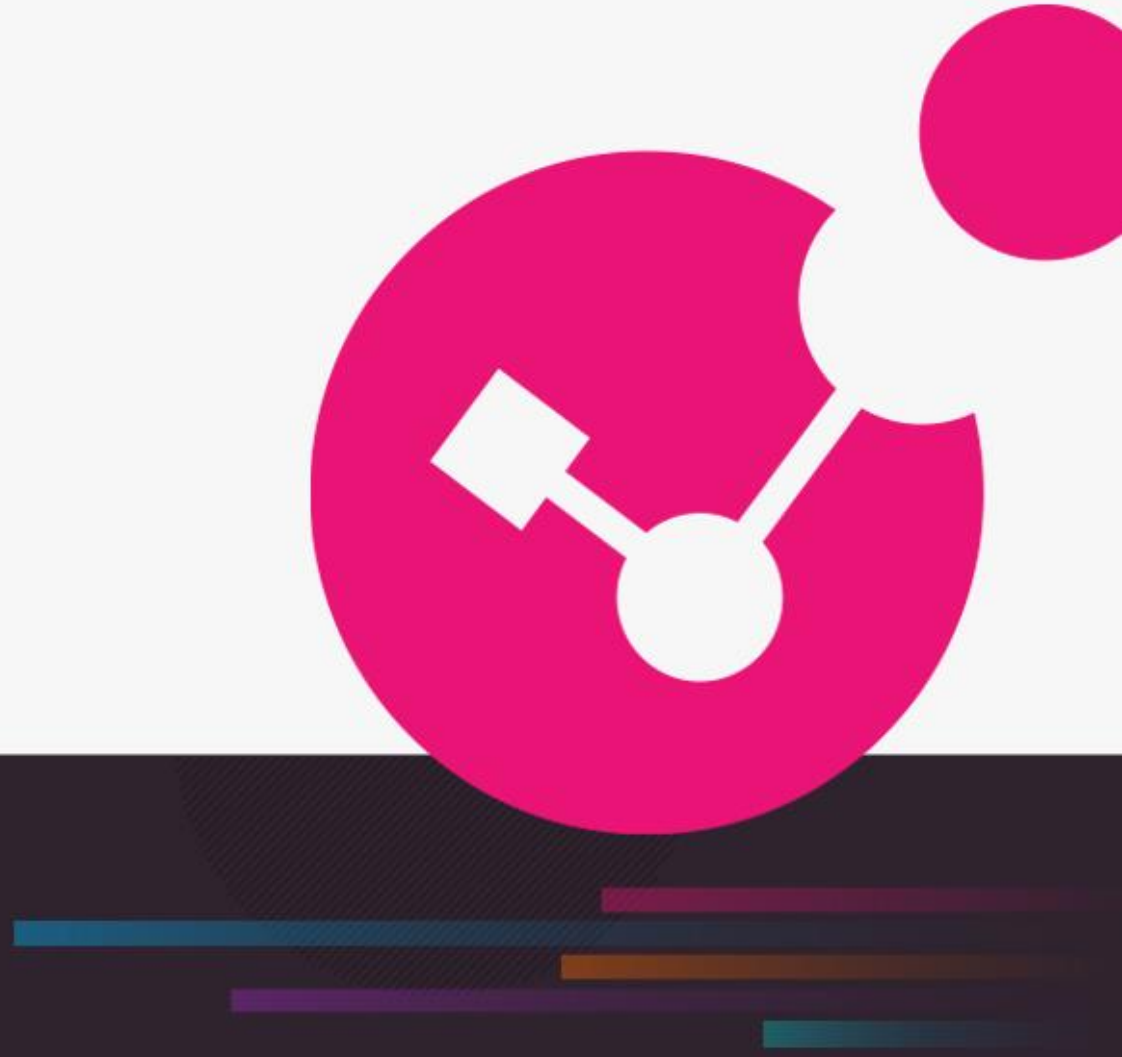
- Network Firewall DNS Deep Learning Engine
- Check Point Firewalls implemented this in Release R81.20 (latest)
- Model based on Deep Learning
- Engine is local and does not require a cloud lookup
- Can detect:
  - Data Exfiltration
  - Botnets / Command and Control networks
  - Domain Generation Algorithms

SUMMARY

- Take DNS Security seriously
- Monitor your DNS Config
- Monitor your DNS Usage

CHECK POINT™

Thank you!



YOU DESERVE THE BEST SECURITY