efficient iP™
DEFINING SMART DDI

FUN with DNS

#JCSA17

afnic

Marck TO

Agenda

- Quelques principes DNS
- Présentation de l'architecture
- Let's have fun with DNS
  - Intrusion
  - Exfiltration
  - Déni de service

DNS recursion in 5 minutes, or refunded (but not actually)

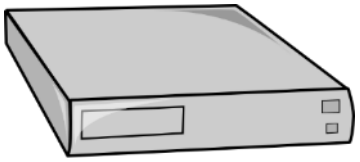
Where is baddomain.com?

Root servers

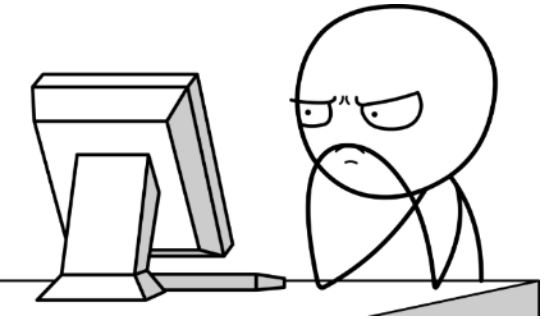
Already know the answer (cached)?
Yes : respond
No: send to root servers

8.8.8.8

Already know the answer (cached)?
Yes : respond
No: send to FAI resolver

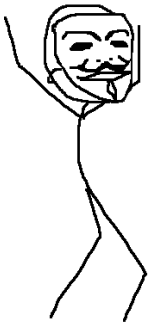


Corporate resolver



Give me the adresse of
www.baddomain.com

Return anything we want!



baddomain.com

[1]EfficientIP 2016 DNS security report

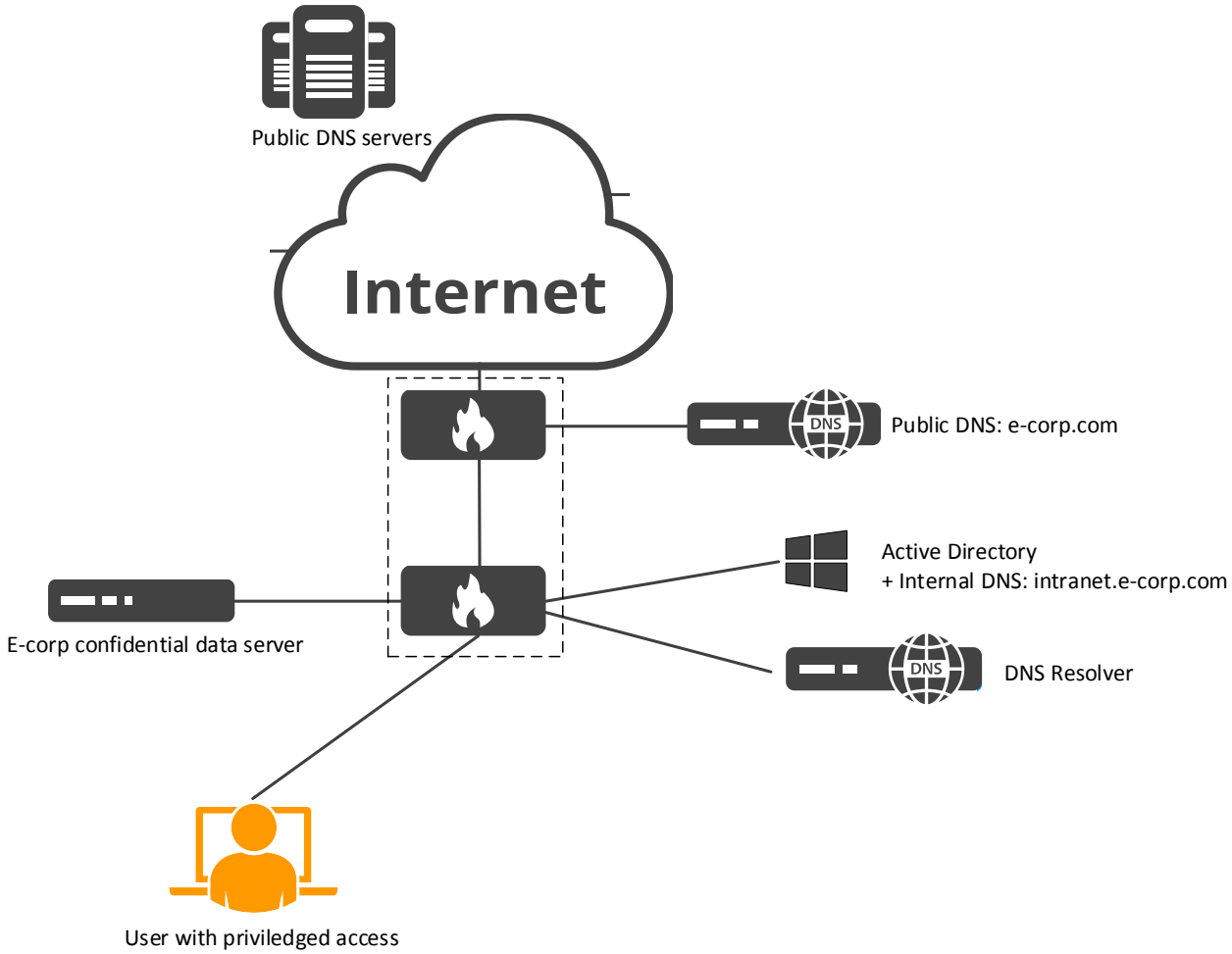
efficient iP™ #JCSA17 afnic

Disclaimer

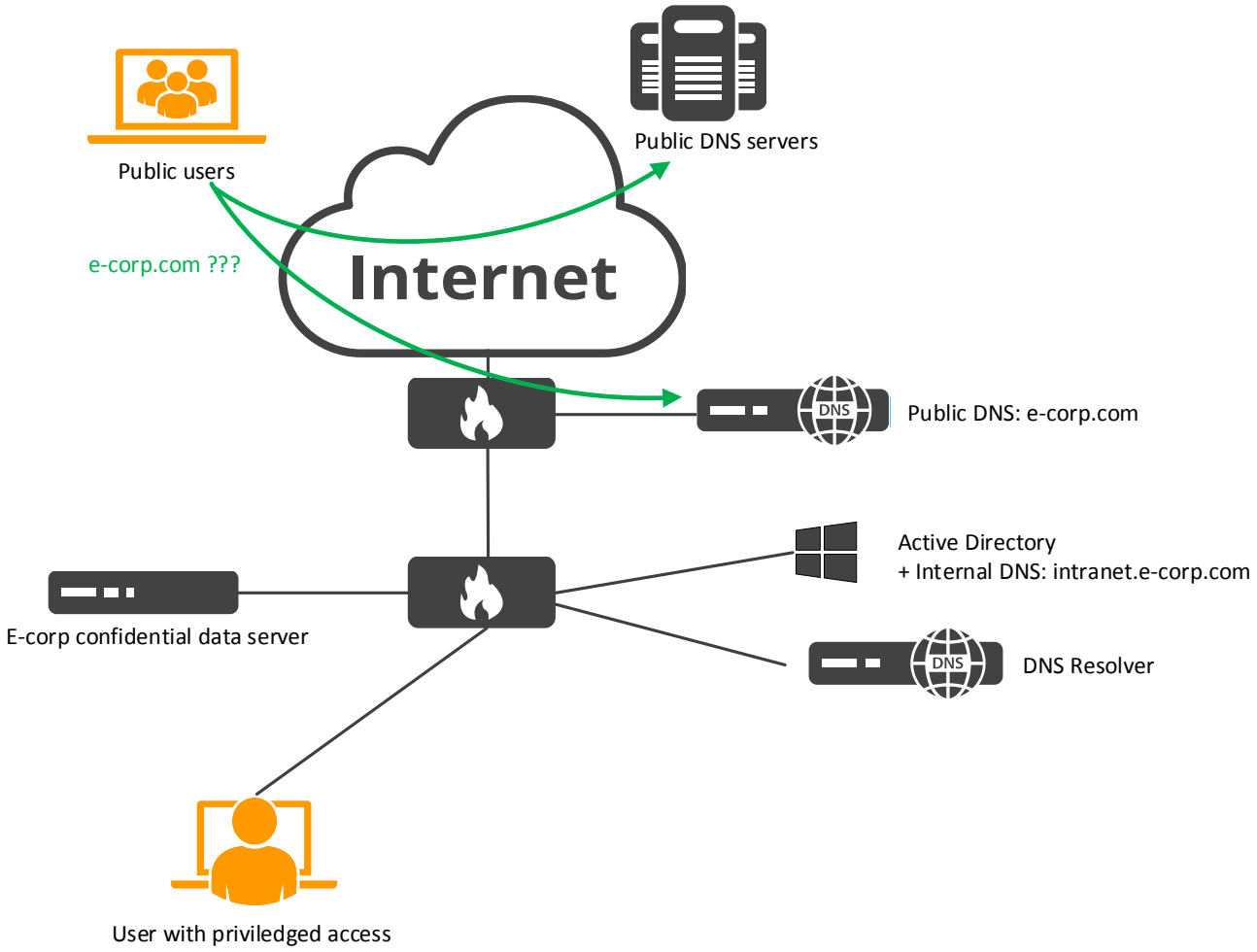
« toute ressemblance avec des personnes existantes ou ayant existées serait purement fortuite »

« Aucun serveur DNS n'a été blessé (pour l'instant) »

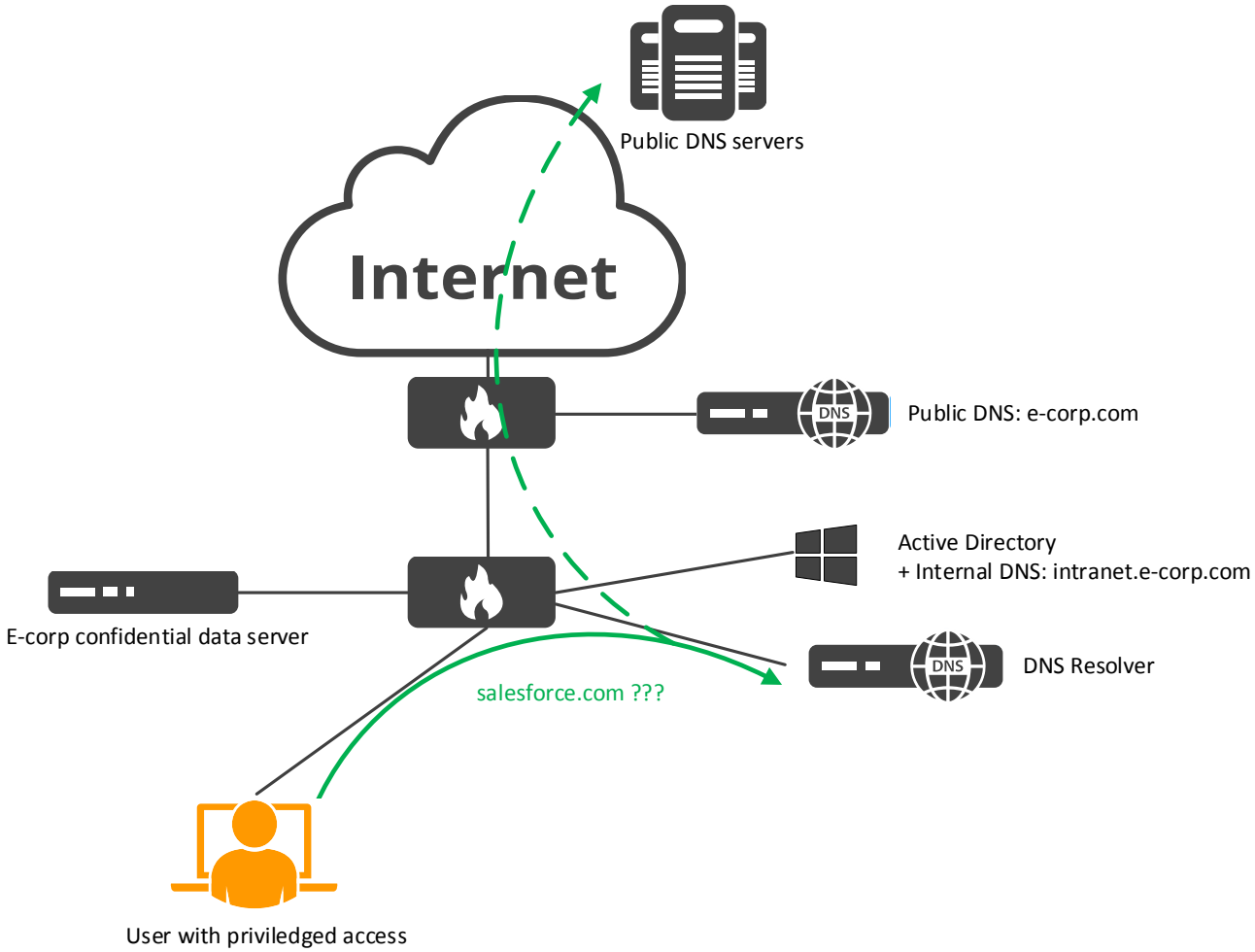
The architecture



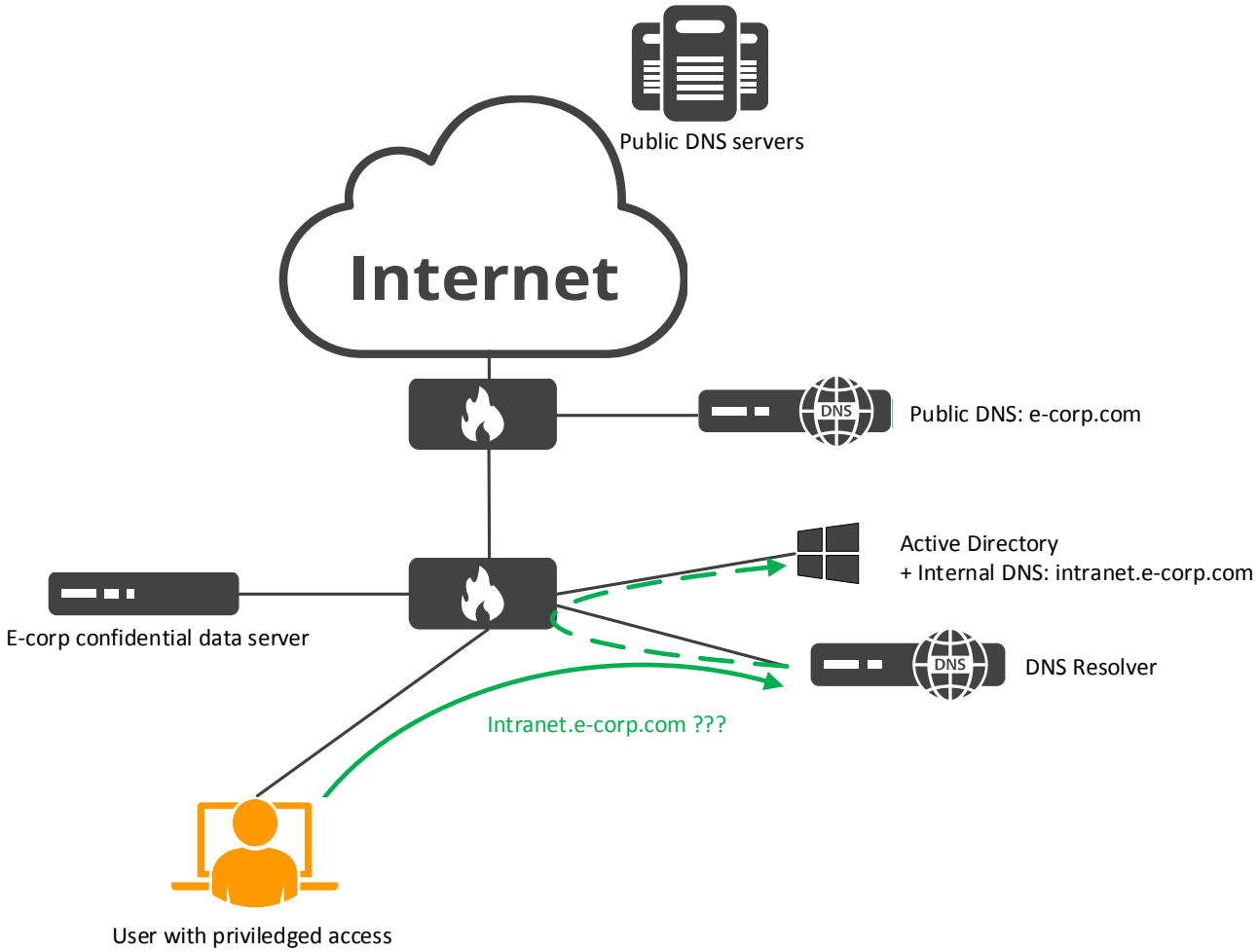
Normal usage: public dns



Normal usage: internal dns

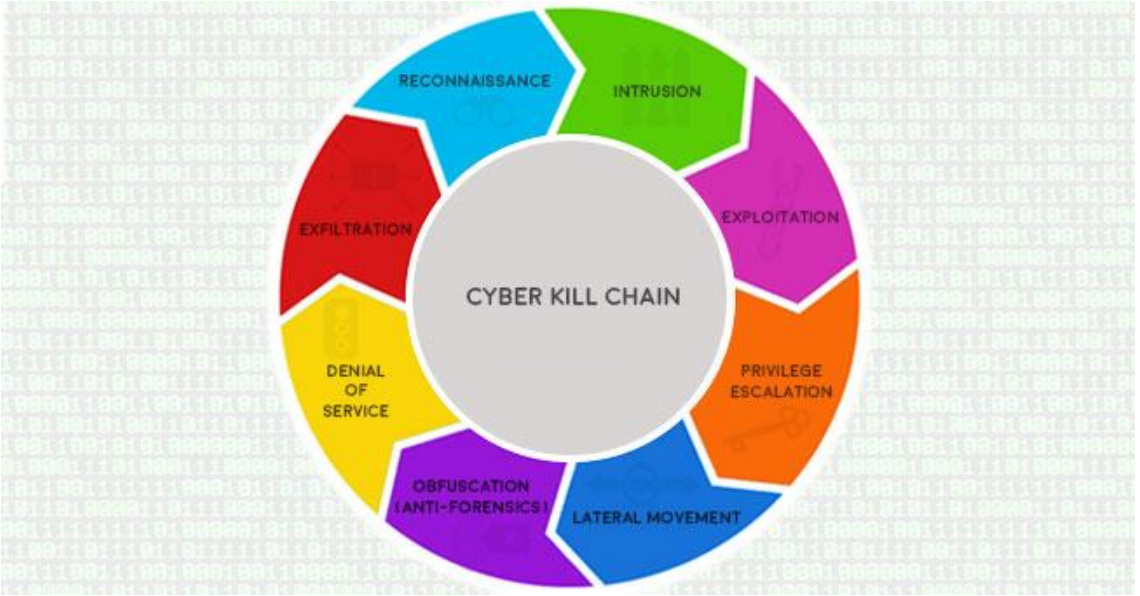


Normal usage: internal dns



Challenge

- Attack E-Corp using DNS only
- The attack will follow a classic killchain sequence:
  - Reconnaissance
  - weaponization
  - Delivery
  - CnC
  - Lateral movement
  - Exfiltration



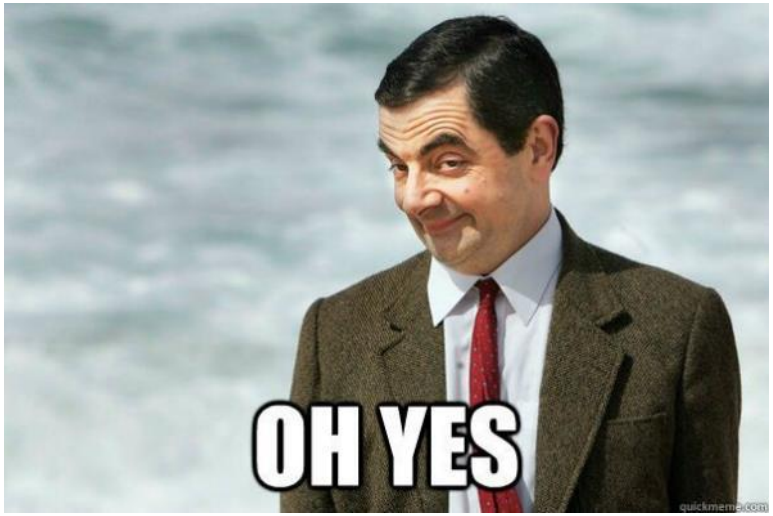
Display setup

Stage 1: Preparation

- Reconnaissance
  - Hacker motivation: ???
  - Target: E-corp
  - Entry point: Phillip Price
  - Position: Network admin
  - Bait: we met at an event some weeks ago…

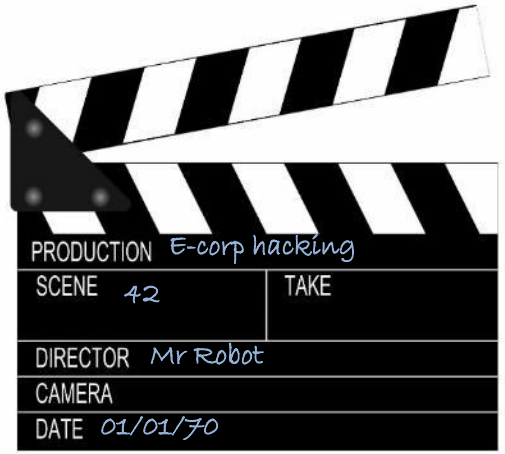
Stage 1: Preparation

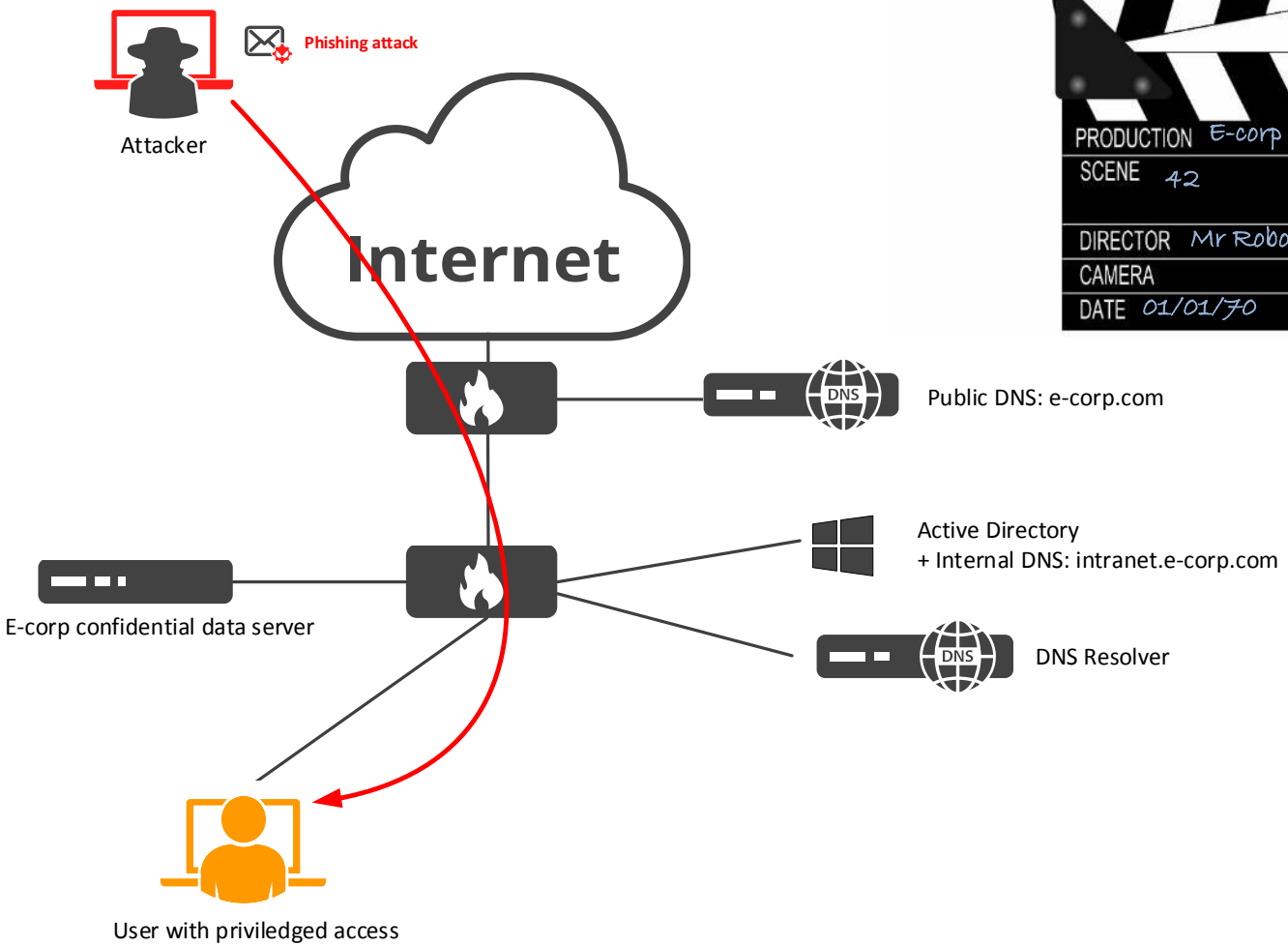
- Weaponization:
  - PDF file…
  - …malicious payload embedded



Stage 1: Intrusion – delivery

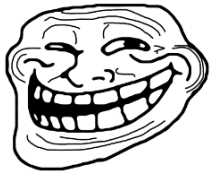
DNS Malware





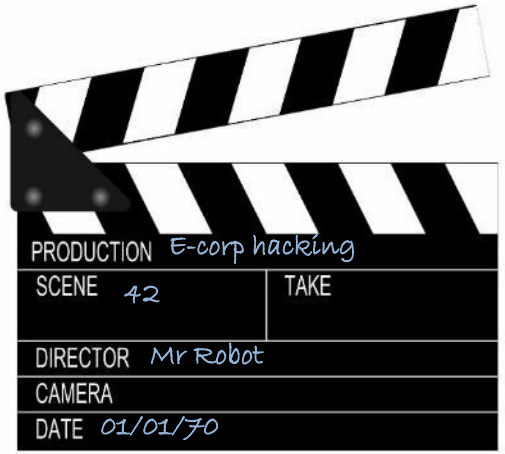
Stage 2: Intrusion: delivery and CnC
DNS Malware

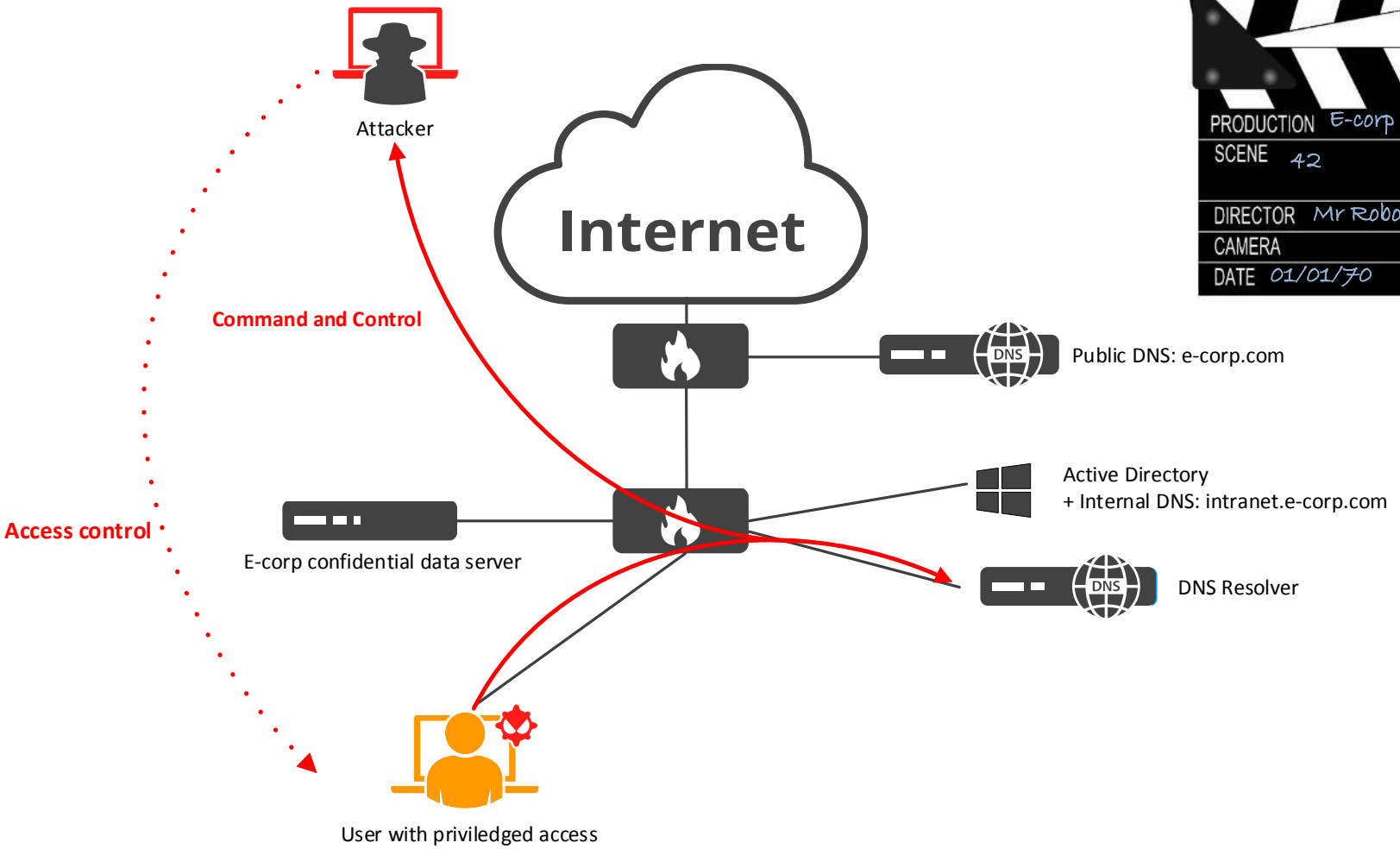
- Delivery and CnC
  - Social engineering to invite to open the malicious file
  - Take control of the machine



Stage 2: Intrusion: delivery and CnC

DNS Malware





efficient iP™

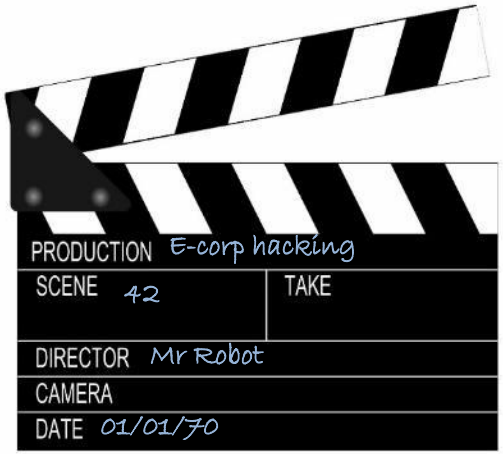
#JCSA17 afnic

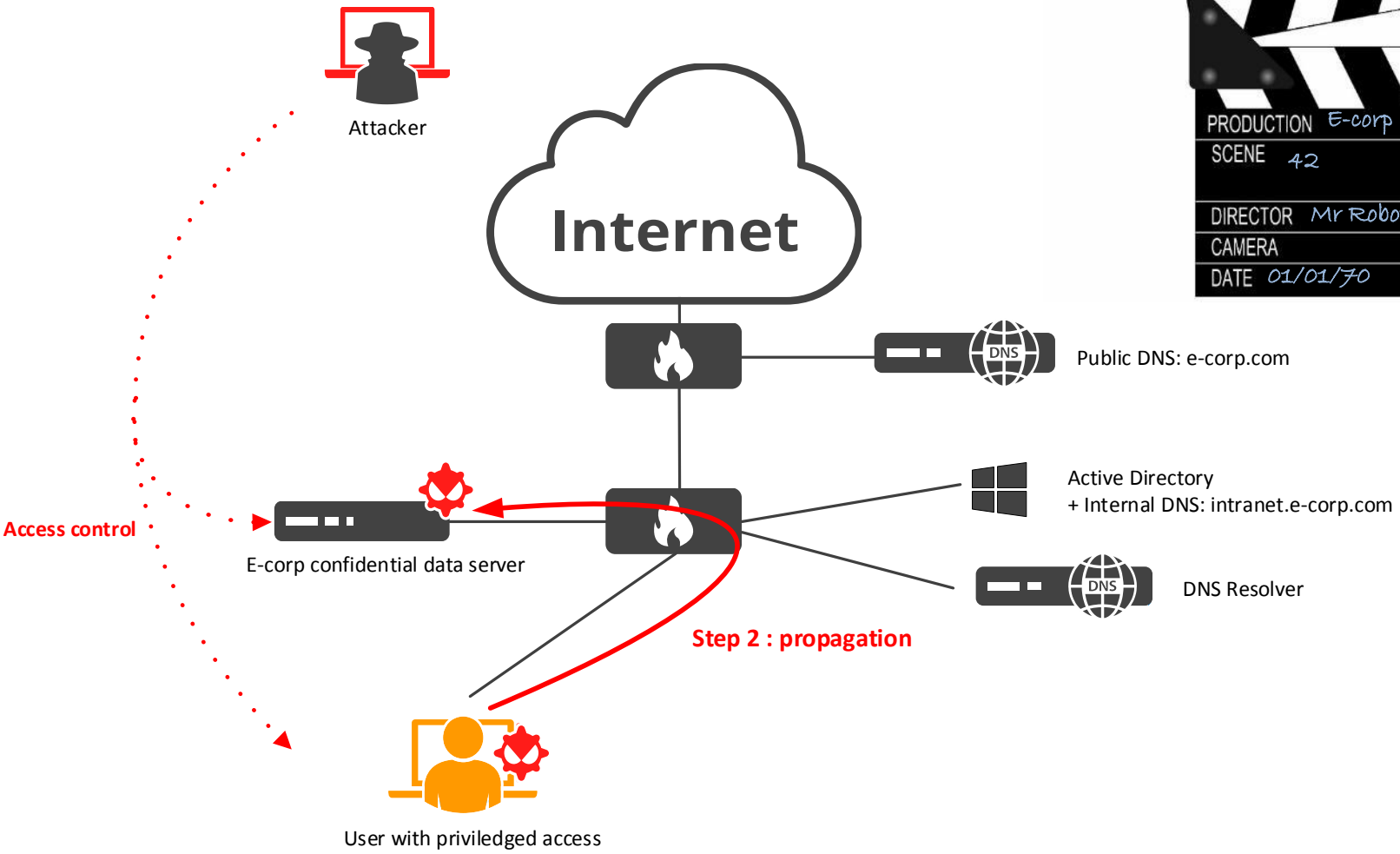
Stage 2: Intrusion: delivery and CnC
DNS Malware

- Lateral movement
  - Spy on the compromised host
  - Drop a password sniffer? A keylogger?
  - Nah, real jerks use state level exploit!
  - Move to other places in the network

Stage 2: Intrusion: delivery and CnC

DNS Malware



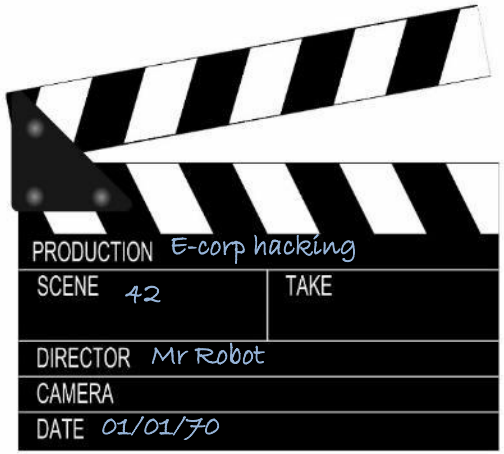


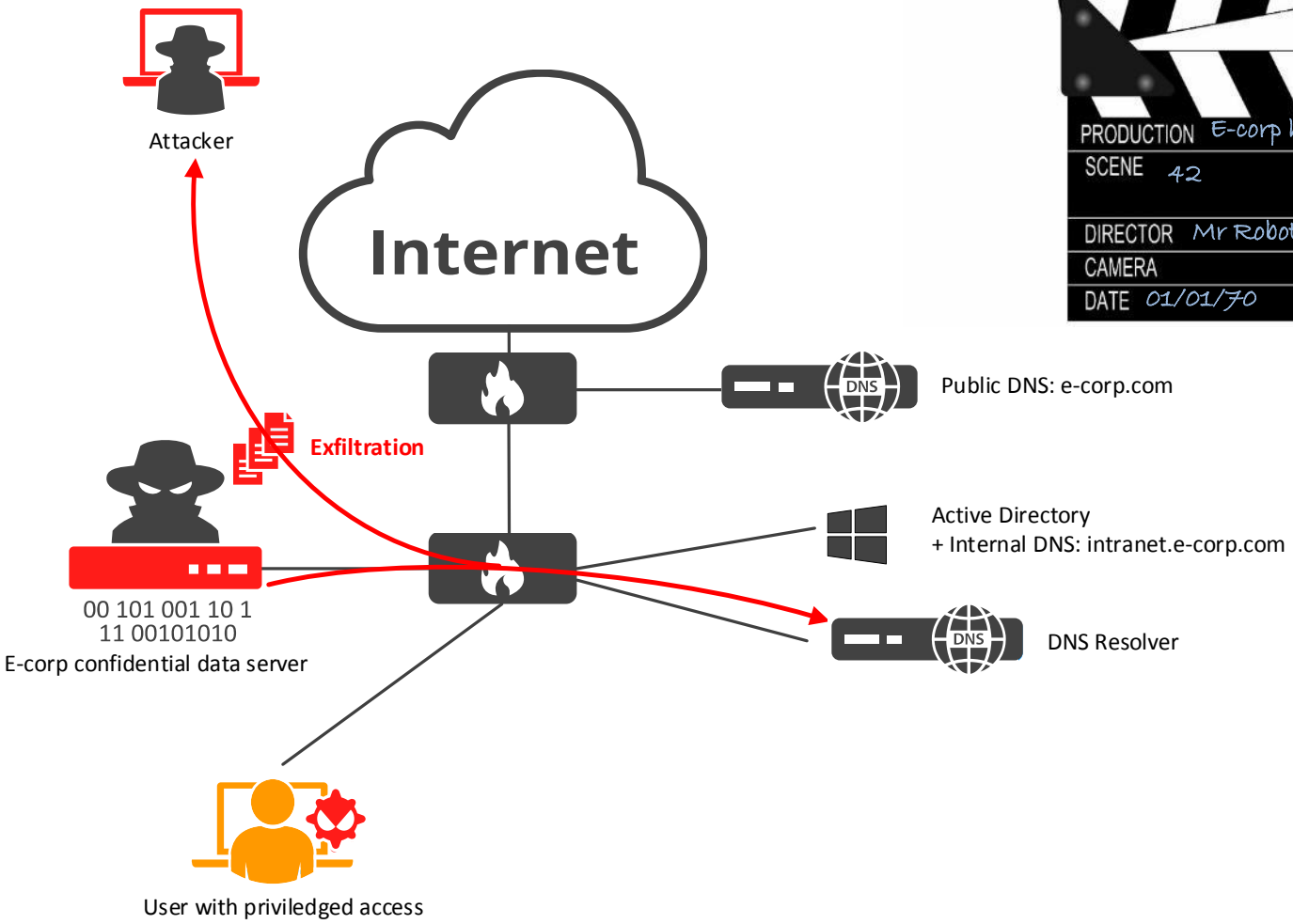
Stage 3: Actions on objectives
Extract data with DNS Tunneling

- Exfiltration
  - Publish files using web server
  - Encapsulate HTTP into DNS

Stage 3: Actions on objectives

Extract data with DNS Tunneling



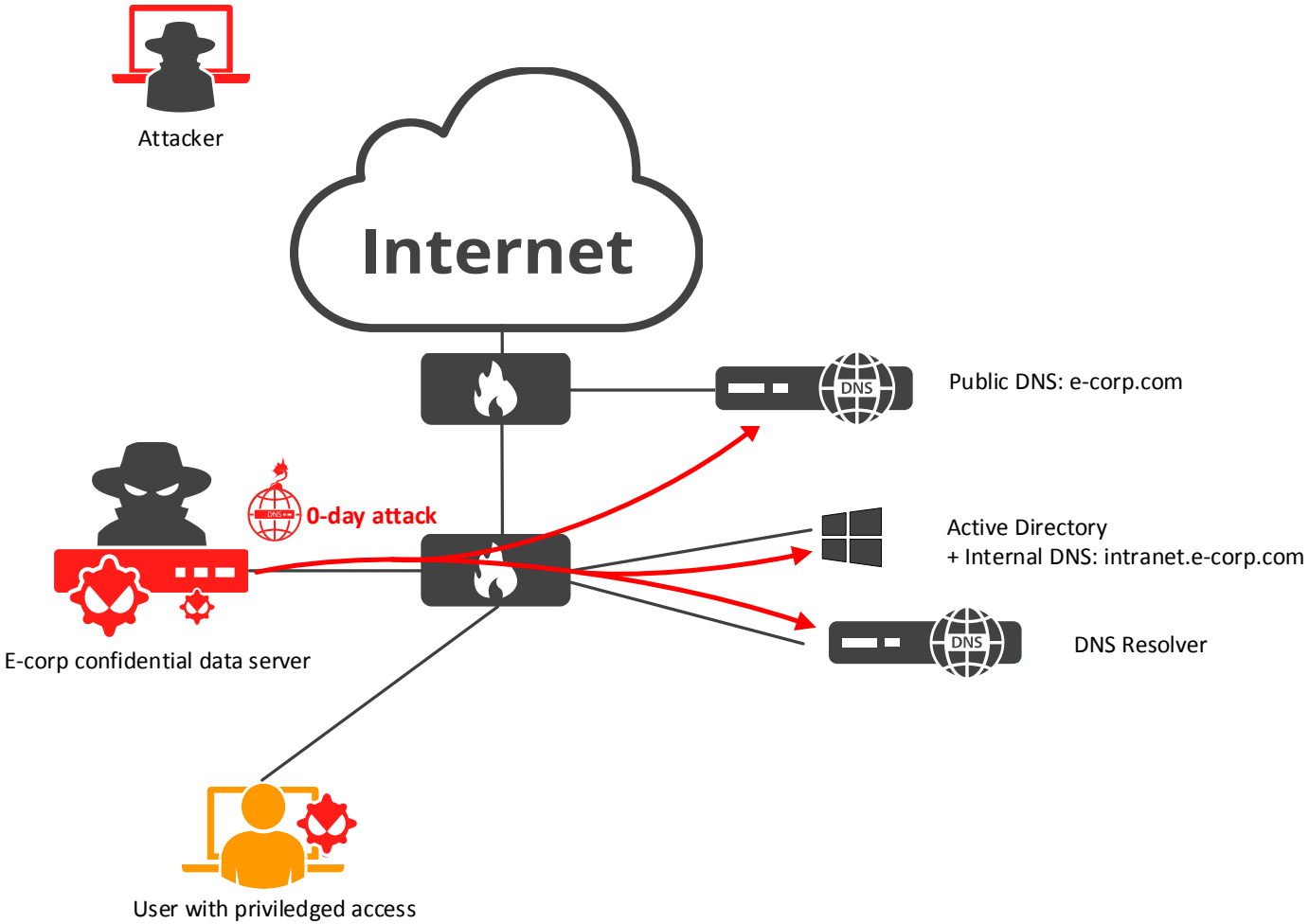


Stage 3: Actions on objectives
0-Day Denial of Service

- DoS attack
  - Using CVE on bind

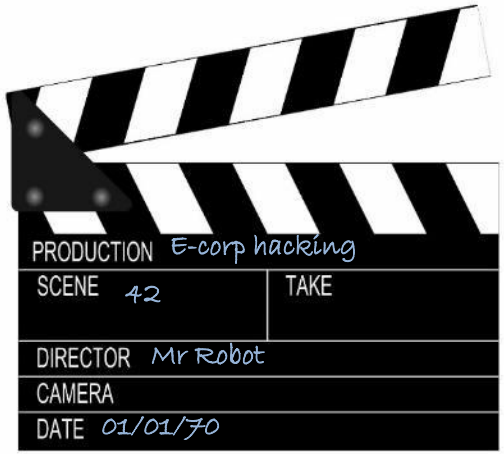
Stage 3: Actions on objectives

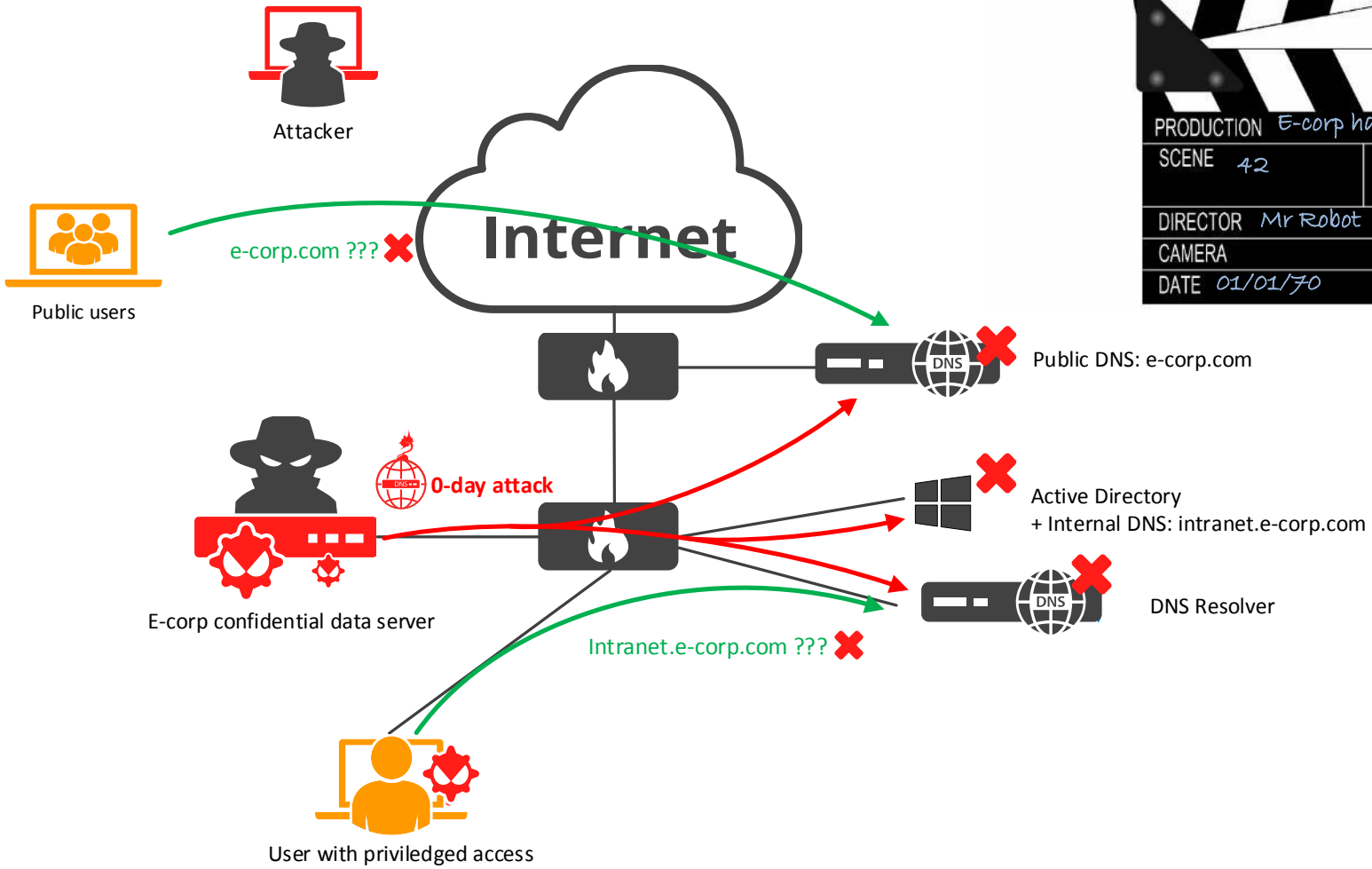
0-Day Denial of Service



Stage 3: Actions on objectives

0-Day Denial of Service



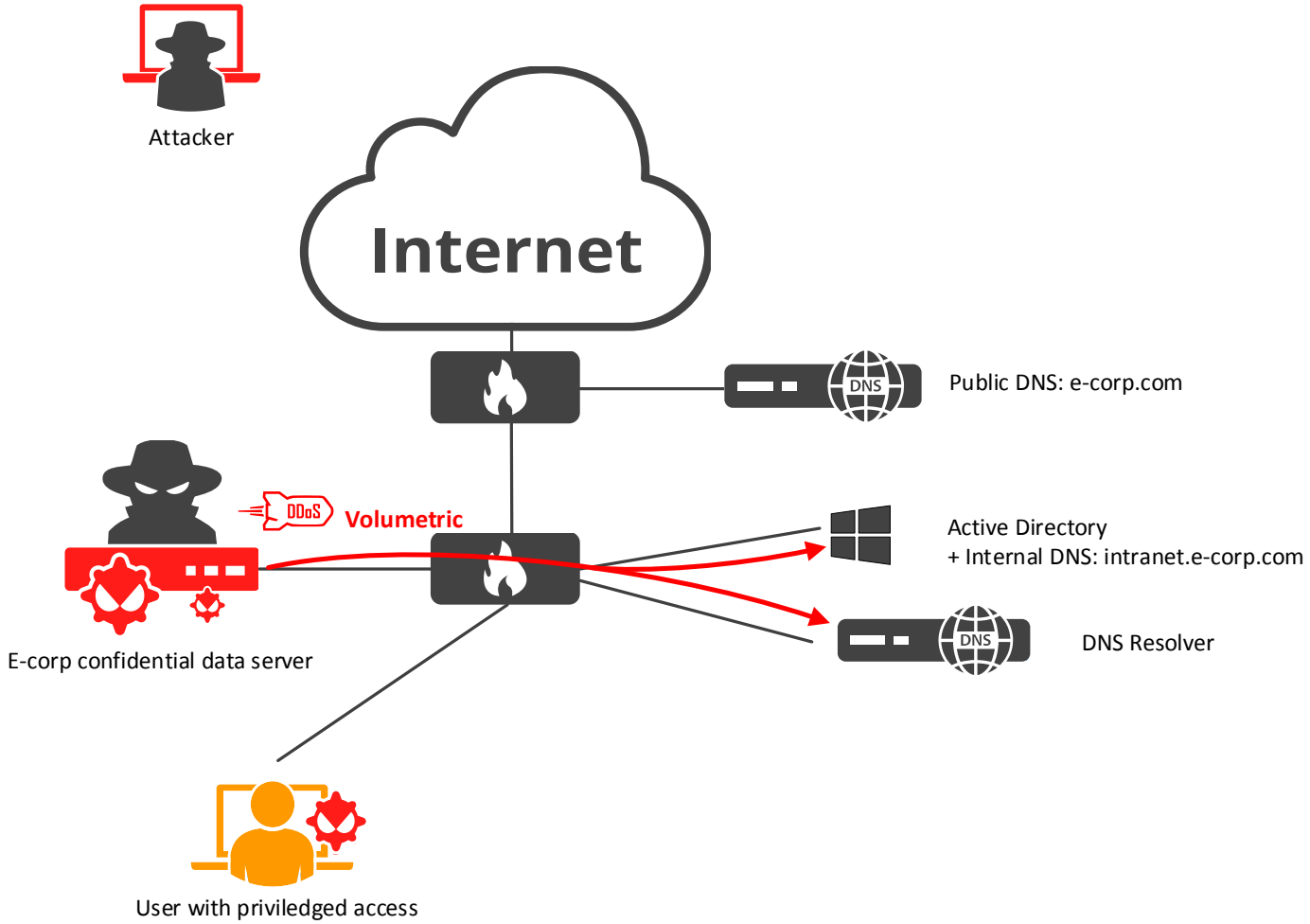


Stage 3: Actions on objectives
Volumetric Denial of Service

- DoS attack
  - Using big amount of queries per second

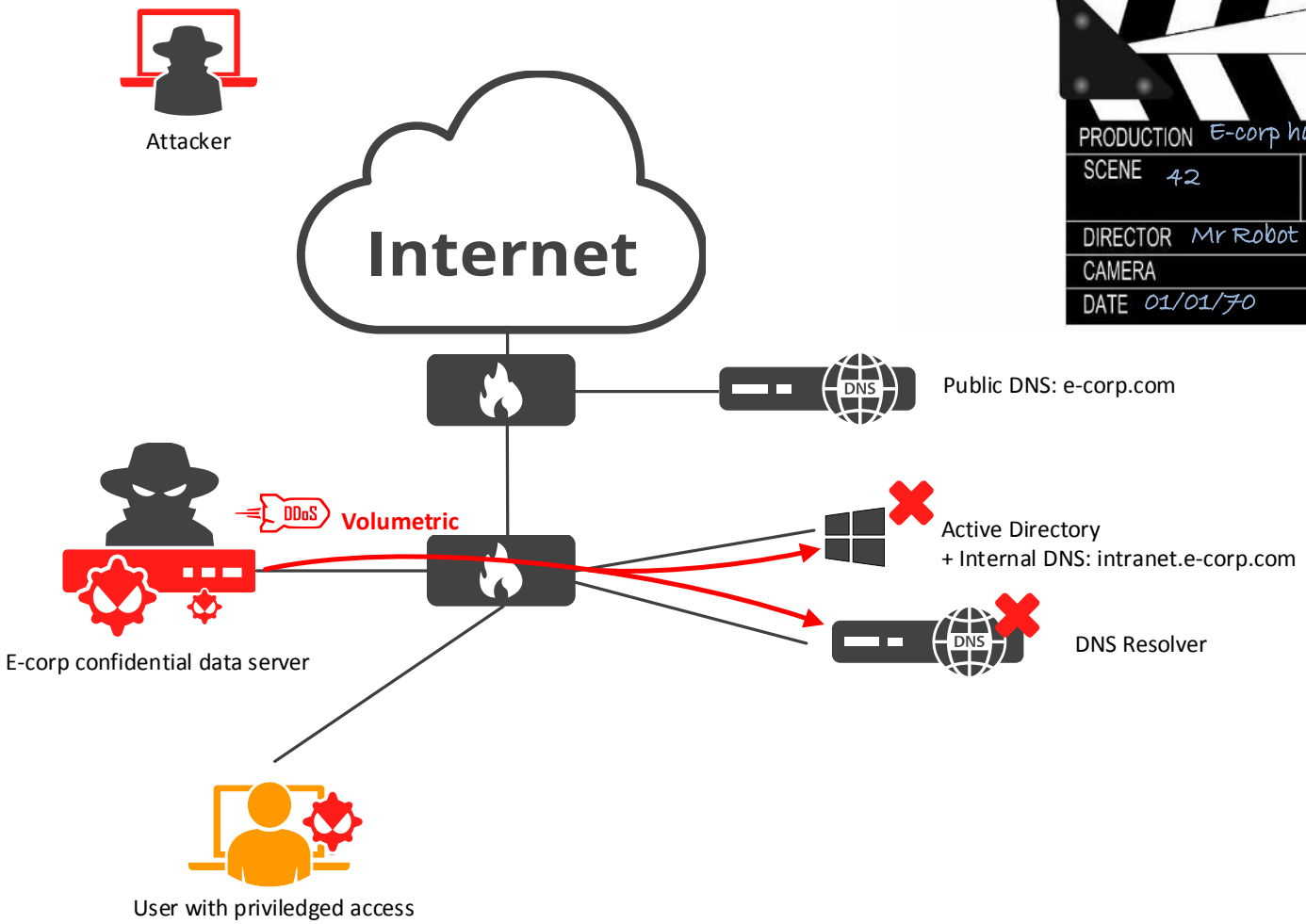
Stage 3: Actions on objectives

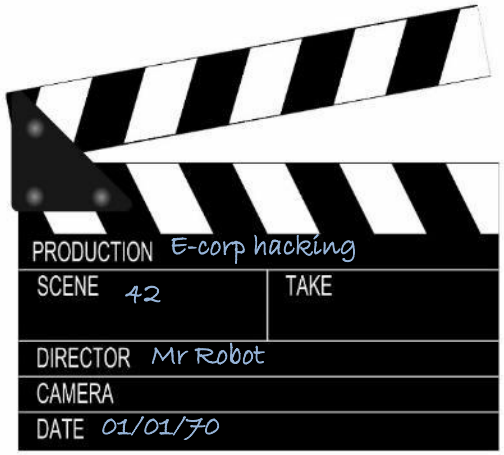
Volumetric Denial of Service



Stage 3: Actions on objectives

Volumetric Denial of Service





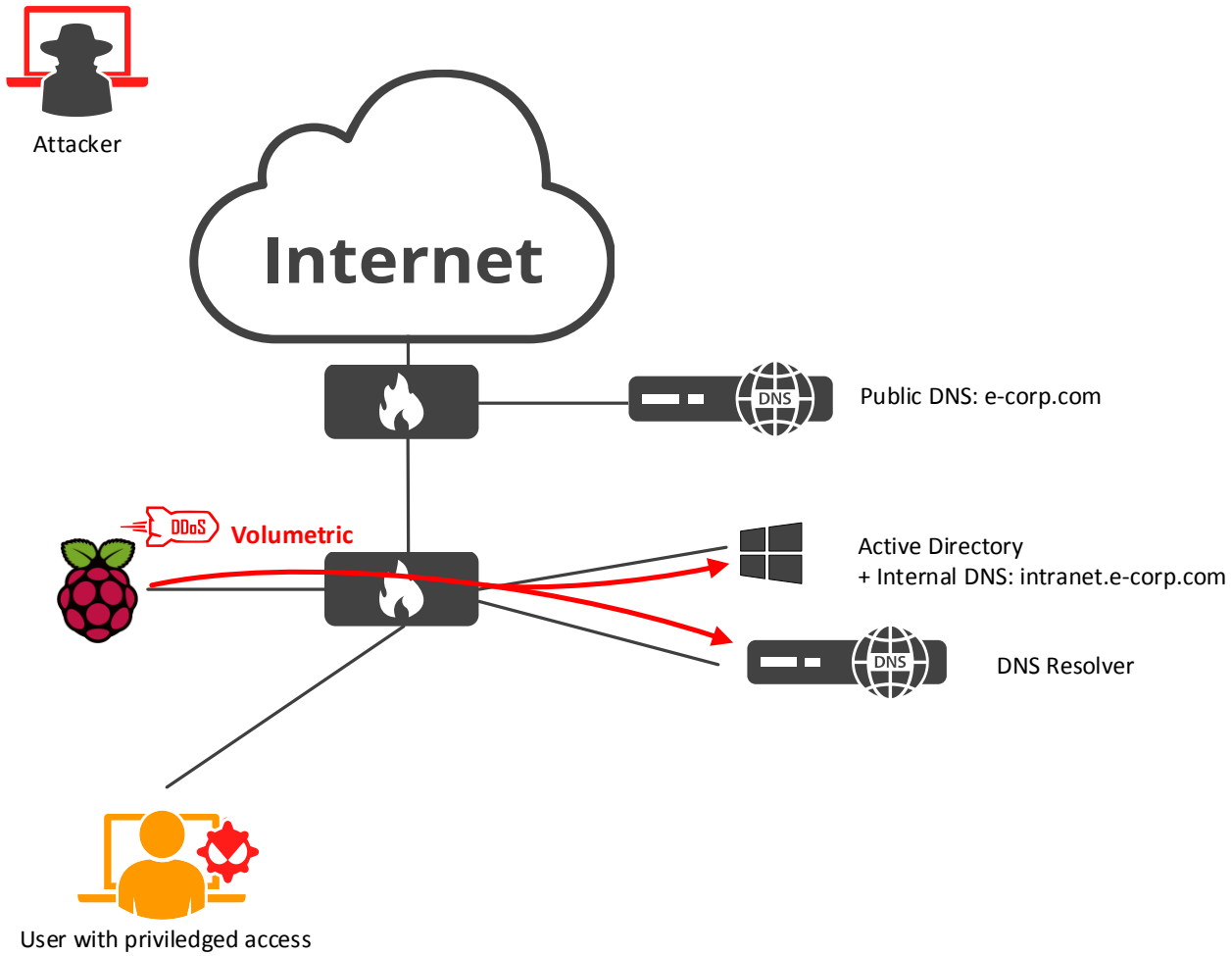
https://isc.org/wp-content/uploads/2015/07/ISC-Webinar-ISC-Random-Subdomain-CCA3.pdf

Stage 3: Actions on objectives
Volumetric Denial of Service

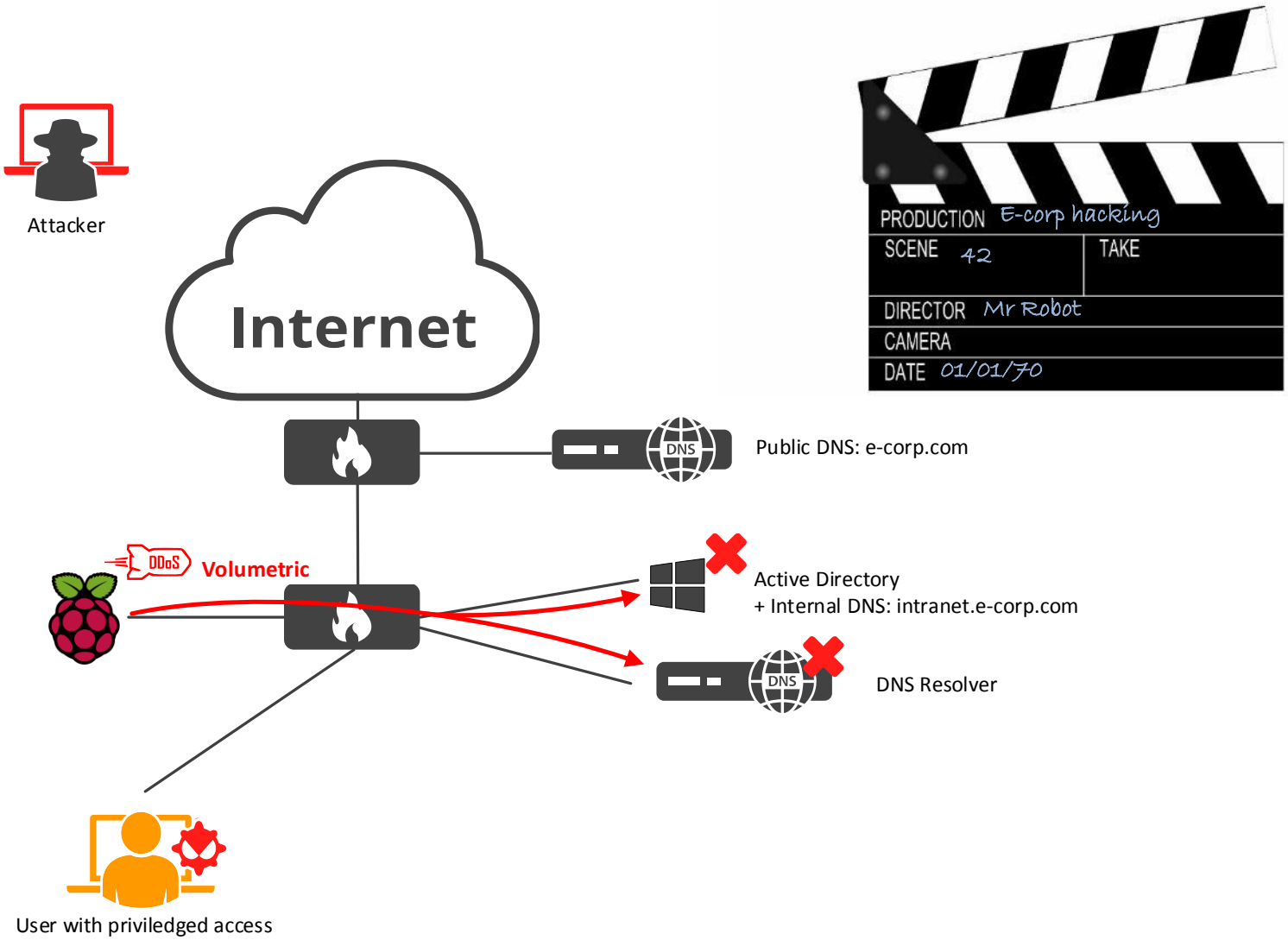
- DoS attack
  - Using other devices…

Stage 3: Actions on objectives

Volumetric Denial of Service

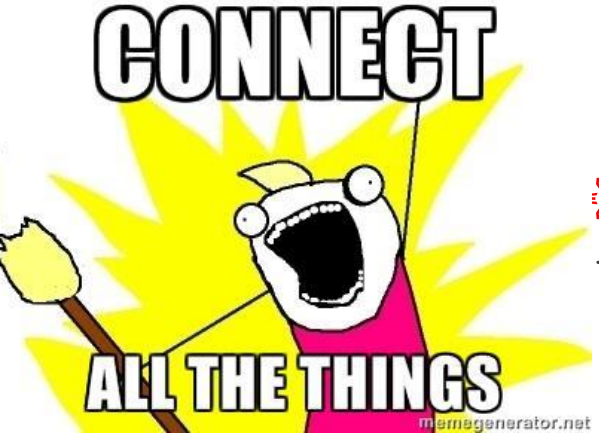


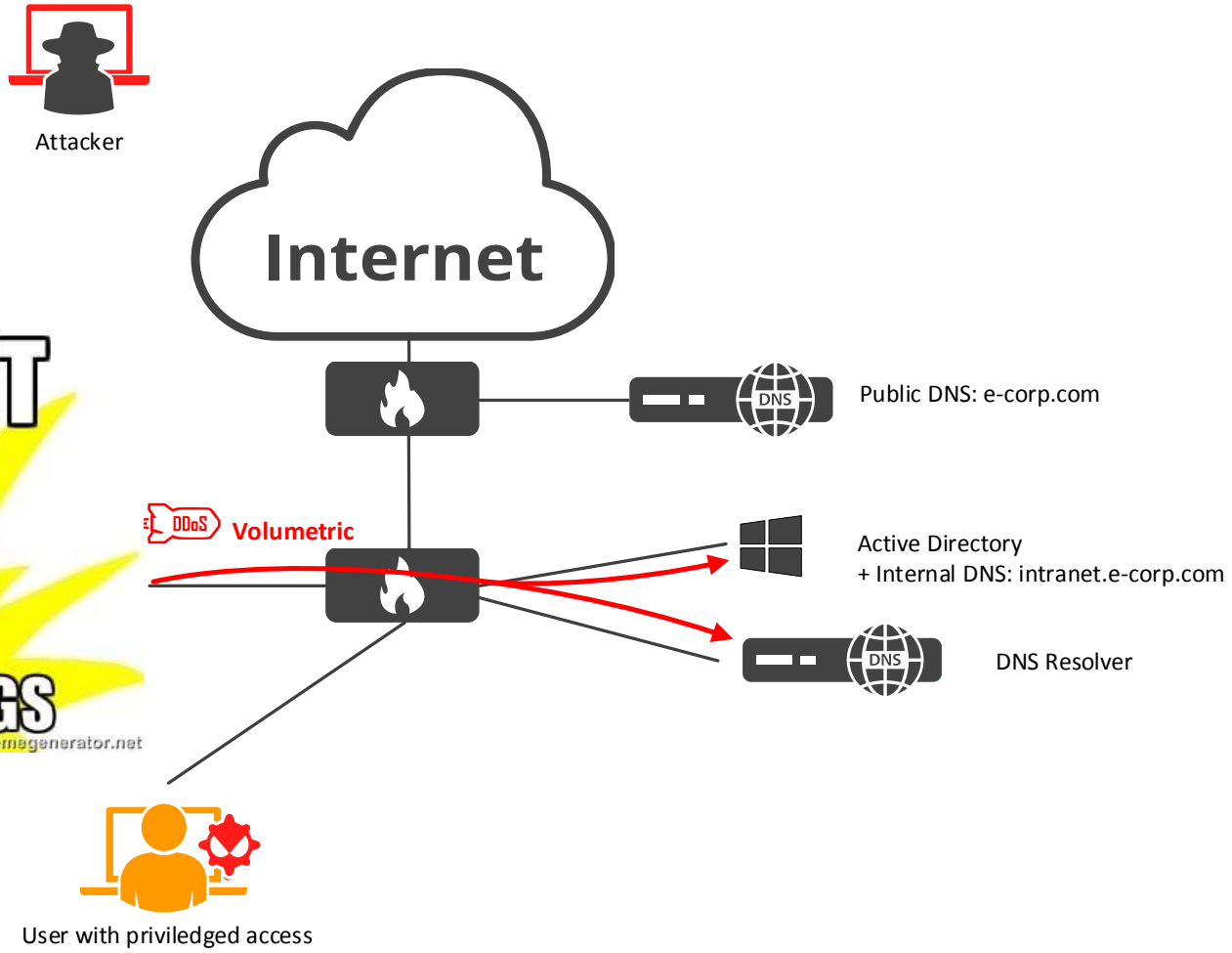
Stage 3: Actions on objectives



Stage 3: Actions on objectives

Distributed Denial of Service





Thank You

marck.to@efficientip.com

efficient iP™
DEFINING SMART DDI