STEVENS
INSTITUTE OF TECHNOLOGY
1870

CS396: Security, Privacy & Society

Fall 2022

Lecture 3: Introduction

Instructor: Abrar Alrumayh

September 7, 2022

Outline

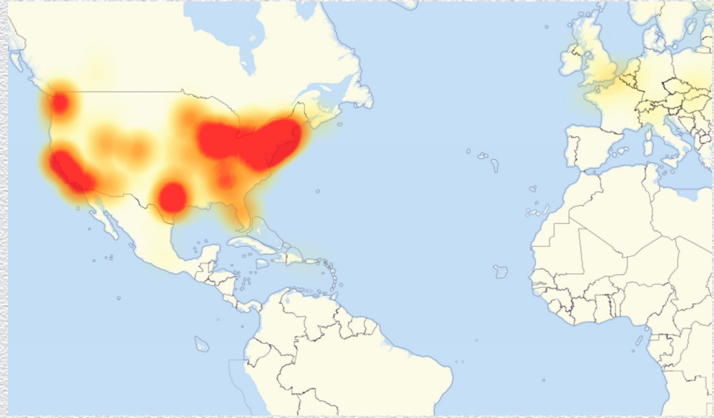
- In-class discussion with real-world examples
  - the Dyn DDOS attack

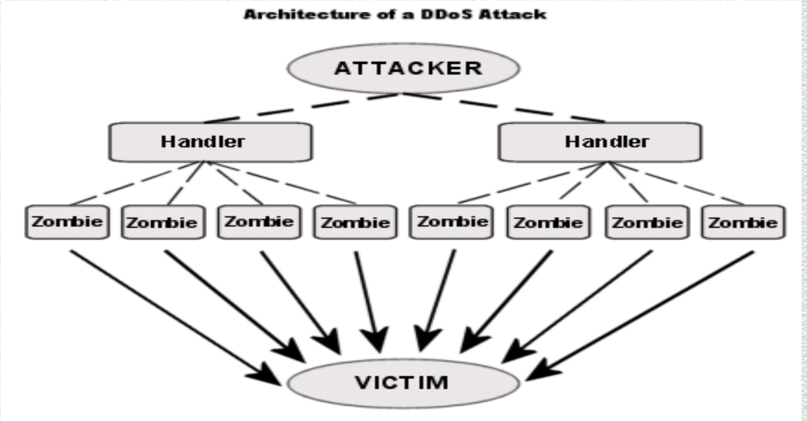
The Dyn DDoS attack

The Dyn **DDoS** attack

On October 21, 2016, a large-scale cyber was launched

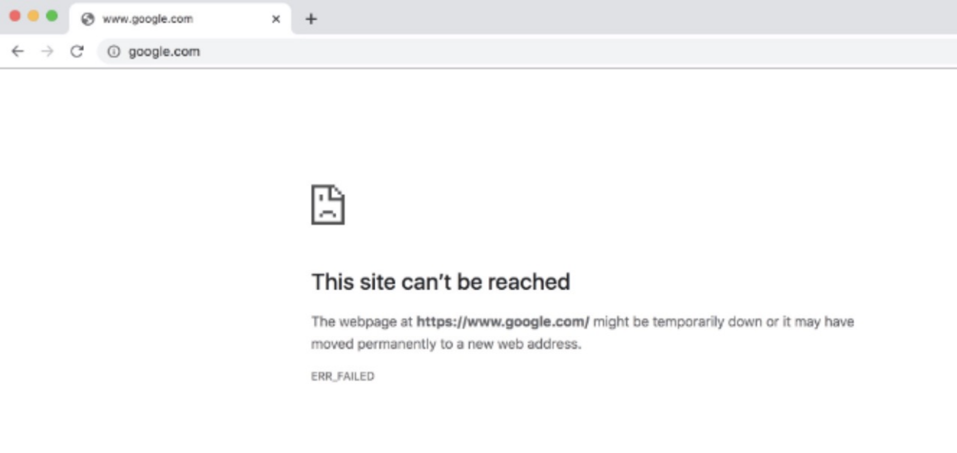
- it affected globally the entire Internet but particularly hit U.S. east coast
- during most of the day, no one could access a long list of major Internet platforms and services, e.g., Netflix, CNN, Airbnb, PayPal, Zillow, …
- this was a **Distributed Denial-of-Service (DDoS)** attack





The Dyn **DDoS** attack

- Distributed Denial-of-Service attack
  - DoS attack: attack against the **availability** of a system's core functionality
    - results in disruption of provided services
  - distributed: many machines contribute to the attack



This site can't be reached

The webpage at **https://www.google.com/** might be temporarily down or it may have moved permanently to a new web address.

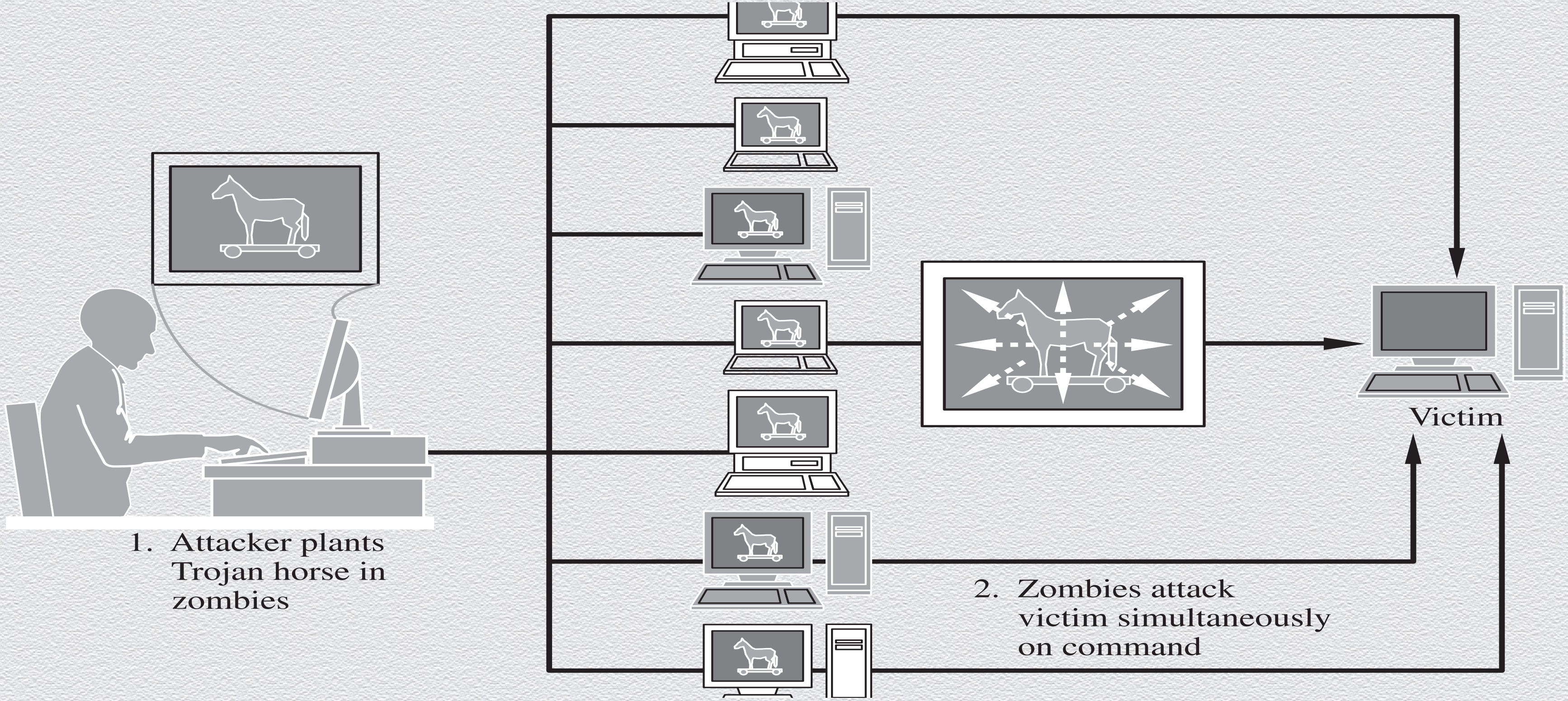
ERR_FAILED

DoS: A threat (mainly) against availability

Which main security property does a Denial-of-Service (DoS) attack attempt to defeat?

- availability; a user is denied access to authorized services or data
  - availability is concerned with preserving authorized access to assets
  - a DoS attack aims against this property; its name itself implies its main goal
- integrity & confidentiality; services or data are modified or accessed by an unauthorized user
  - elements of a DoS attack may include breaching the integrity or confidentiality of a system
  - but the end goal is disruption of a service or data flow; not the manipulation, fabrication or interception of data and services

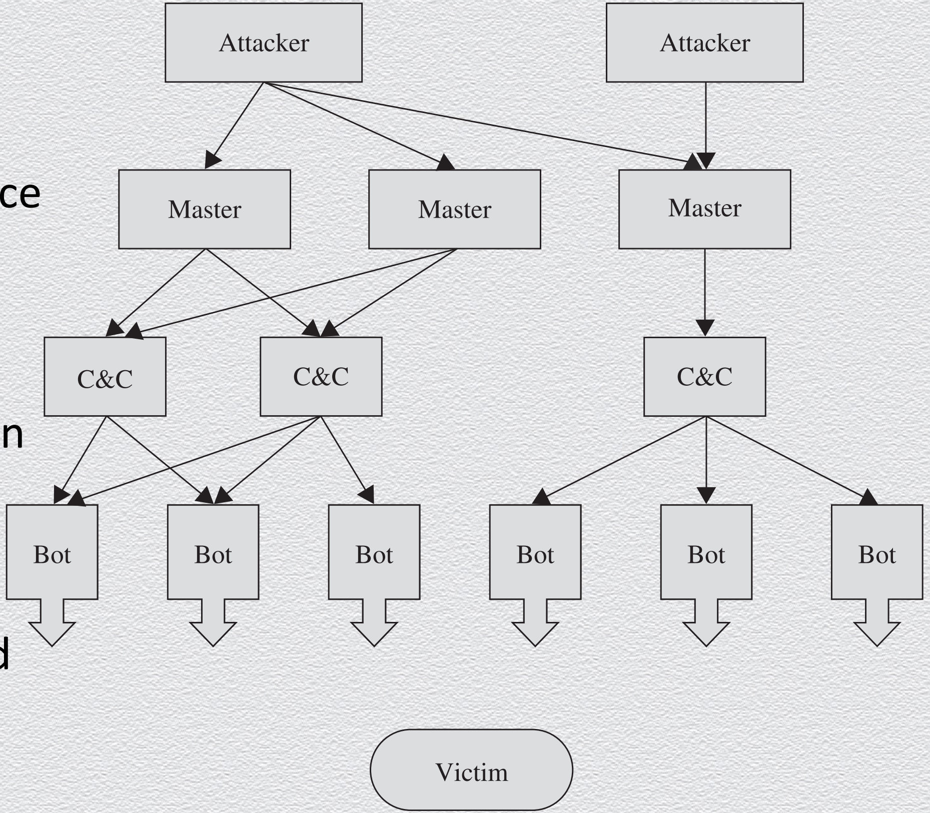
Distributed Denial of Service (DDoS)


1. Attacker plants Trojan horse in zombies
Victim
2. Zombies attack victim simultaneously on command

Botnets

Networks of machines running malicious code under remote control

- massive: scale to million of bots
  - comprise main tool for DDoS attacks
- stealth: remain undetected & difficult to trace
  - do little harm to the host machines
    - users won't likely remove malware
  - multiple-level attacker Vs. bots separation
- resilient: have redundant components
  - even if one master or C&C node
    is taken down, connectivity is maintained



The **Dyn** DDoS attack

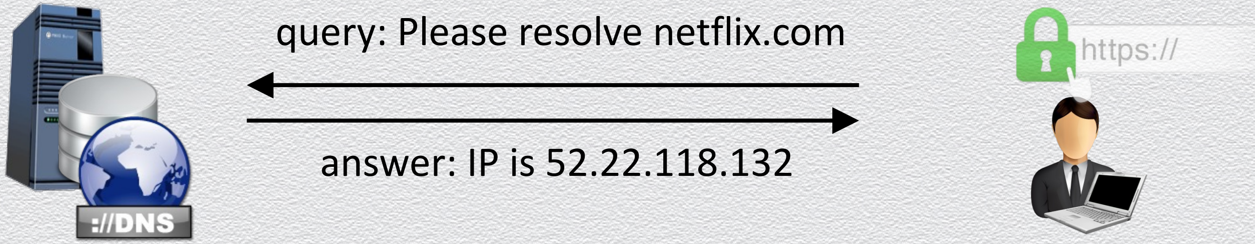
- Dyn has been a major DNS provider
- DNS stands from Domain Name System
  - naming system for computers, serviced and other resources connected to the Internet
  - hierarchical, decentralized
- DNS services are crucial for any web connection
  - translation of domain names to IP addressed

The DNS service

The Domain Name Service (DNS) protocol

Resolving domain names to IP addresses

- when you type a URL in your Web browser, its IP address must be found
  - e.g., domain name “netflix.com” has IP address “52.22.118.132”
  - larger websites have multiple IP responses for redundancy to distributing load
- at the heart of Internet addressing is a protocol called DNS
  - a database translating Internet names to addresses



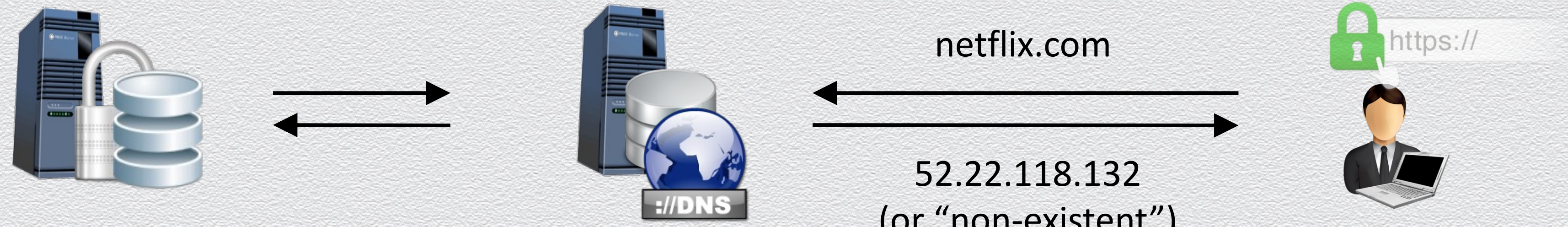
query: Please resolve netflix.com

answer: IP is 52.22.118.132

Recursive name resolution: hierarchical search

Search is performed recursively and hierarchically across different type of DNS resolvers

- application-level (e.g., Web browser), OS-level (e.g., stub resolver): locally managed
- recursive DNS servers: query other resolvers and cache recent results



DNS entries:
<netflix.com, 52.22.118.132>

primary

subset of cached queried entries
(or information of other resolvers)

secondary

netflix.com

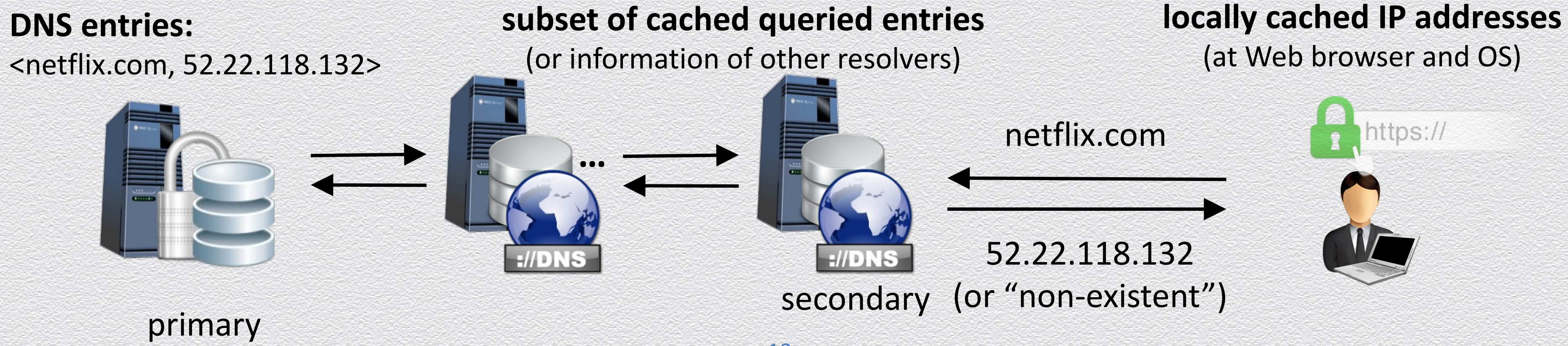
52.22.118.132
(or “non-existent”)

locally cached IP addresses
(at Web browser and OS)

Recursive name resolution: hierarchical search

Search is performed recursively and hierarchically across different type of DNS resolvers

- application-level (e.g., Web browser), OS-level (e.g., stub resolver): locally managed
- recursive DNS servers: query other resolvers and cache recent results
- root name servers: refer to appropriate TLD (top-level domain) server
- TLD servers: control TLD zones such as .com, .org, .net, etc.



DNS entries:
<netflix.com, 52.22.118.132>

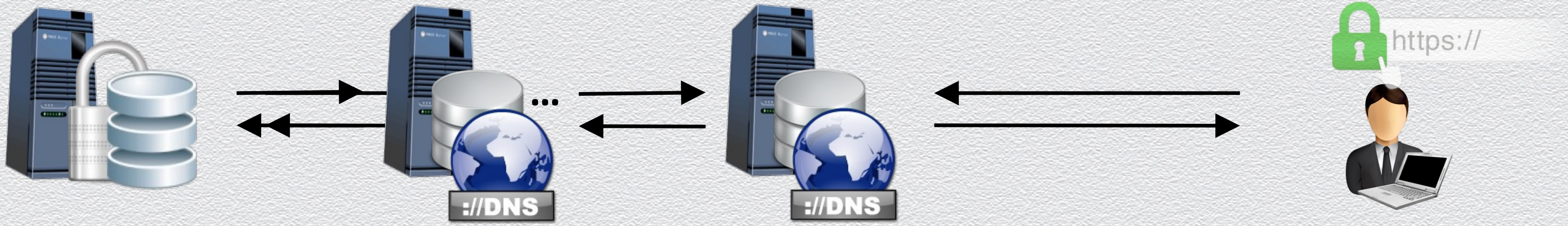
subset of cached queried entries
(or information of other resolvers)

locally cached IP addresses
(at Web browser and OS)

Recursive name resolution: flexibility

Infrastructure allows for different configurations

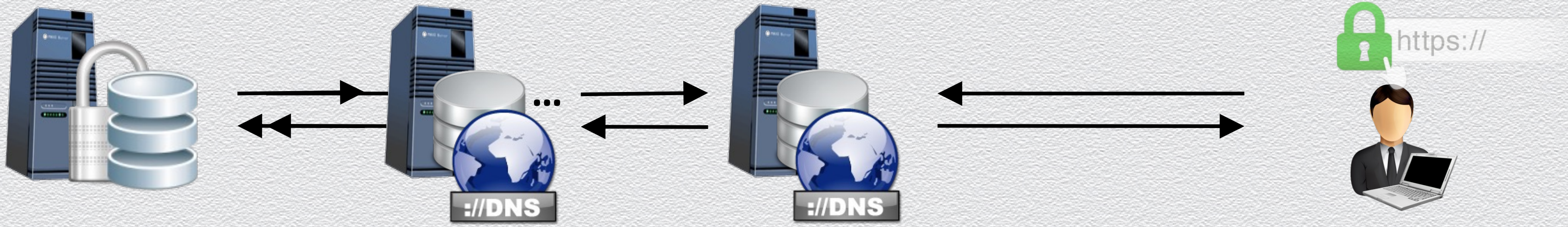
- authoritative-only servers: answer queries on zones they are responsible for
  - fast resolution, no forwarding, no cache
- caching / forwarding DNS servers: answer queries on any public domain name
  - recursive search / request forwarding, caching for speed, first-hop resolvers
- master / slaves DNS servers: authoritative servers replicating DNS data of their domains
- public / private DNS servers: control access to protected resources within an organization



Recursive name resolution: benefits

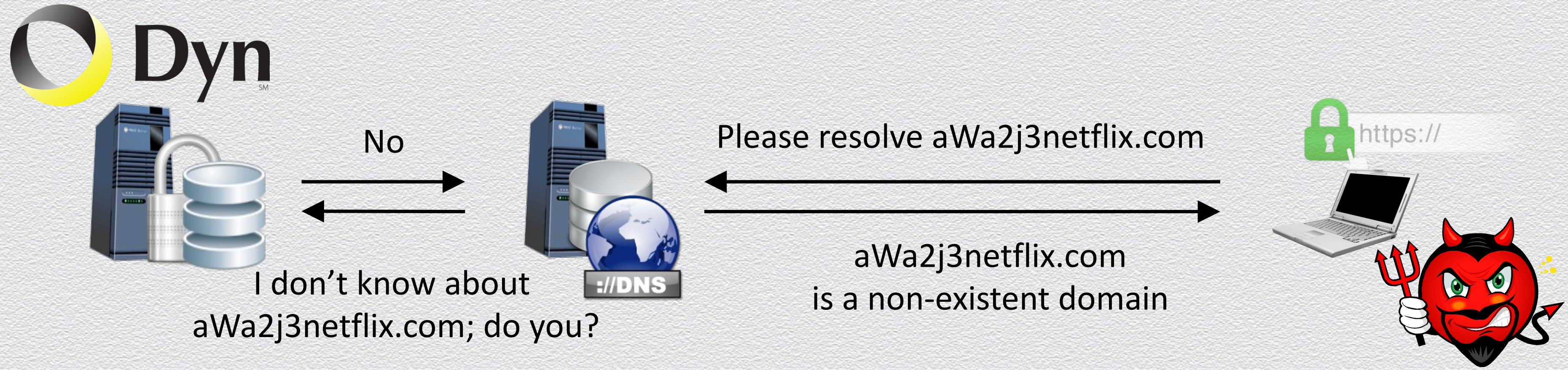
Why DNS uses non-authoritative name servers (that is, recursive resolution)?

- for more scalability & locality
  - high query loads can saturate the response capacity of primary servers
  - secondary do not have to store large volumes of DNS entries
  - cached recently queried domain names speed up searches due to locality of queries
- for added security / locality / scalability alone – not quite
  - e.g., non-authoritative name servers are untrusted and thus possibly compromised



The Dyn DDoS attack (continued)

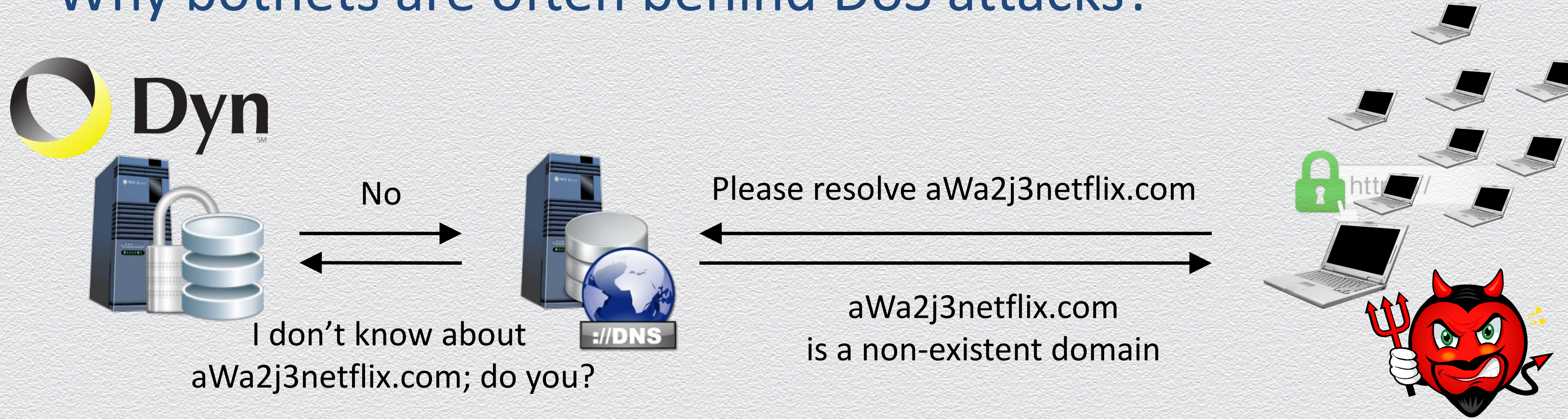
Core idea of attack: Saturate Dyn's primary servers



Attack:

- from a compromised machine ask for domain names that do not exist
- query is forwarded to fewer primary Dyn servers, i.e., defeating benefits of distribution
- ask **A LOT** of such queries to bring down the Dyn DNS service!

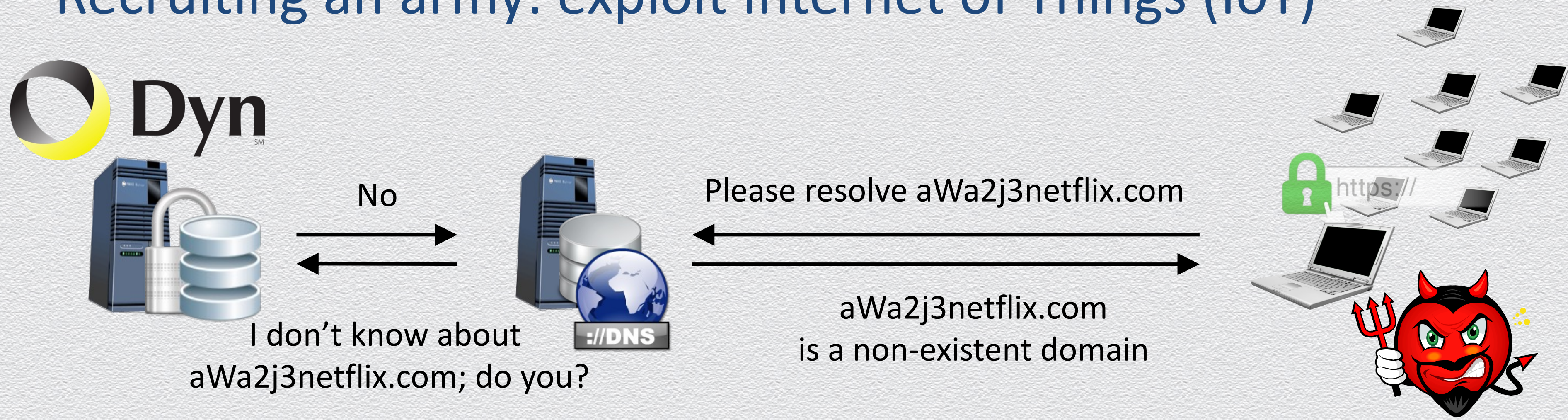
Why botnets are often behind DoS attacks?


Dyn
No
I don't know about aWa2j3netflix.com; do you?
://DNS
Please resolve aWa2j3netflix.com
aWa2j3netflix.com is a non-existent domain
http://

Use a botnet:

- To avoid effective countermeasures and increase attack traffic
  - if the high-volume attack traffic comes from few devices, they can be filtered out by blocking their connections to the Dyn servers
  - by employing a large botnet of millions of devices the attacker inflicts a larger, more devastating attack traffic against the victim Dyn servers

Recruiting an army: exploit Internet of Things (IoT)



No

I don’t know about
aWa2j3netflix.com; do you?

Please resolve aWa2j3netflix.com

aWa2j3netflix.com
is a non-existent domain

Create a botnet:

- compromise easy targets: IoT “thin” devices, e.g., printers, cameras, home routers, …
- how? find a vulnerability on these devices...
- all such devices used an OS with a static, hard-wired, thus known, admin password...!

The Internet of Things (IoT)

Refers to Internet-connected everyday devices

- comprise a world of so-called smart devices
- examples:
  - smart appliances, such as refrigerators and dishwashers
  - smart home, such as thermostats and alarm systems
  - smart health, such as fitness monitors and insulin pumps
  - smart transportation, such as driverless cars
  - smart entertainment, such as video recorders
- potential downsides
  - loss of privacy
  - loss of control of data
  - potential for subversion
  - mistaken identification
  - uncontrolled access

Smartphones

The control hub of the IoT – important target for malware

- 2013: 143,211 distinct new forms of malware against mobile devices
- 98% targeted Android devices, far in excess of its market share
  - Android: open approach
    - unlike its competitors, does not limit the software users are allowed to install
    - thus, an easier target
  - Apple: locked-down approach
    - in contrast, only allows apps from its app store to be installed on its smartphones
    - all apps go through an approval process, which includes some security review
    - once approved, apps are signed, using a certificate approach