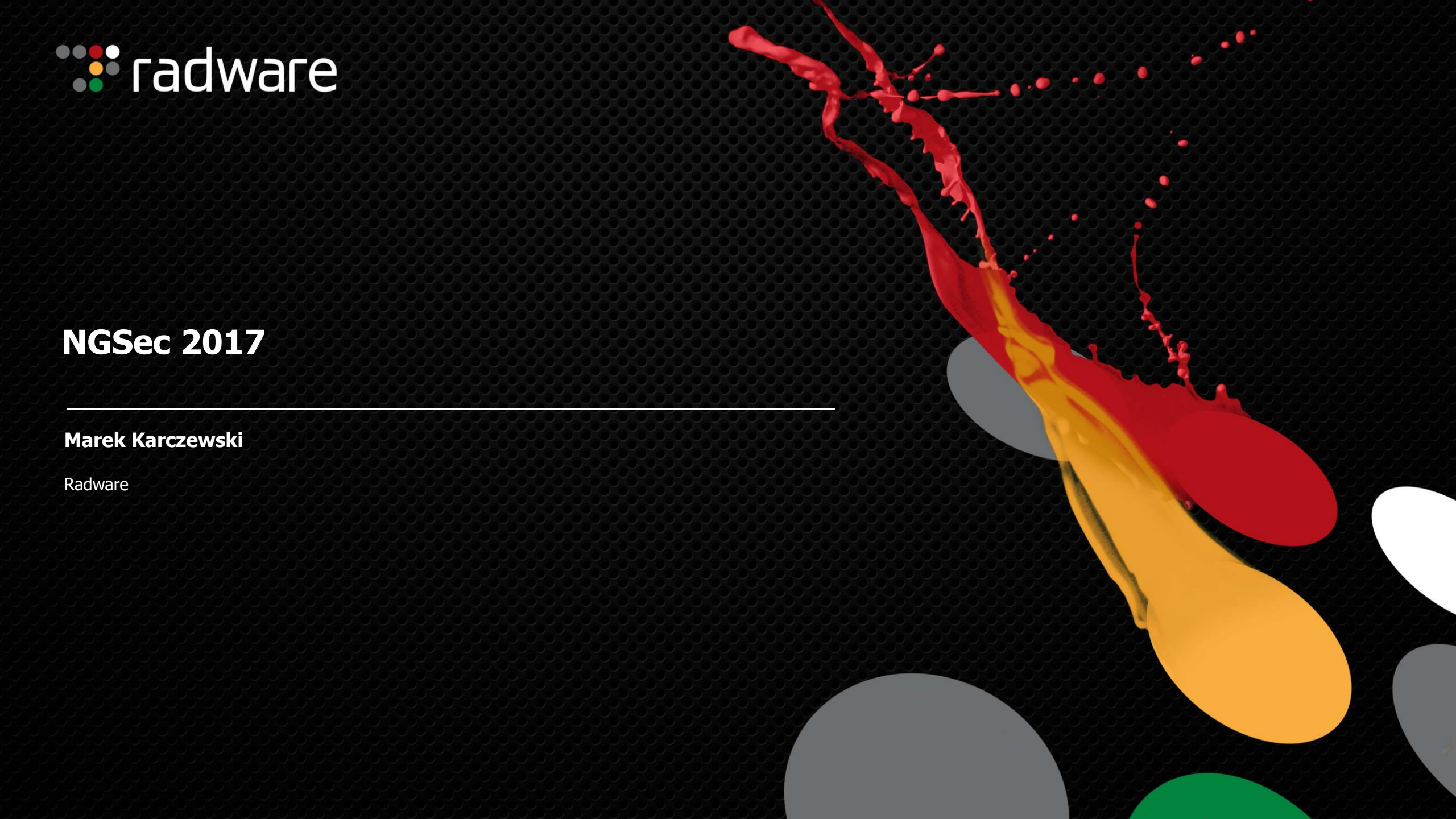


NGSec 2017

Marek Karczewski

Radware

radware

Cyber Attacks

Sales Tools

Resource Map

Products

Solutions

Cloud Services

Cross Sell

Applications

Promotions

Latest in Sales Tools

Radware Cloud Security Services - Sales Presentation

21 February, 2017
No description available

Download

Radware Cloud DDoS Protection Services - Service Description

20 February, 2017
No description available

Download

Security Solutions for Cloud Providers Presentation

Corporate Resources

If you are after the corporate presentation, an RFP template or the archive of the Radware insider newsletter – look no further. The corporate Resources page combines the content developed for you by corporate marketing

RFI/RFP Response Tools & Templates

FastView Sales Portal

Radware Corporate Data Sheet 2016 v2

Radware Departments Organization Chart

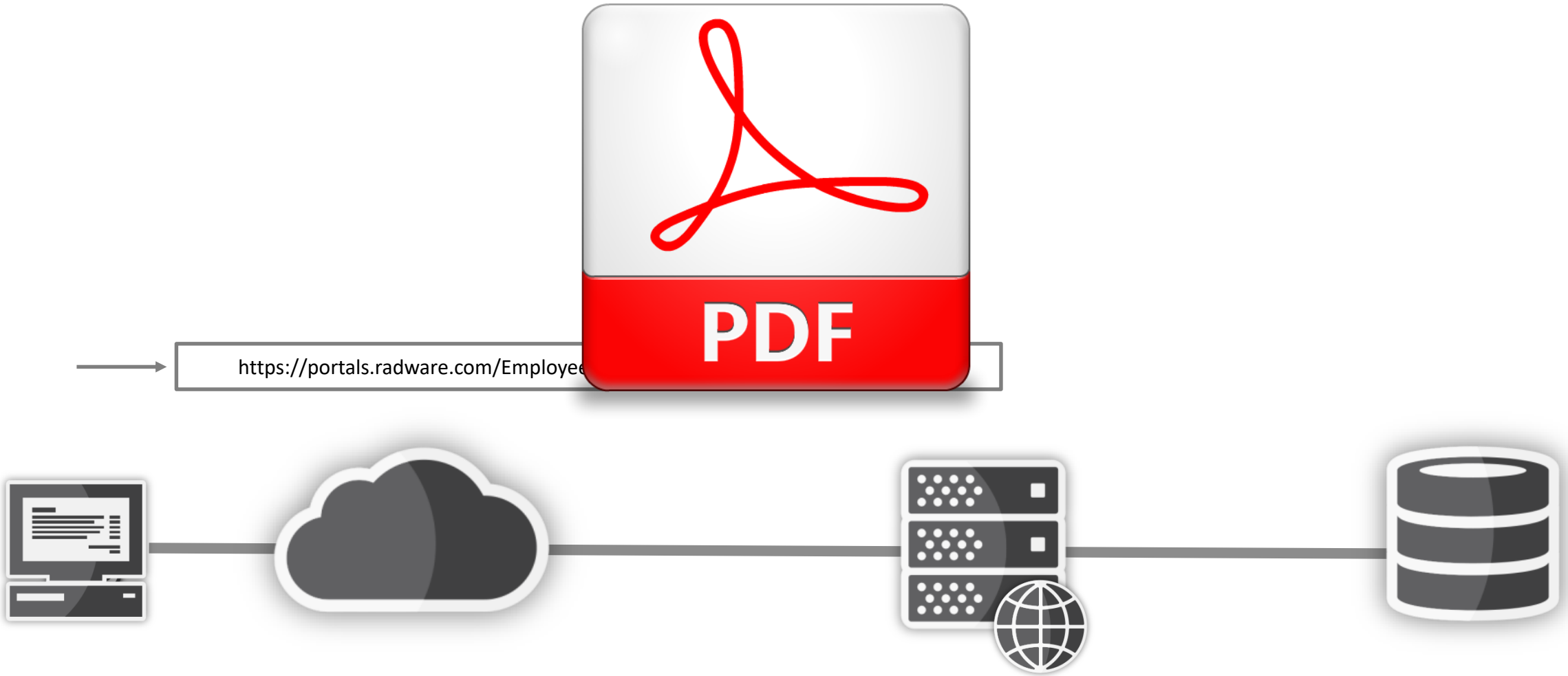
Radware Solutions Toolkit

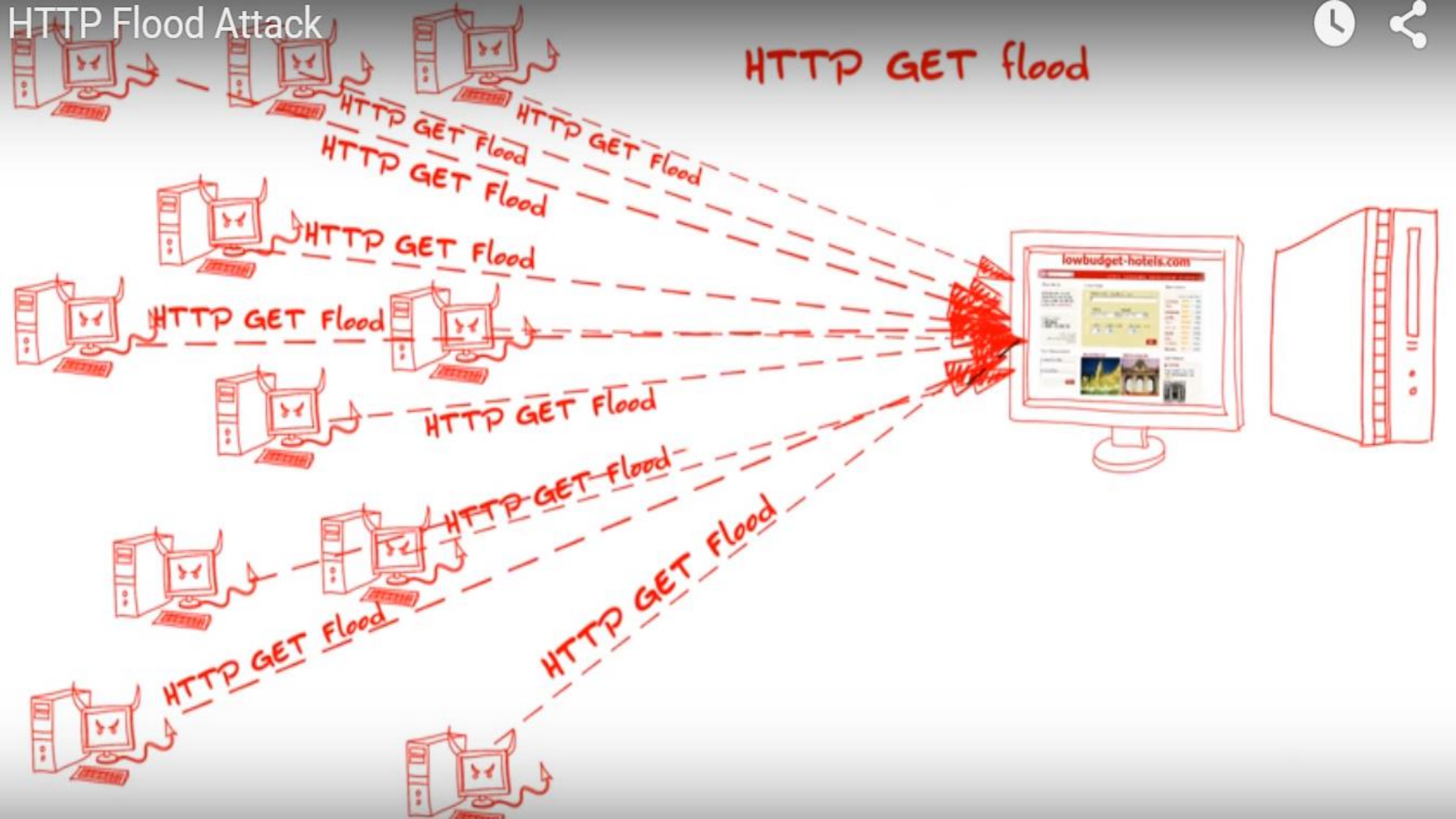
Radware Enterprise Introduction Letter

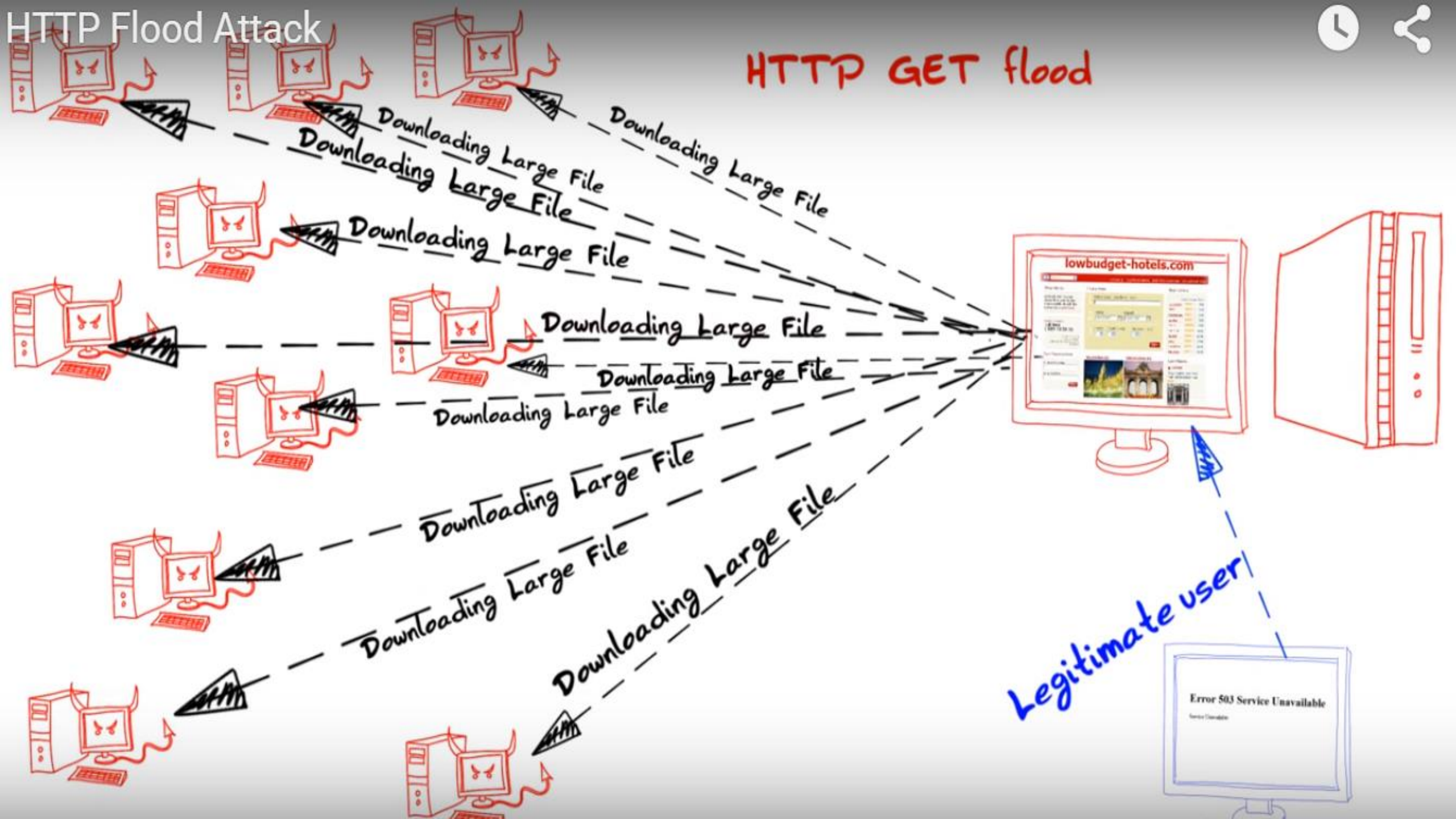
Radware Intro for Enterprise

Product Shipping Cover Page

HTTP „GET” Flood Attack




HTTP Flood Attack
HTTP GET flood
HTTP GET Flood
HTTP GET Flood
HTTP GET Flood
HTTP GET Flood
HTTP GET Flood
HTTP GET Flood
HTTP GET Flood
HTTP GET Flood
HTTP GET Flood
HTTP GET Flood
lowbudget-hotels.com


HTTP Flood Attack
HTTP GET flood
Downloading Large File
Downloading Large File
Downloading Large File
Downloading Large File
Downloading Large File
Downloading Large File
Downloading Large File
Downloading Large File
Downloading Large File
Downloading Large File
lowbudget-hotels.com
Legitimate user
Error 503 Service Unavailable

Find a Radware Employee

People Search

Marek Karczewski

Find

Radware Products

Product Search

Enter MAC, SN or Customer Name

Find

Latest Documents

Alteon REST API Guide version 31.0.0.0 — Feb 21, 2017

Alteon Application Switch and VMware Horzion 7.0 Integration Guide — Feb 20, 2017

Employee News

Announcing the New Operator Toolbox Community

Come on in and see what's new in the first ever Radware's Operator Toolbox Community

Radware Blog gets a makeover!

Check out our new user-friendly design

Alteon NG Go-To-Market Online Course

Announcing the new e-learning course for Radware's Application Delivery (ADC) solution!

Human Resources

HR Training

CoffeeTech

Onboarding

HR Documentation

Search Employee

Search Employee

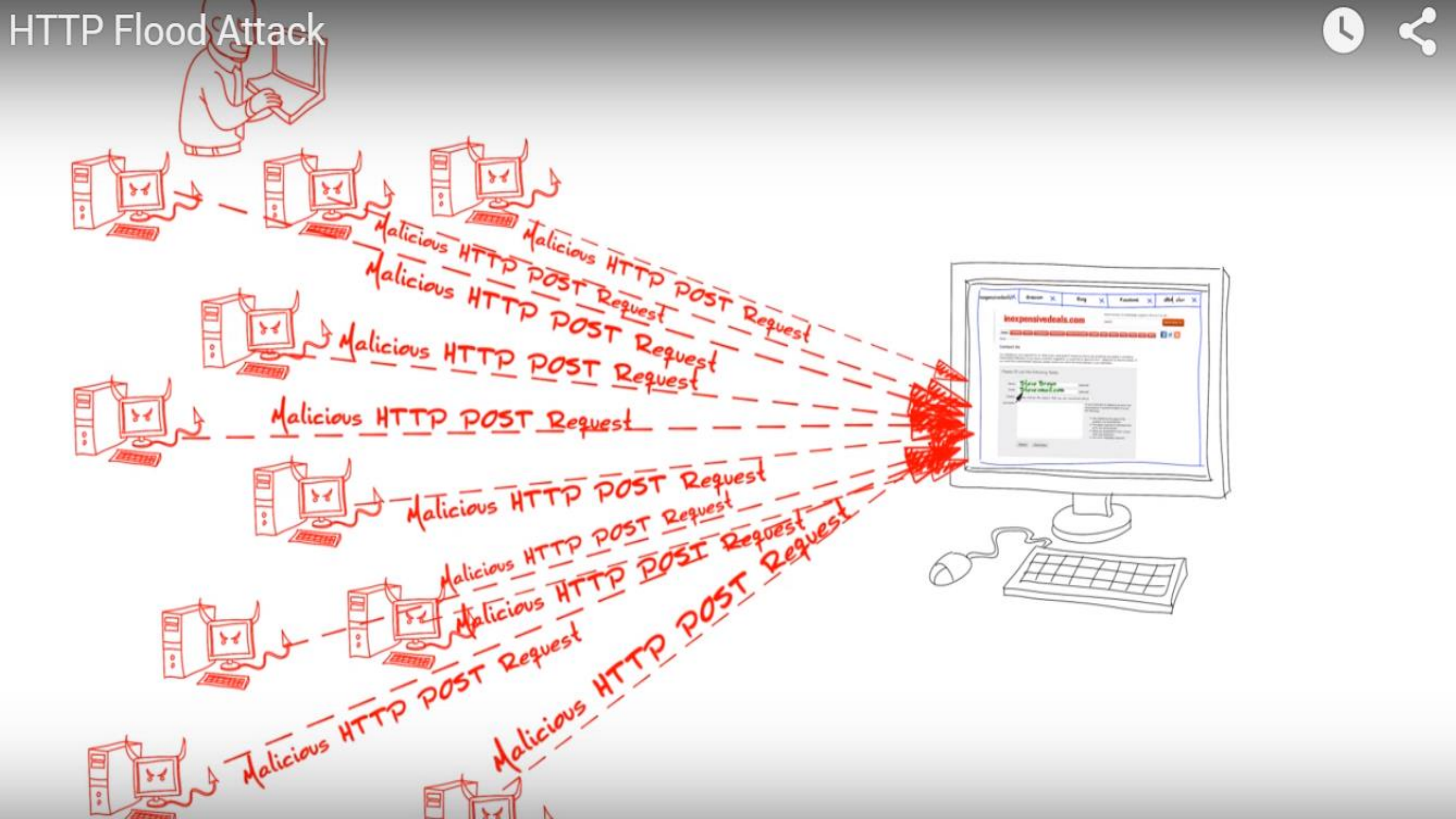
1 Results found

Search Employees: Marek Karczewski

Search

Marek Karczewski

ID: 33806
T:
E: marekk@radware.com
P: +972 723917977
M: +48 601080454
IP:


HTTP Flood Attack
Malicious HTTP POST Request
Malicious HTTP POST Request
Malicious HTTP POST Request
Malicious HTTP POST Request
Malicious HTTP POST Request
Malicious HTTP POST Request
Malicious HTTP POST Request
Malicious HTTP POST Request
Malicious HTTP POST Request
Malicious HTTP POST Request
inexpensivedeals.com

Find a Radware Employee

People Search

' OR 'a'='a

Find

Radware Products

Product Search

Enter MAC, SN or Customer Name

Find

Latest Documents

Alteon REST API Guide version 31.0.0.0 — Feb 21, 2017

Alteon Application Switch and VMware Horzion 7.0 Integration Guide — Feb 20, 2017

Employee News

Announcing the New Operator Toolbox Community

Come on in and see what's new in the first ever Radware's Operator Toolbox Community

Radware Blog gets a makeover!

Check out our new user-friendly design

Alteon NG Go-To-Market Online Course

Announcing the new e-learning course for Radware's Application Delivery (ADC) solution!

SQL Injection Attack


```
SELECT * FROM `CreditCardNumbers` WHERE `user`='' OR  'a'='a' AND `pass`='' OR  'a'='a'
```

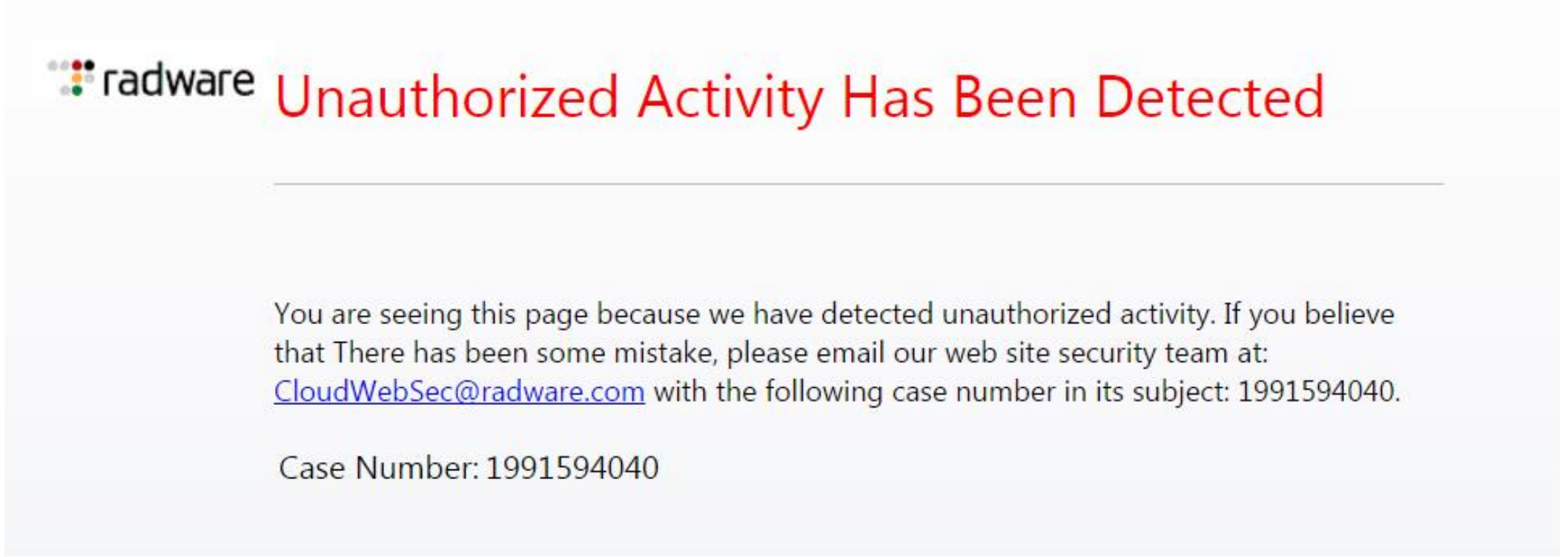
```
SELECT * FROM `login` WHERE `user`=''; INSERT INTO `login` ('user','pass') VALUES (,John',,Doe');--' AND `pass`=''
```

```
SELECT * FROM `login` WHERE `user`=''; UPDATE `login` SET `pass`='pass123' WHERE `user`='Marek';--' AND `pass`=''
```

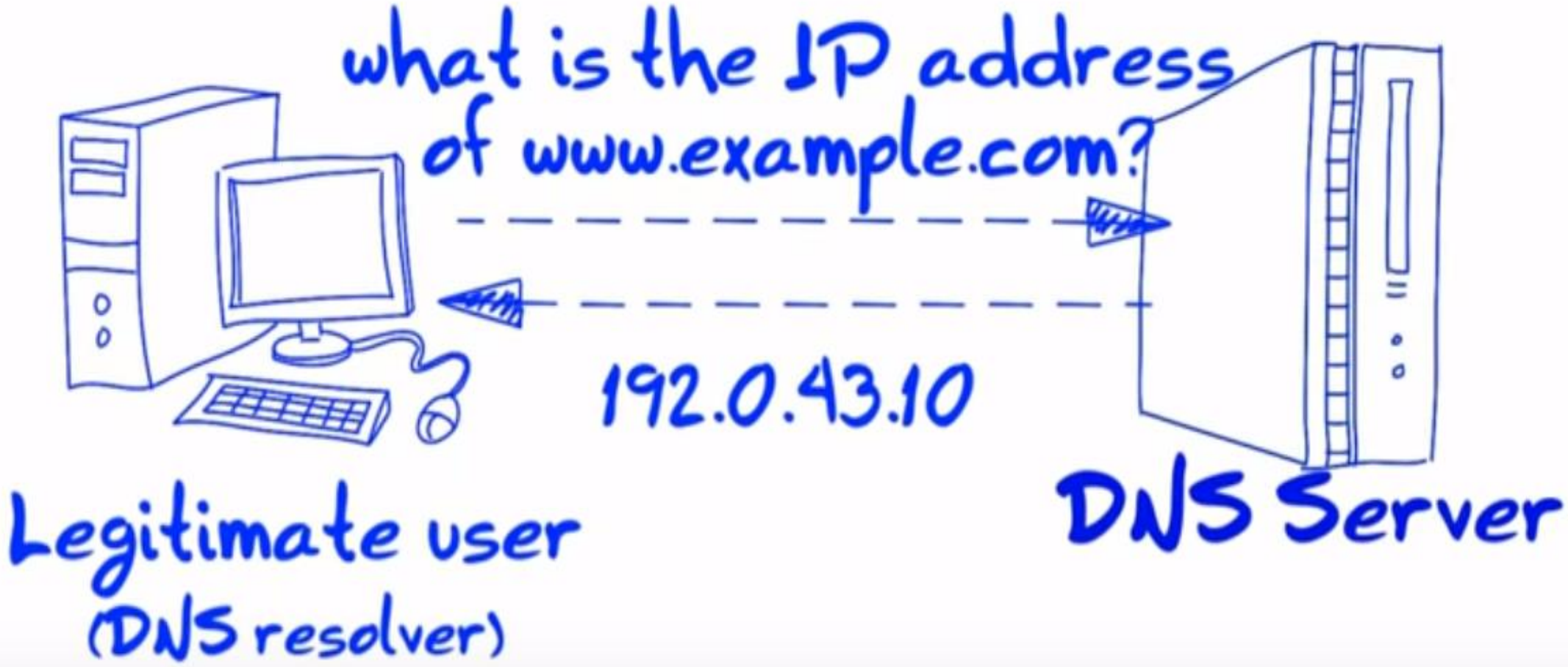
IP: IP: IP:

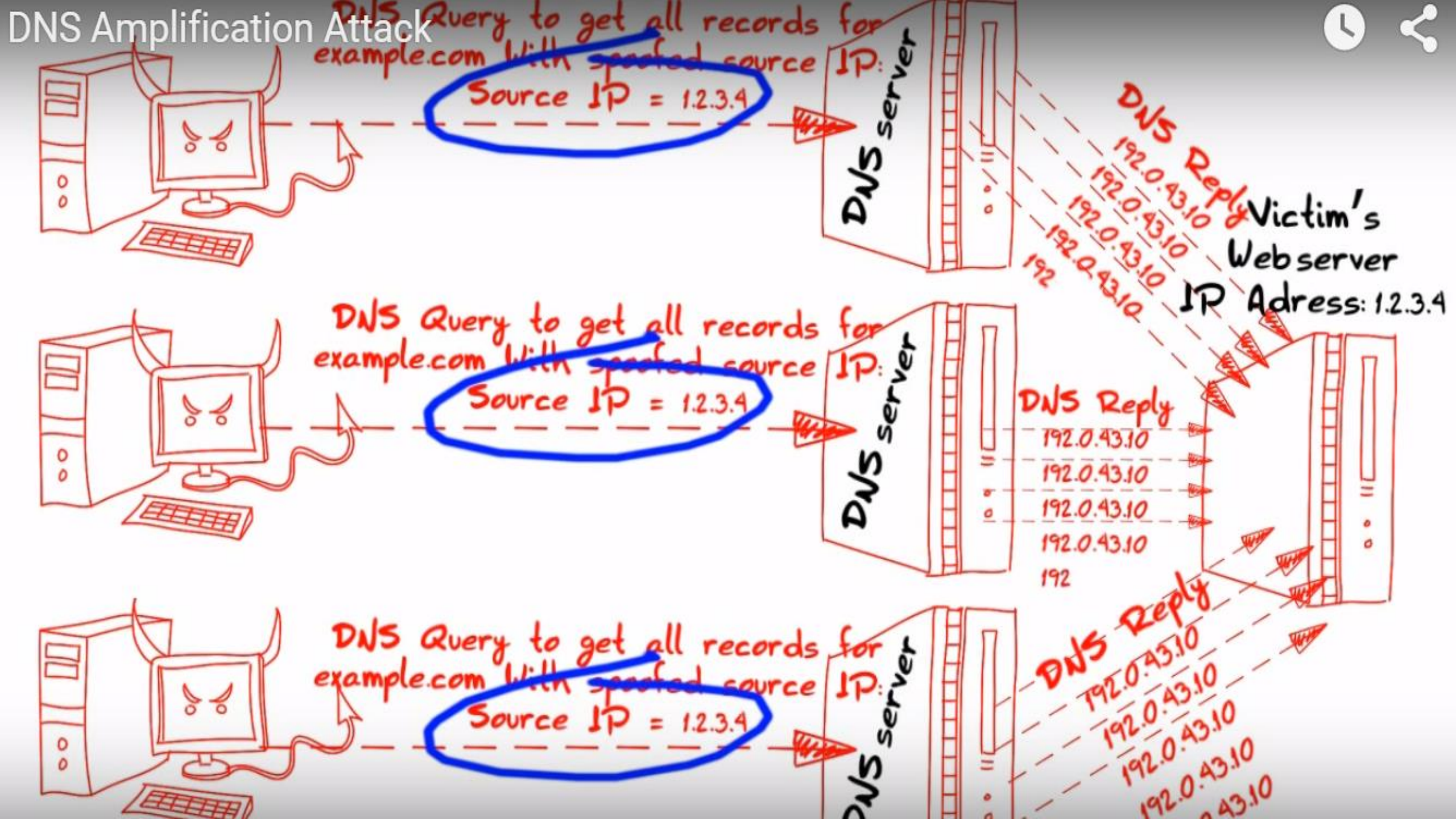
SQL Injection Attack

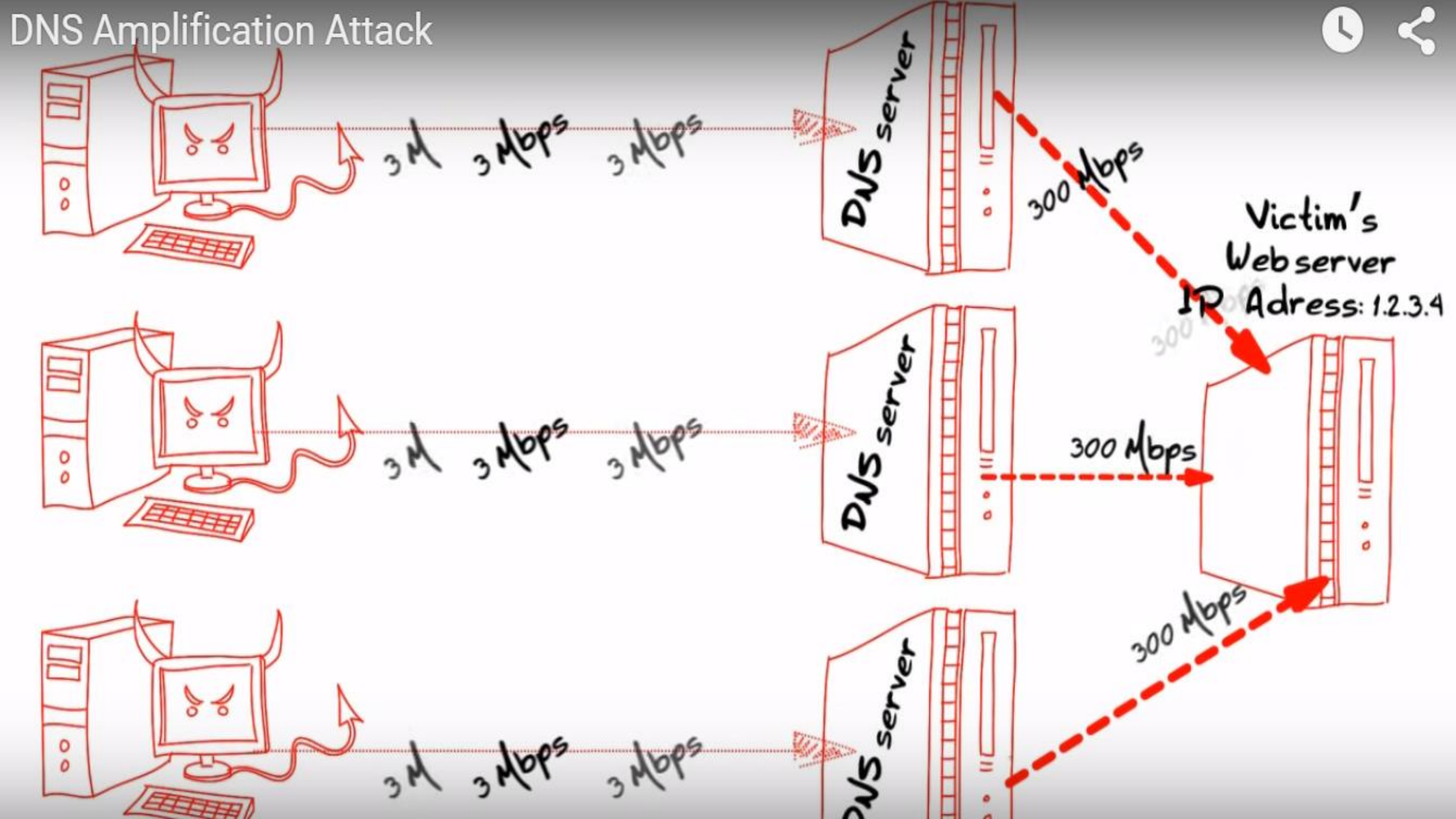
WAF



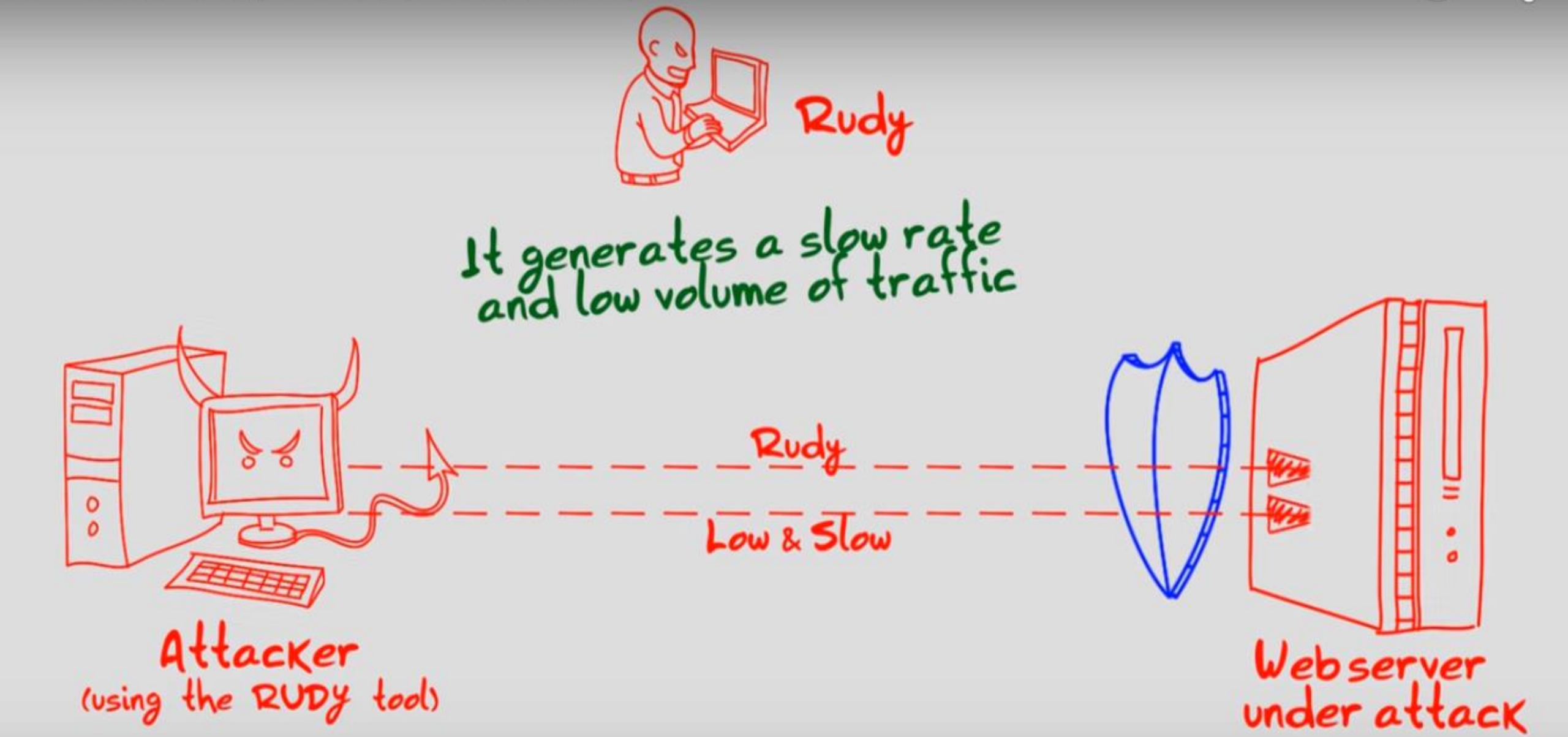
DNS Amplification Attack




DNS Amplification Attack
DNS Query to get all records for example.com With spoofed source IP:
Source IP = 1.2.3.4
DNS server
DNS Reply
192.0.43.10
192.0.43.10
192.0.43.10
192.0.43.10
192
Victim's Webserver IP Adress: 1.2.3.4
DNS Query to get all records for example.com With spoofed source IP:
Source IP = 1.2.3.4
DNS server
DNS Reply
192.0.43.10
192.0.43.10
192.0.43.10
192.0.43.10
192
DNS Query to get all records for example.com With spoofed source IP:
Source IP = 1.2.3.4
DNS server
DNS Reply
192.0.43.10
192.0.43.10
192.0.43.10
192.0.43.10


DNS Amplification Attack
3M
3Mbps
3Mbps
DNS server
300 Mbps
Victim's
Webserver
IP Adress: 1.2.3.4
300 Mbps
300 Mbps

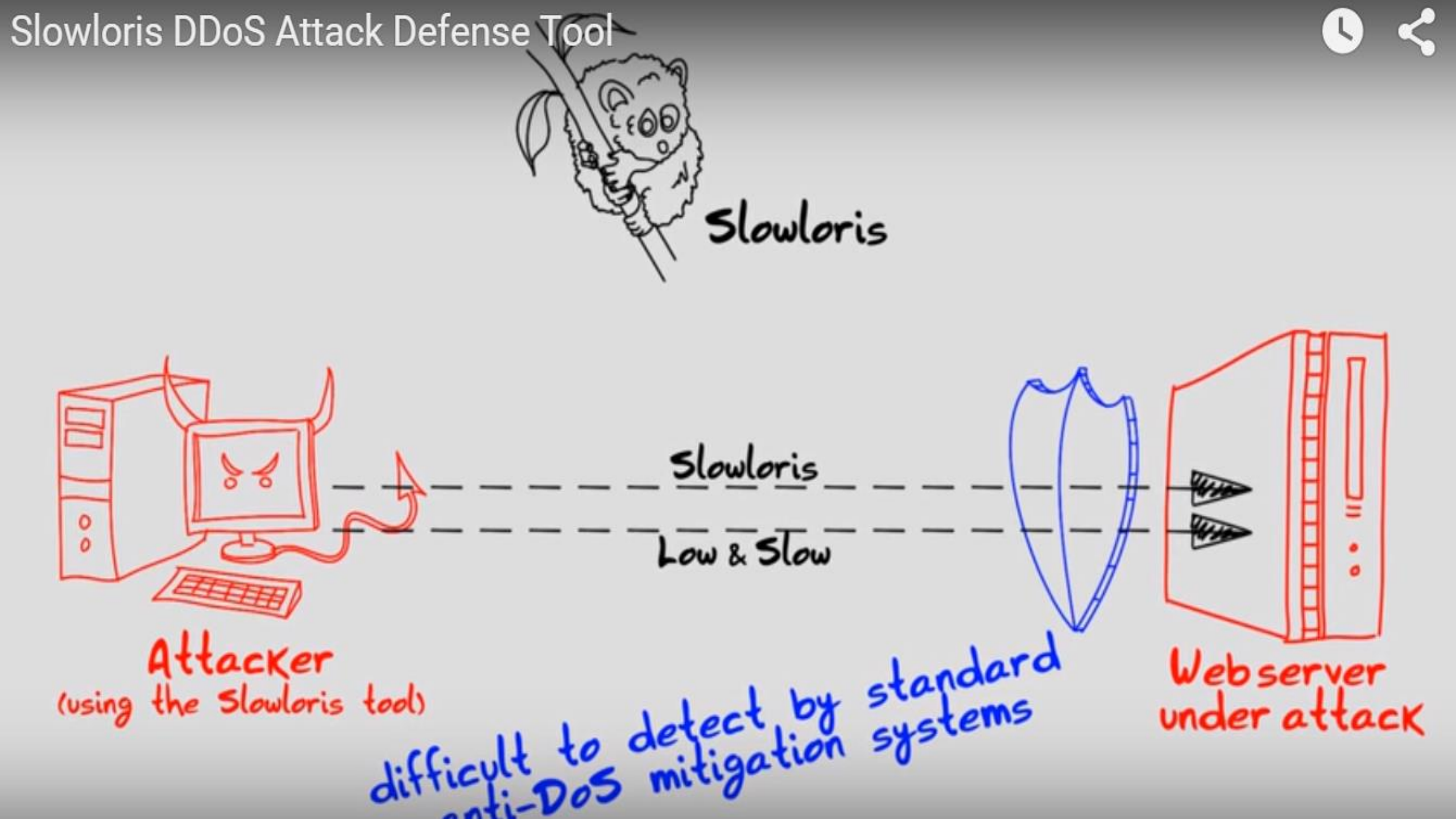
R-U-Dead-Yet, RUDY DDoS Attack Tool



R-U-Dead-Yet, RUDY DDoS Attack Tool

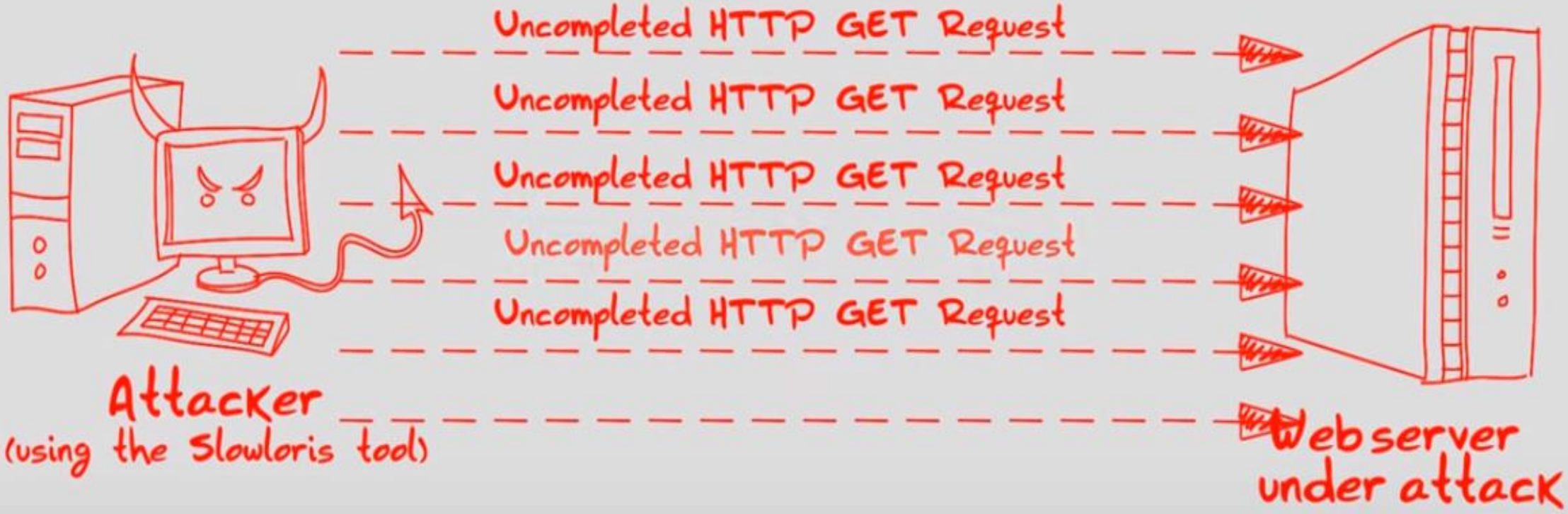
R-U-Dead-Yet, RUDY DDoS Attack Tool

Slowloris DDoS Attack Defense Tool



Slowloris DDoS Attack Defense Tool

Slowloris DDoS Attack Defense Tool

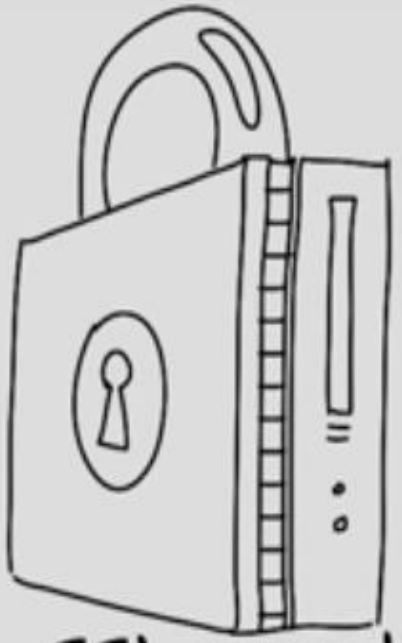


THC-SSL-DOS Attack Tool

The SSL protocol is used to secure connections and transactions over the Internet

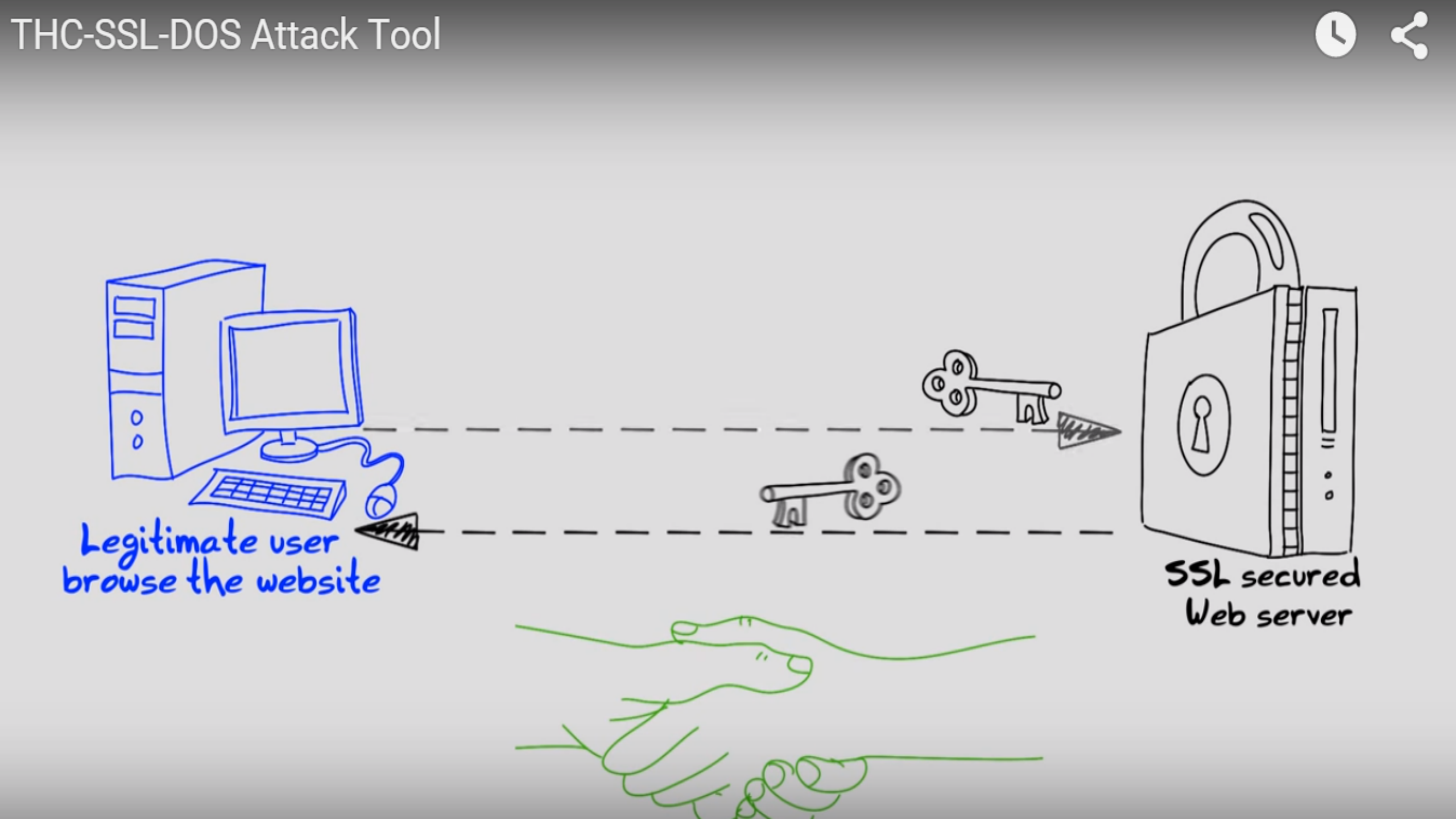
- online financial transactions
- web email
- social networks

Legitimate user browse the website



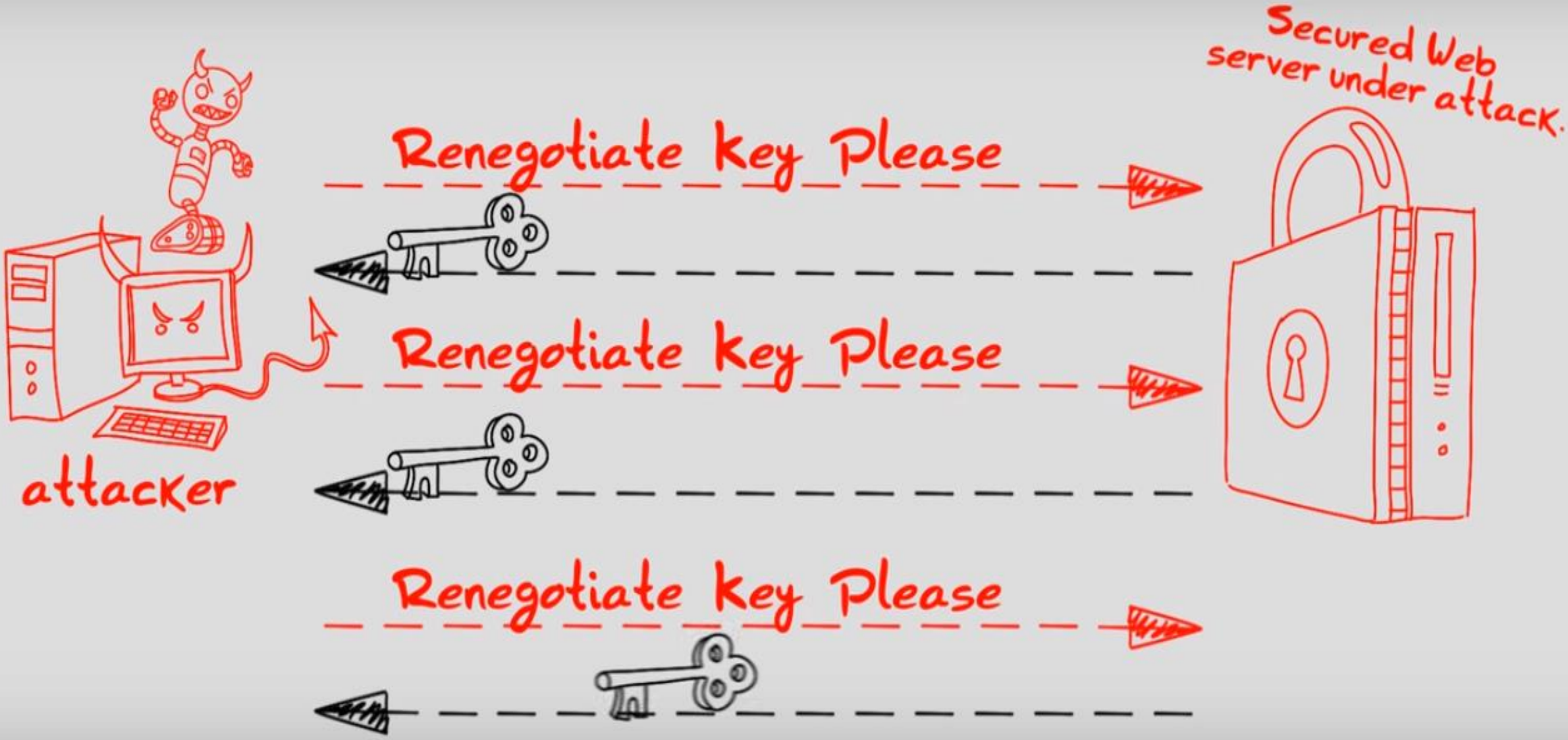
SSL secured Web server

THC-SSL-DOS Attack Tool

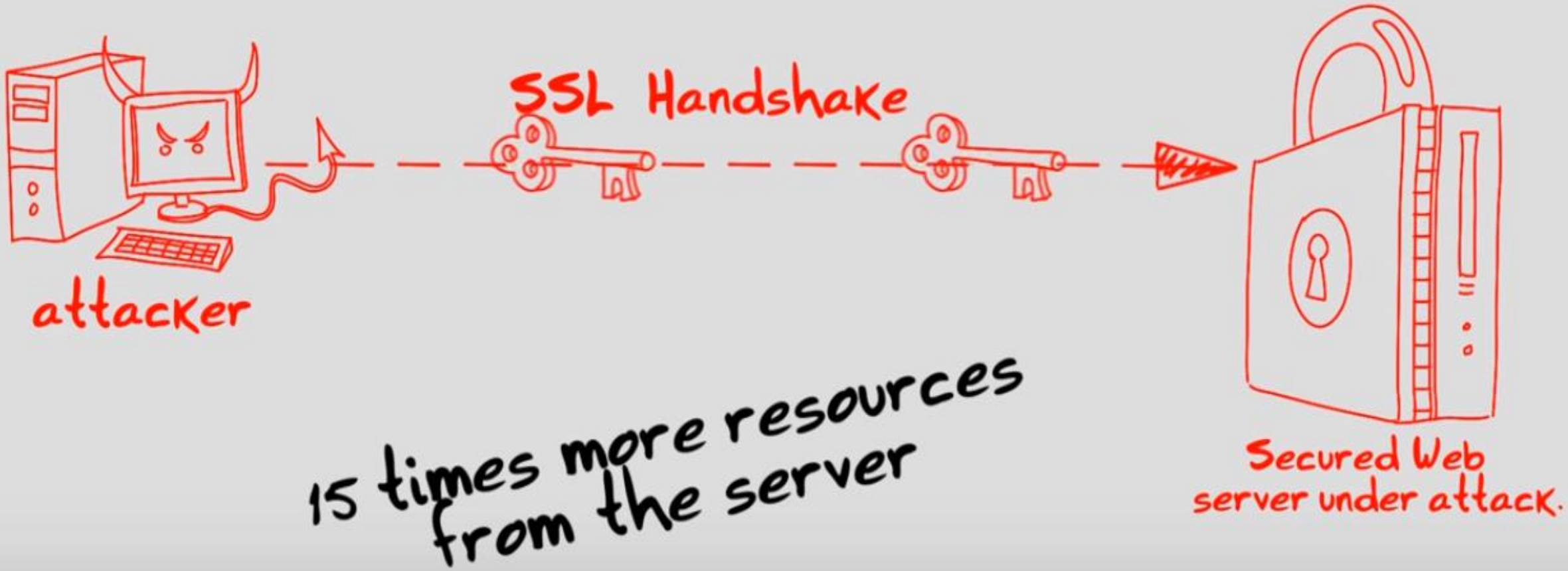


THC-SSL-DOS Attack Tool

THC-SSL-DOS Attack Tool



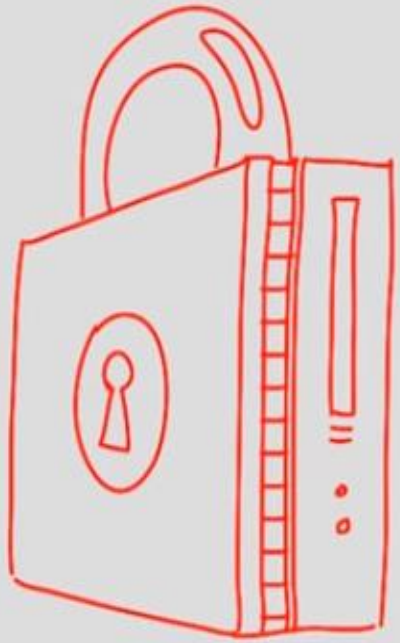
THC-SSL-DOS Attack Tool



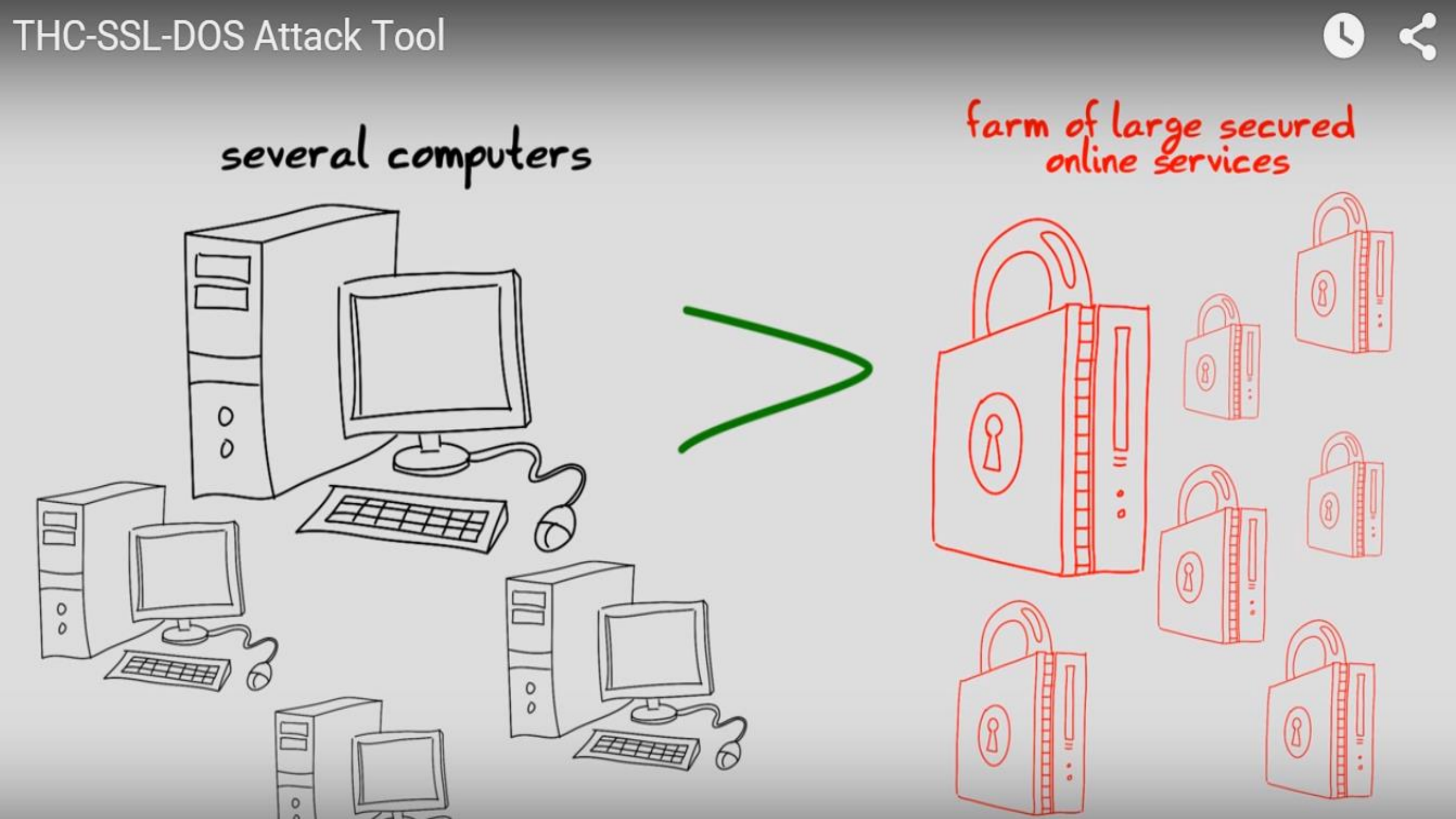
THC-SSL-DOS Attack Tool

1 standard home PC

SSL based web server

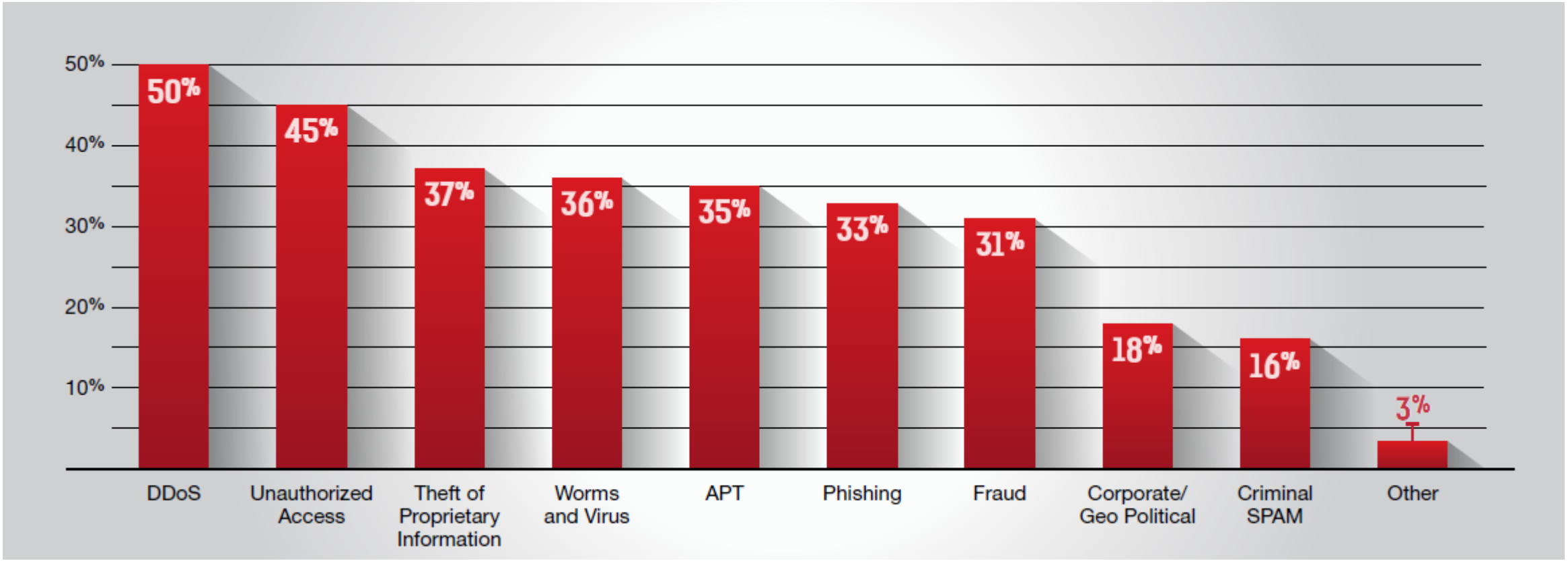


THC-SSL-DOS Attack Tool

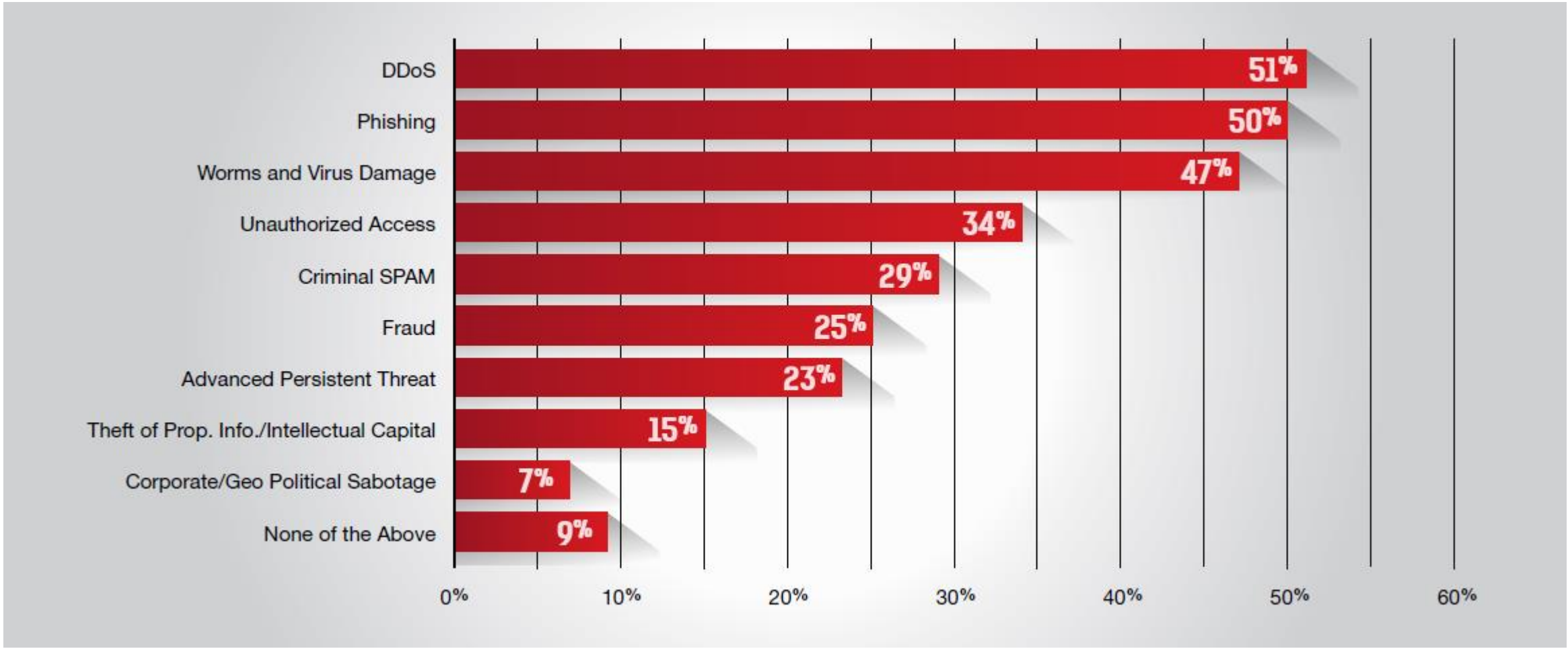


Cyber Attacks in numbers

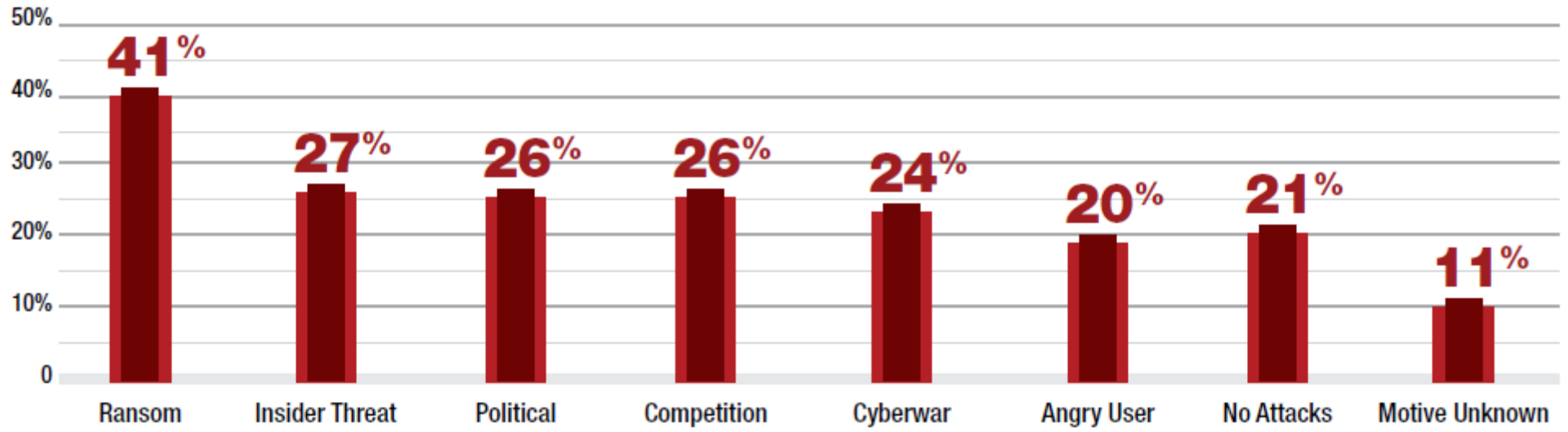
Attacks that will cause the most harm to businesses



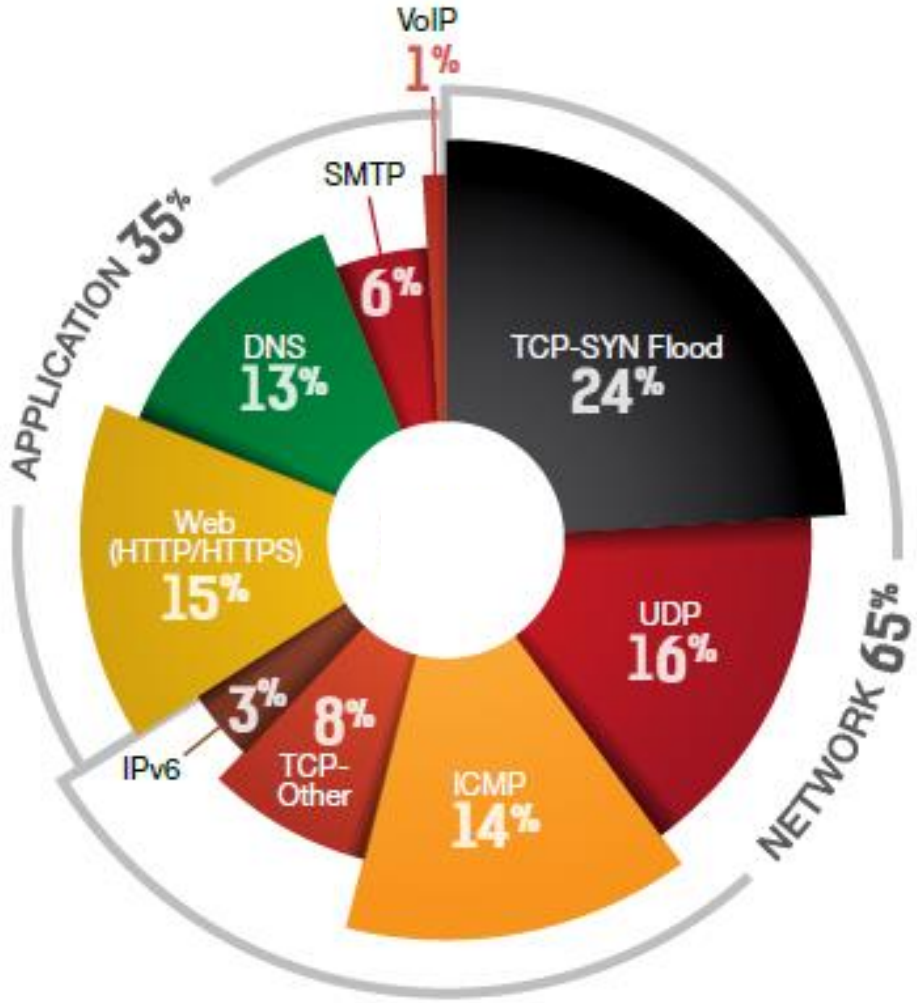
Types of Attacks Experienced By Organizations in 2015



Motives behind any cyber-attack



Biggest DDoS Attacks in 2016

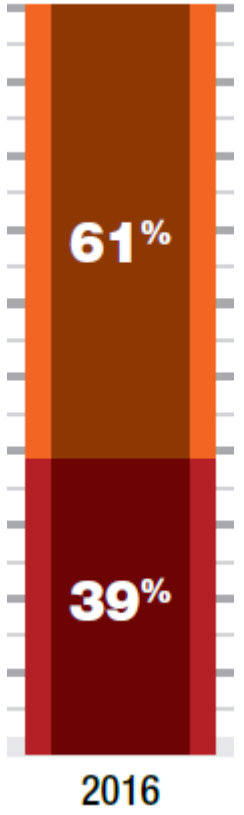


SSL or TLS based Attacks

Over 50% of traffic in enterprises is encrypted

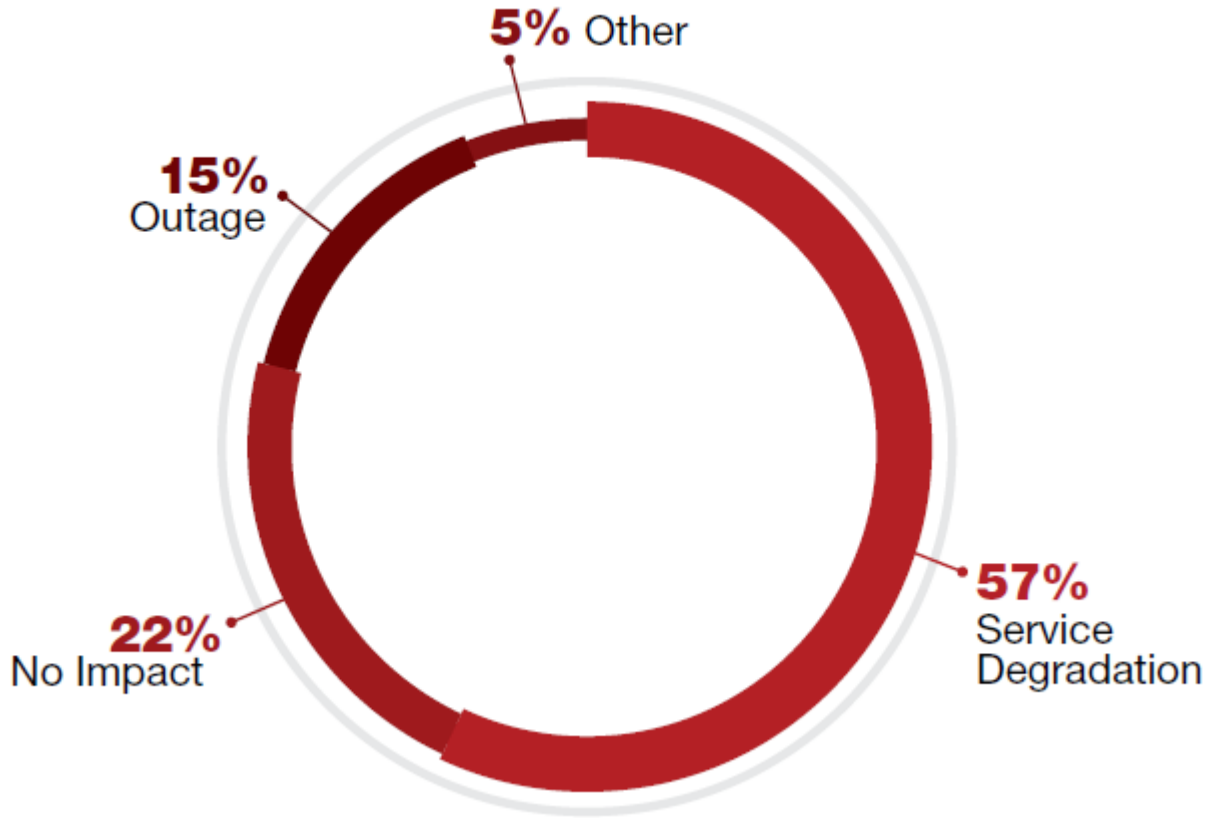
20% of organizations Inspect SSL

80% of organizations don't inspect SSL Traffic

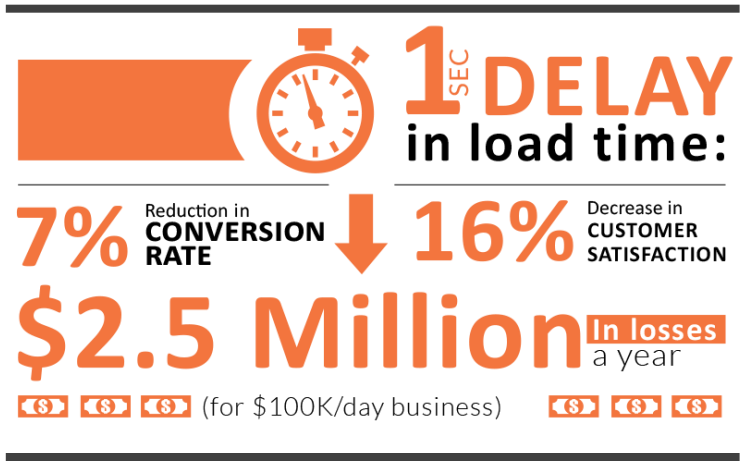


SSL based attacks in 2016

Impact of DDoS Attacks on Systems



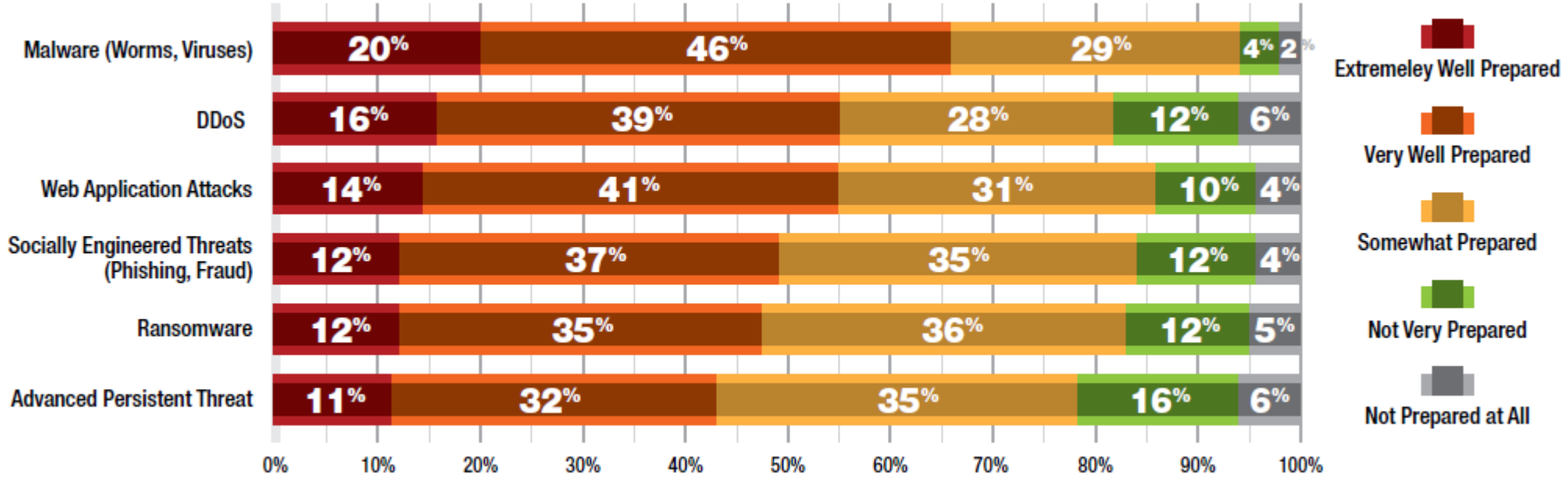
Impact of DDoS Attacks on Business



Today more than ever, **TIME IS MONEY**

Impact of DDoS Attacks on Business

How Prepared Are Today's Organizations?



Attacks on Krebs, OVH and Dyn

09/20 – KrebsOnSecurity.com target of record-breaking 620Gbps DDoS attack
09/21 – French web hoster OVH targeted by 1.5Tbps IoT DDoS attack
09/30 – Source Code of IoT Botnet Mirai Released on Hackforums.net by Anna-senpai

The Hackforums post that includes links to the Mirai source code.

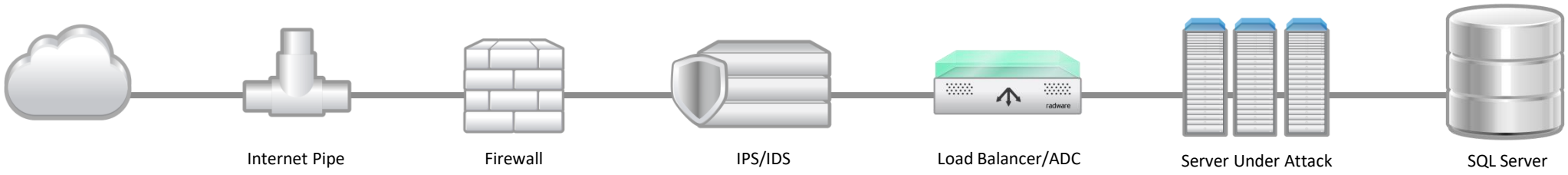
10/21 – Dyn's managed DNS infrastructure in the US under DDoS attack. Impacting many websites and services including Twitter, Amazon, Tumblr, Reddit, Spotify and Netflix

October 21st - DDoS attack on Dyn (Managed DNS Network) - Mirai malware

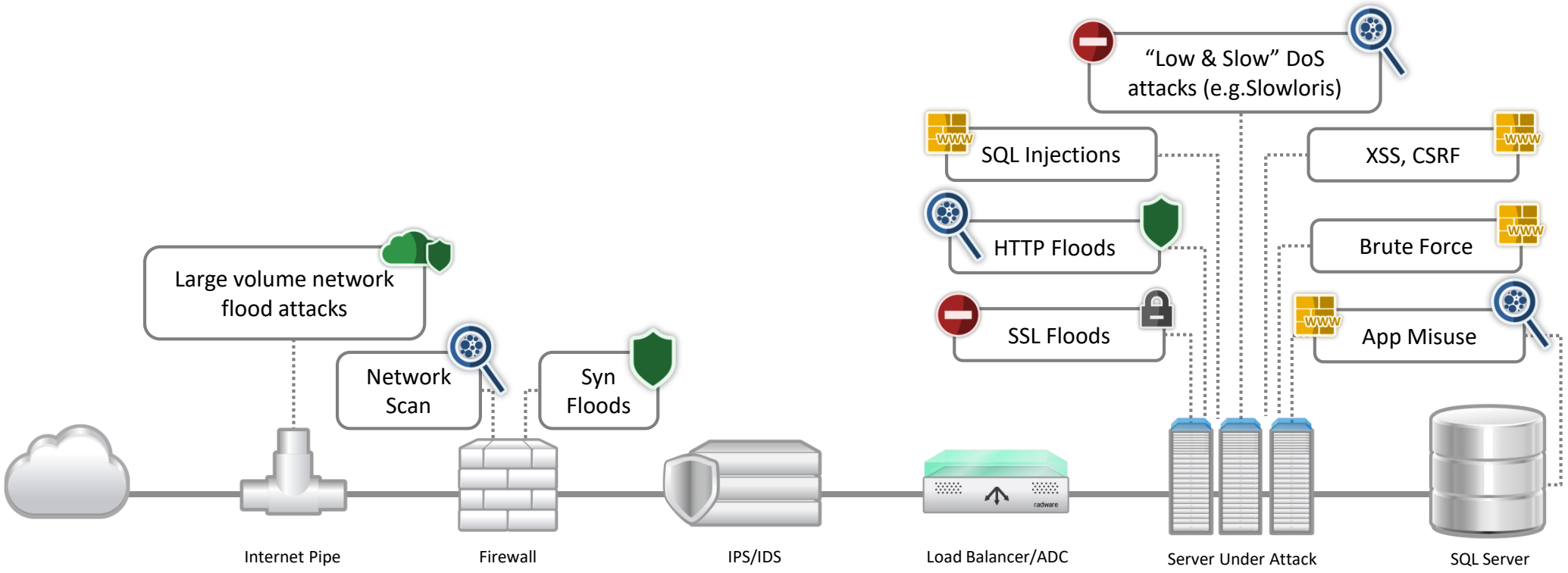
- ActBlue
- Basecamp
- Big cartel
- Box
- Business Insider
- CNN
- Cleveland.com
- Etsy
- Github
- Grubhub
- Guardian.co.uk
- HBO Now
- Iheart.com (iHeartRadio)
- Imgur
- Intercom
- Intercom.com
- Okta
- PayPal
- People.com
- Pinterest
- Playstation Network
- Recode
- Reddit
- Seamless
- Spotify
- Squarespace Customer Sites
- Starbucks rewards/gift cards
- Storify.com
- The Verge
- Twillo
- Twitter
- Urbandictionary.com
- Weebly
- Wired.com
- Wix Customer Sites
- Yammer
- Yelp
- Zendesk.com
- Zoho CRM
- Credit Karma
- Eventbrite
- Netflix
- NHL.com
- Fox News
- Disqus
- Shopify
- Soundcloud
- Atom.io
- Ancersty.com
- Constant Contact
- Indeed.com
- New York Times
- Weather.com
- WSJ.com
- time.com
- xbox.com
- dailynews.com
- Wikia
- donorschoose.org
- Wufoo.com
- Genonebiology.com
- BBC
- Elder Scrolls Online
- Eve Online
- PagerDuty
- Kayak
- youneedabudget.com
- Speed Test
- Freshbooks
- Braintree
- Blue Host
- Qualtrics
- SBNation
- Salsify.com
- Zillow.com
- nimbleschedule.com
- Vox.com
- Livestream.com
- IndieGoGo
- Fortune
- CNBC.com
- FT.com
- Survey Monkey
- Paragon Game
- Runescape
- Amazon

Cyber attacks from infrastructure perspective

	INTERNET PIPE (Saturation)	FIREWALL	IPS/IDS	LOAD BALANCER (ADC)	THE SERVER UNDER ATTACK	SQL SERVER
2016	36%	21%	10%	3%	28%	2%
2015	36%	13%	8%	9%	33%	1%



Complexity of attacks continues to grow



Cloud DDoS protection | DoS protection | Behavioral analysis | IPS | WAF | SSL protection

Multi-technology protection






Only a **multi-technology** solution can provide full protection from **multi-vector** threats

 Cloud DDoS protection |  DoS protection |  Behavioral analysis |  IPS |  WAF |  SSL protection

radware

Thank You!