ACM NetSec

Cybersecurity Made Simple

Personal Security: Availability

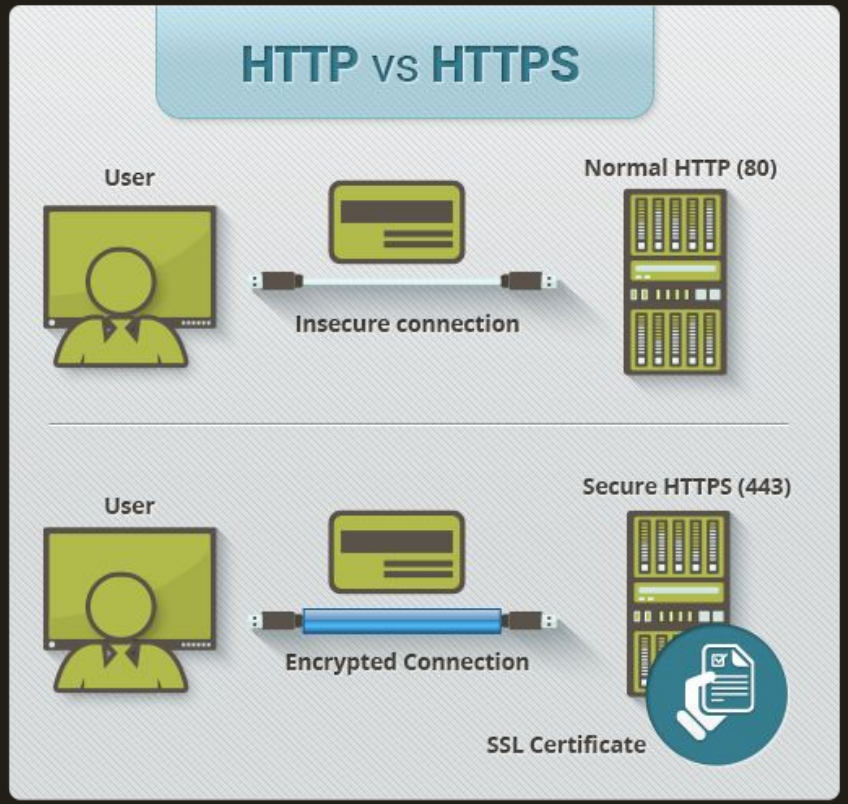
Agenda

- Recap
- Follow Up: Equifax
- Malware
- DDoS
- IOT
- Addressing Availability Issues

Recap

- Anyone still using TFA for MyUCLA?
- Anyone install a password manager?
- HTTP/HTTPS

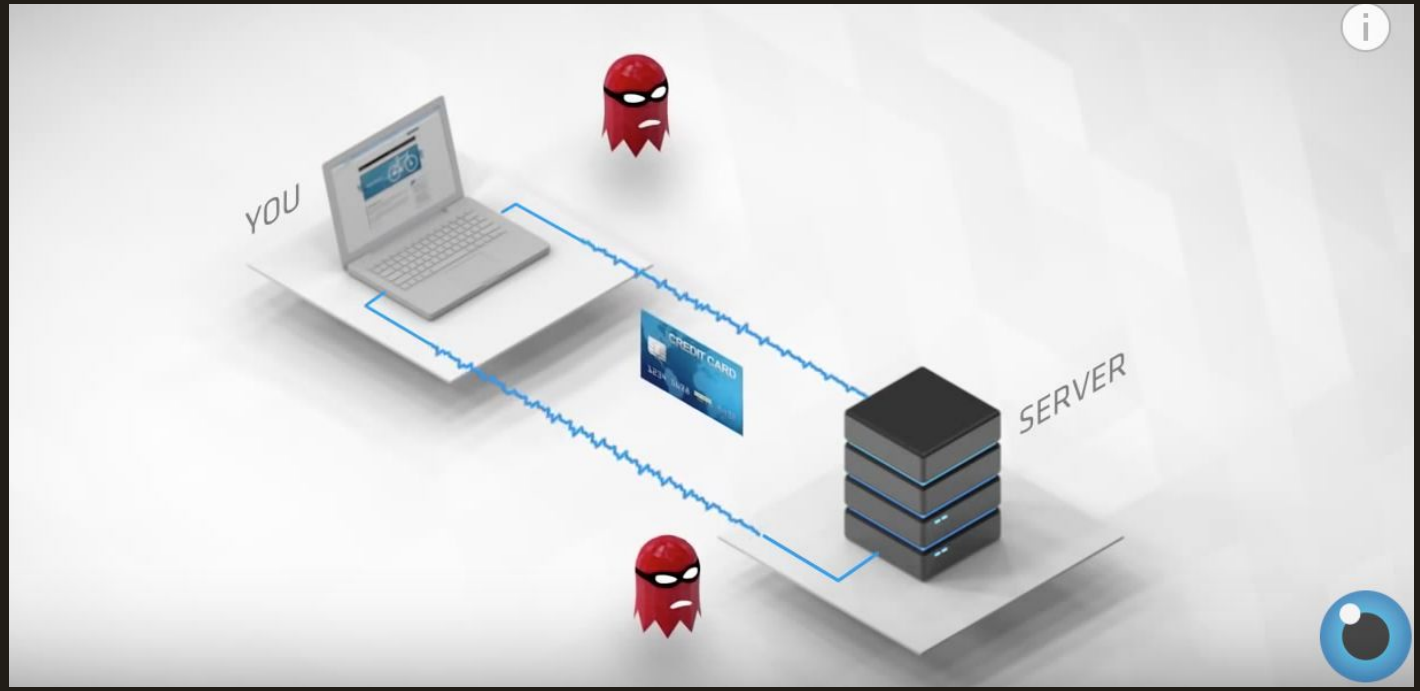
HTTP vs. HTTPS



HTTPS


COMODO
SSL Certificate from Comc
Comodo CA Ltd [GB] https://www.instantssl.com
SSL Certificate from Comc
Comodo CA Ltd [GB] https://www.instantssl.com
SSL Certificate from Como...
Comodo CA Ltd [GB] https://www.instantssl.com
Search
https://www.instantssl.com/
Comodo CA Ltd [GB]
SSL Certificate from Como...
SSL Certificate from Comodo | Secure Socket Layer and More
https://www.instantssl.com/ Comodo CA Ltd
Google
Opera
SSL Certificate from Co...
Trusted www.instantssl.com
Search with Google

Aside: SSL Certificates



https://youtu.be/dsuVPxuU_hc

Agenda

- Recap
- Follow Up: Equifax
- Malware
- DDoS
- IOT
- Addressing Availability Issues

[case] Equifax

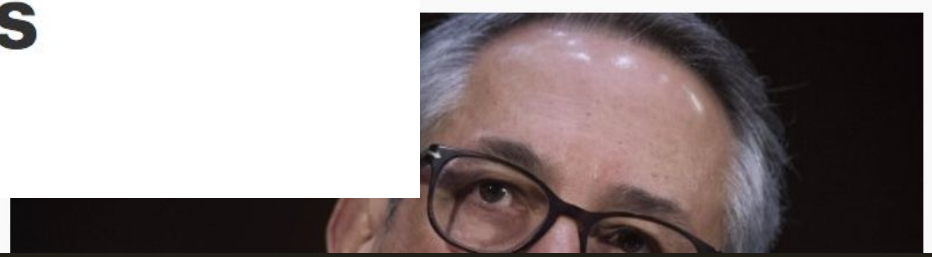
- Slow to detect and notify consumers
- Difficult-to-find link for checking if affected
- URL Spoof
- Name and SSN are not things you can **change,** passwords can be changed

[case] Equifax

Equifax CEO to Congress: Not Sure We Are Encrypting Data

Two months after Equifax reported one of the worst data breaches in history, its interim chief executive told a congressional hearing Wednesday he wasn't

ny was encrypting consumer



Following Equifax breach, CEO doesn't know if data is encrypted

http://searchsecurity.techtarget.com/news/450429891/Following-Equifax-breach-CEO-doesnt-know-if-data-is-encrypted

Cryptography

Constructing and analyzing protocols that prevent third parties or the public from reading private messages


```
-----BEGIN PGP MESSAGE-----
Version: GnuPG v1.4.5 (FreeBSD)
Comment: This is what your message looks like after encryption.

hQEOA1e+1x6YuUMCEAP/VJyavkOX0KRMdVJUS7TW7P/QWXe27a4T55oLsR6n4S/a
9nU/gLa7ZEeZDD8KCf975dCrf1y8fZzryrSwOxhZfWYYjJWYg/XE1JrrPPMfL/BU
OzmJrve3XNu+ECG4oWOqDcP+5kuI9LLTDMM3VX+Id61833UpBYUObGmIyCWXnBMD
/1f335KFdh0BvkXumG4Mp3NnXvVaOUNL7TMCUMKKNcTQhV4iXZmiW+aQqkGijWtX
ydzg39lr2/5pAlbJsVsMFHsZU01qe12n0tfl0mvcApOvQbr/Tpm2WES2jIc7ZFOv
1ShbEO5GkSiBude0W7K1t62sWQyQNj2nZ7wyzSyvOQDj0lgBxGAiolg1bkpzPx+W
z95B1lB25obPJsII9qSXl+V/NPgHuOI5WR5ASYabU22alEkGEU0ydmpJpYYlsCPA
esQ7EX+i1F8mB8FSMsGbfiQY3oRuOrOdW9O6
=FpRv
-----END PGP MESSAGE-----
```

Misconception

- Encryption is the **LAST** line of cyber defense, not the first
- It is only useful for keeping data secret once access has already been gained
  - E.g. Hashing Passwords
- Encryption assumes that attacks will happen

Agenda

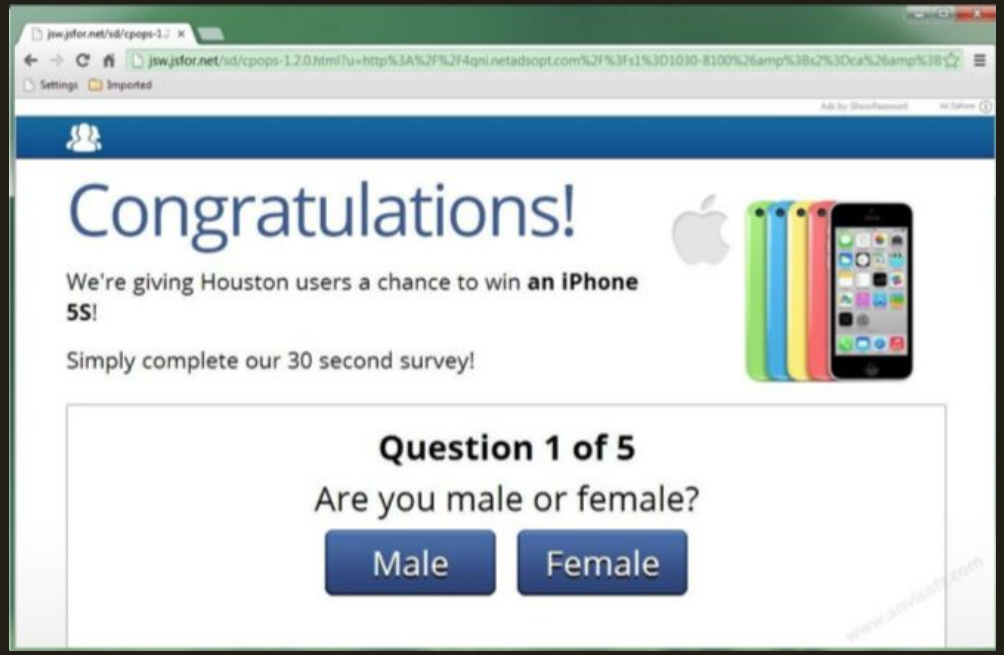
- Recap
- Follow Up: Equifax
- Malware
- DDoS
- IOT
- Addressing Availability Issues

Malware

Malware is short for malicious software, meaning software that can be used to compromise CIA principles of a system

Adware

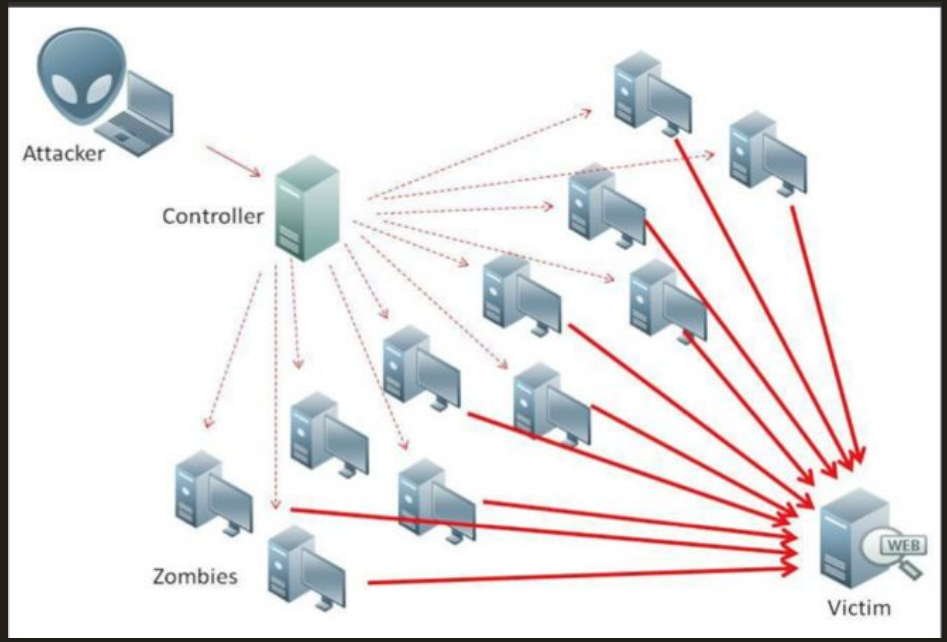
Adware (short for advertising-supported software) is a type of malware that automatically delivers advertisements.



http://symc.ly/2pkTubZ

Bot

Bots are software programs created to automatically perform specific operations.



http://symc.ly/2pkOp3q

Ransomware

Ransomware is a form of malware that holds a computer captive while demanding a ransom.

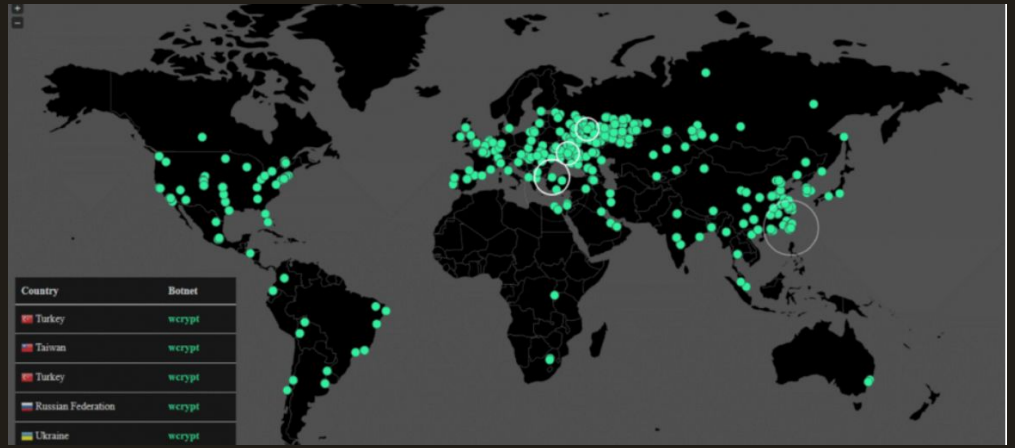
http://symc.ly/2oMbU4t

Zero-Day Vulnerability

A zero-day vulnerability is one that is unknown to those who would be interested in mitigating the vulnerability. Until the vulnerability is mitigated, attackers can exploit it

[case] WannaCrypt

- File sharing vulnerability in Windows
- Microsoft issued a patch, however legacy systems were not patched
- NSA developed the attack vector, Eternal Blue (Zero-Day Vulnerability)



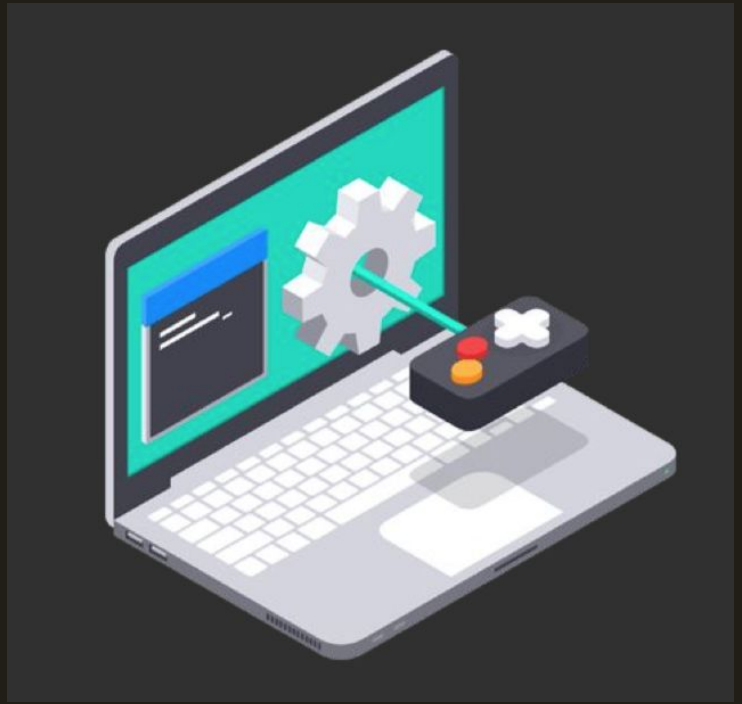
[case] WannaCrypt

- British National Health Service one of largest entities affected
- 90% of NHS hospitals were still running Windows XP
- Patient records, appointment schedules, internal phone lines and emails were rendered inaccessible

https://www.nbcnews.com/news/world/why-wannacry-malware-caused-chaos-national-health-service-u-k-n760126

Rootkit

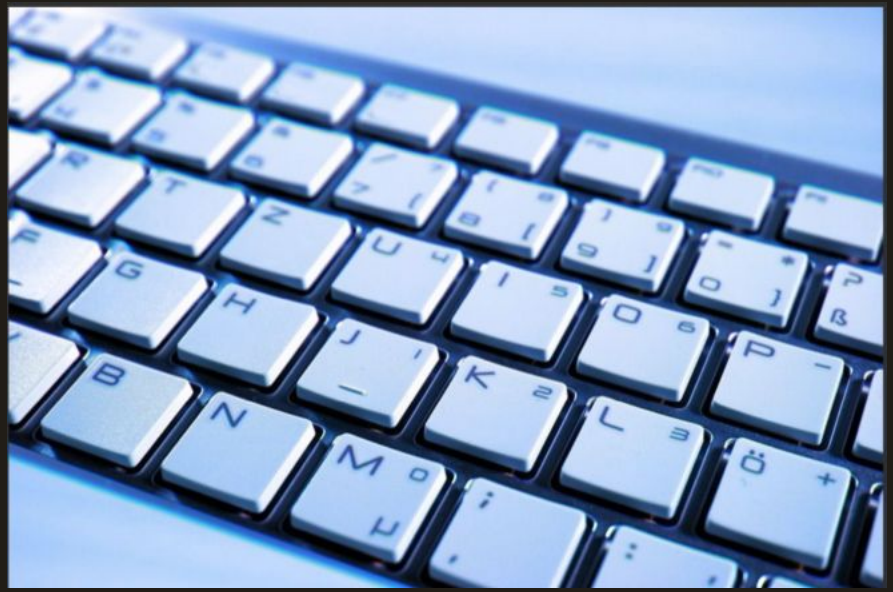
A rootkit is a type of malicious software designed to remotely access or control a computer without being detected by users or security programs



https://www.avast.com/c-rootkit

Spyware

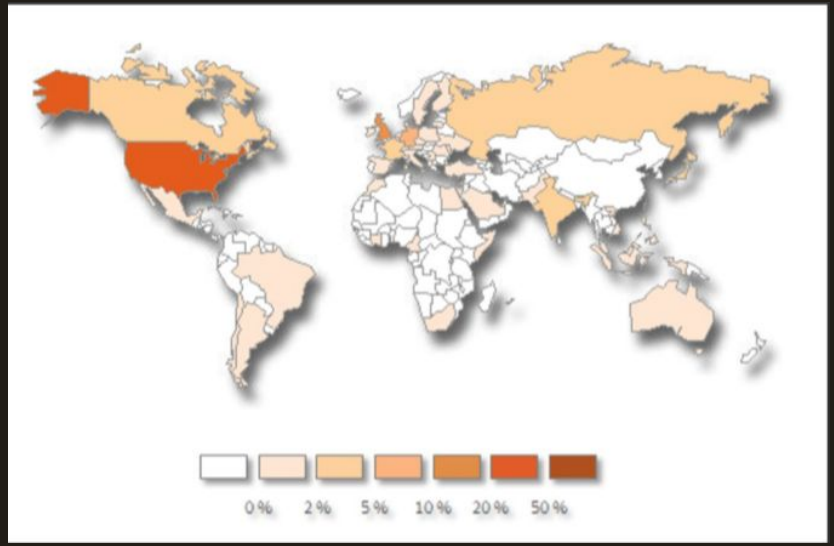
Spyware is a type of malware that functions by spying on user activity without their knowledge. These spying capabilities can include activity monitoring, collecting keystrokes, data harvesting.



http://bit.ly/2mZDefB

Trojan Horse

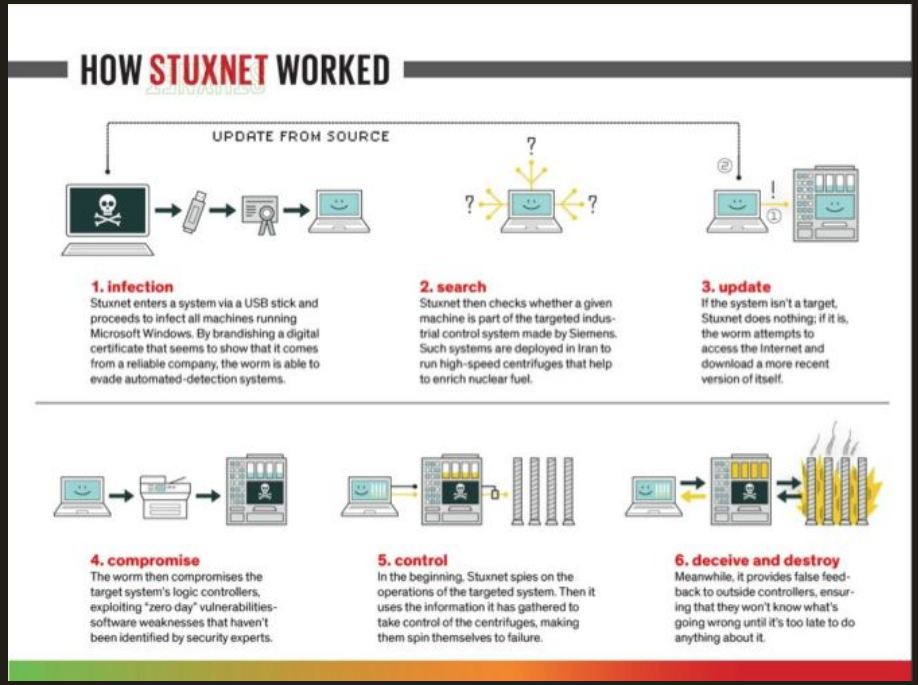
A Trojan horse, commonly known as a “Trojan,” is a type of malware that disguises itself as a normal file or program to trick users into downloading and installing malware.



http://symc.ly/2joUzZG

Virus

A virus is a form of malware that is capable of copying itself and spreading to other computers.



http://symc.ly/2pkOp3q

Worm

Worms spread over computer networks by exploiting operating system vulnerabilities. Worms typically cause harm to their host networks by consuming bandwidth and overloading web servers.

http://bit.ly/2p6Mz6h

Agenda

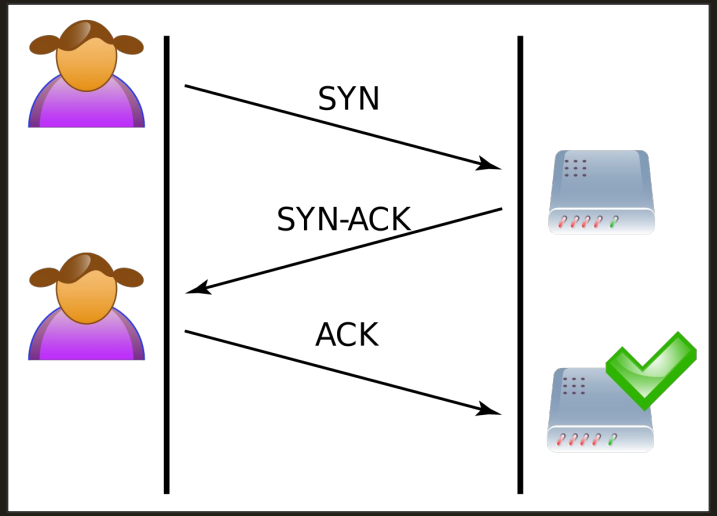
- Recap
- Follow Up: Equifax
- Malware
- DoS
- IOT
- Addressing Availability Issues

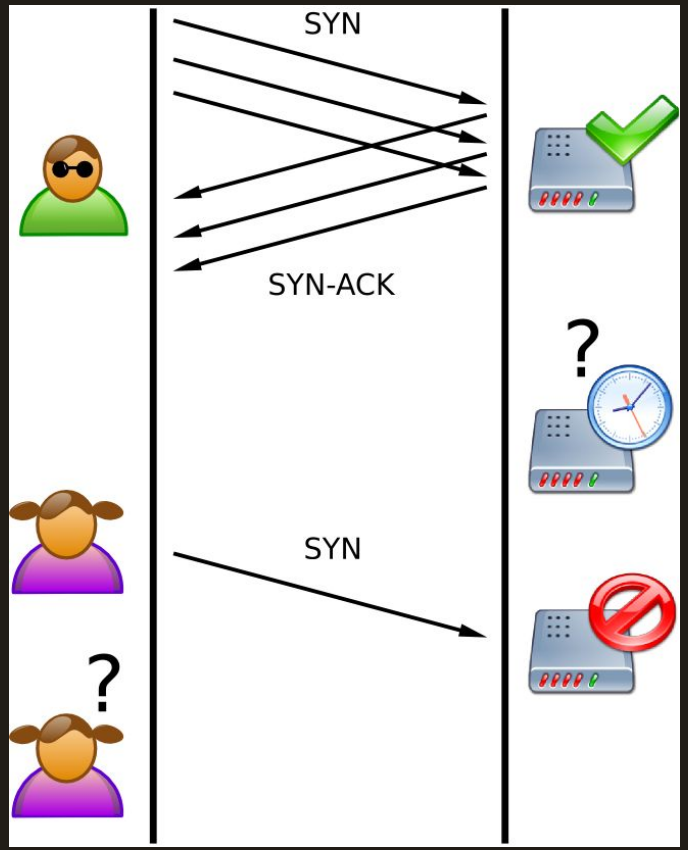
Denial Of Service

- disrupting access to a machine or other network resource
  - core of availability violation
-

Denial Of Service

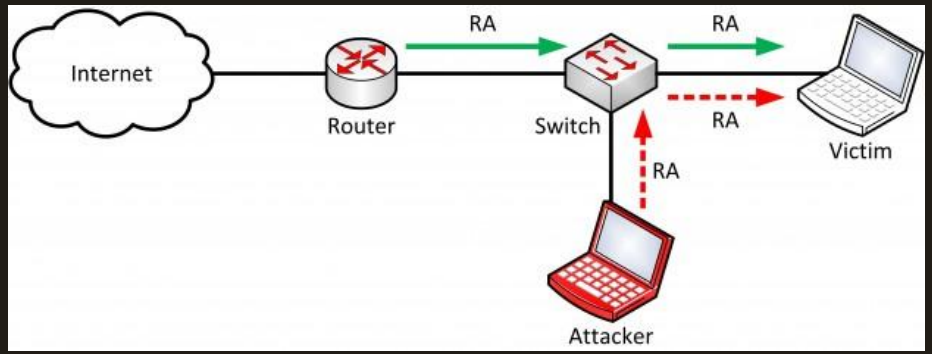
- SYN flood
  - Attack on servers
  - Overloads network capabilities

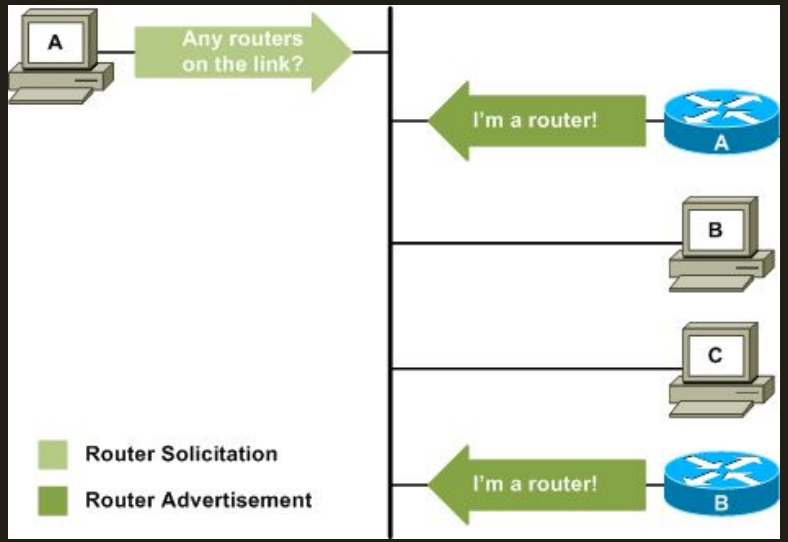




Denial Of Service

- IPv6 request flood
  - Attack on clients!
  - Overloads network capabilities





Denial of Service Defense

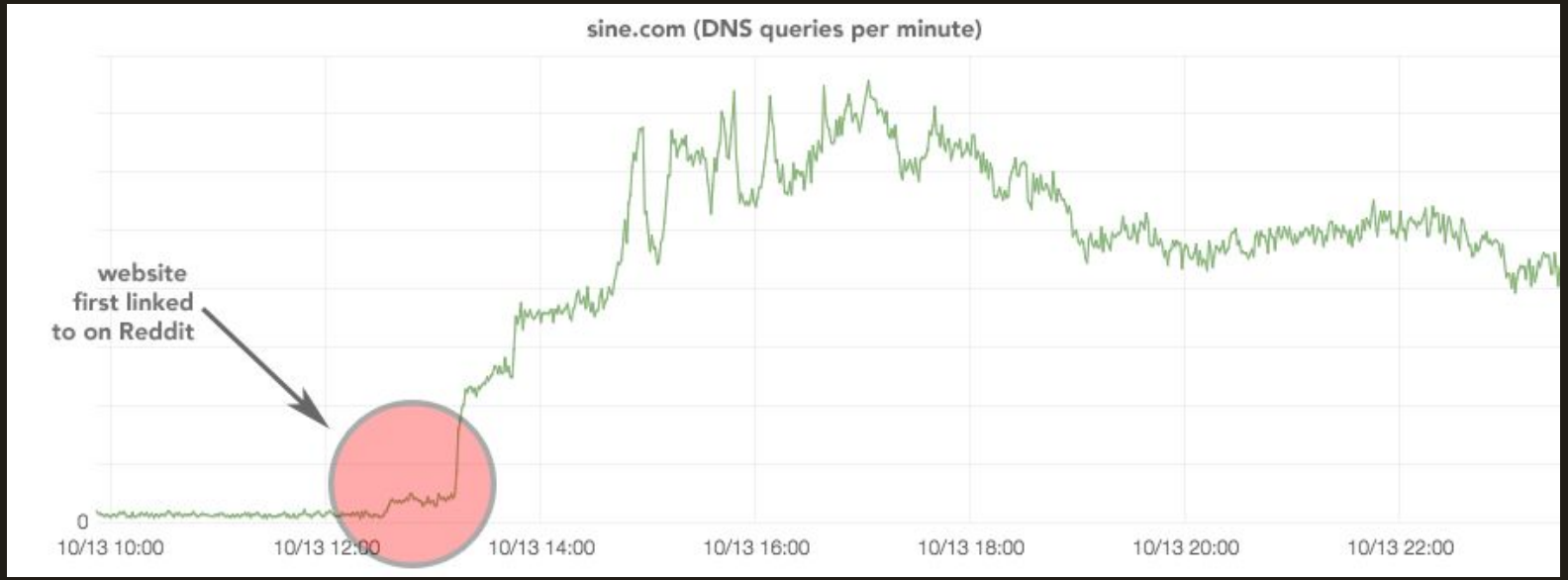
- SYN cookie
  - Don’t actually process SYN requests
- RA stack
  - Store RA advertisements in a stack, don’t process more than stack size
- In general
  - Exploit asymmetry in processing power or capabilities
  - Flawed assumptions about network safety
  - Noticing and fixing them is tricky, but can be done
  - Patch patch patch!

Denial of Service Without Vulnerabilities?

- Assume there are no major software vulnerabilities
  - Not realistic, but it takes time and effort to discover them

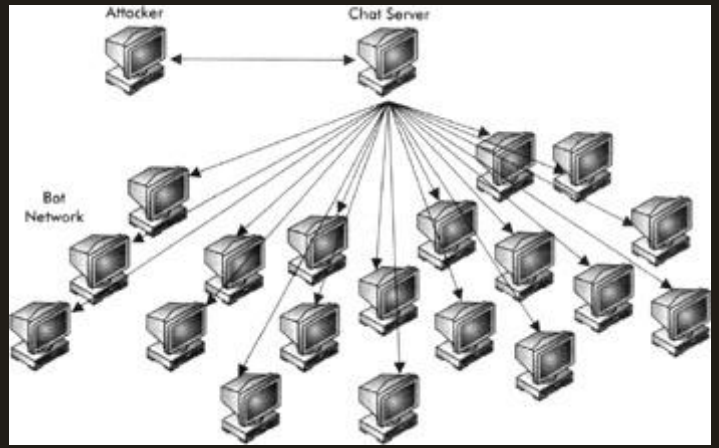
Distributed Denial of Service

- Reddit hug of death

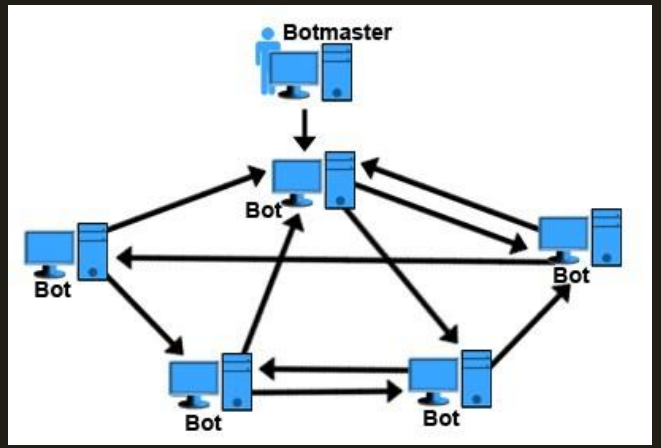


DDoS Botnets

- Hijack computers to perform a hug of death
- Many use a command and control server
  - Directs zombie computers



- Some create a P2P network
  - More resilient



DDoS Defense

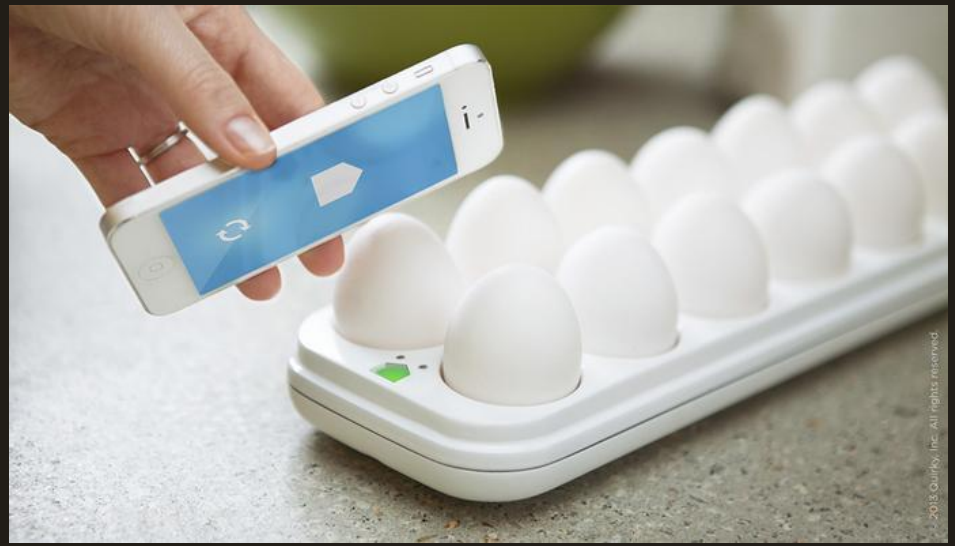
- Not many options
  - Throw more processing power
  - Cloudflare DDoS protection
- Users can help mitigate attacks
  - Botnets distributed via social engineering and common exploits
  - Use good security practices
  - Patch and update devices
- However, there is a new issue...

Agenda

- Recap
- Follow Up: Equifax
- Malware
- DDoS
- IOT
- Addressing Availability Issues

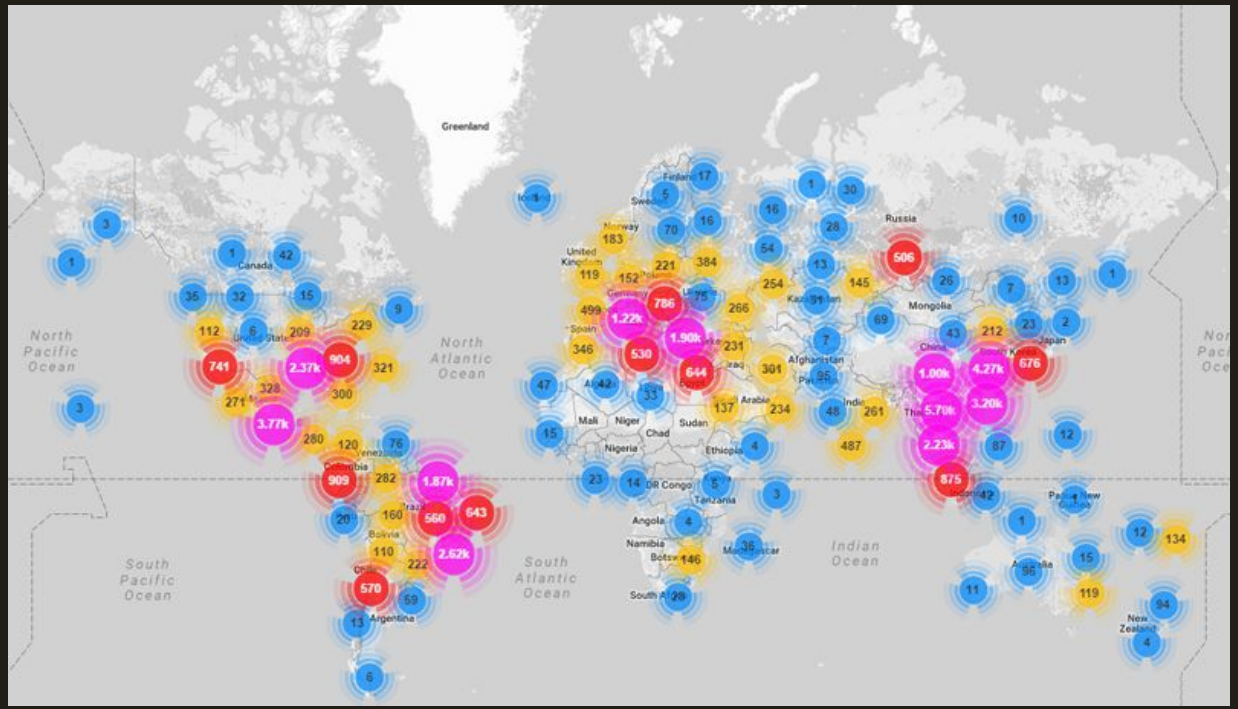
What is the Internet of Things?

- Internet-Enabled “things”
  - Fridges
  - Cars
  - Thermostats
  - Egg Tray



Mirai Botnet

- One of the largest IoT botnets



Mirai Botnet

- Targets
  - IP cameras
  - Routers
  - ~60 device types total
- Command and control server
- Impact
  - Krebs on Security
  - French web host OVH
  - DynDNS
    - DNS disruption prevents many sites from being reachable

IoT Botnet Problem

- The normal defenses fail
- Not infected through human error
- Often can’t be patched
  - Side note: this means IoT is more vulnerable to all other attacks.

- How to defend the IoT?
  - Firewalls?
  - More security programmers?

Agenda

- Recap
- Follow Up: Equifax
- Malware
- DDoS
- IOT
- Addressing Availability Issues

Update Often

- Patches to security issues are distributed through updates
  - E.g. EternalBlue
- Updates fix other annoying issues

Backup Data

External Hard Drive

Cloud Storage

OneDrive

box

CARBONITE

“Award Winning” Anti-Virus Software

https://www.av-test.org/en/award/2016/

Free Antivirus Software

UCLA Sophos

https://www.it.ucla.edu/bol/software-downloads/sophos-antivirus