

Ransomware, Denial of Service, and Other Attacks

Rajendra V. Boppana
Systems and Networks (SYN) Lab
Computer Science Department
UT San Antonio

1



Ransomware

Ransomware is a type of malicious software that blocks access to data (and systems)

The attacker demands a ransom to restore access or sells data on the dark web

2

Famous and Recent Ransomware Attacks

- Wannacry (2017)
 - Unpatched Windows vulnerability
 - \$4B damages
- Colonial pipeline (2021)
 - Shutdown pipeline supplying 45% of East Coast fuel
- British Library (2023)
 - Down for months
 - Double extortion
- REvil (2019)
 - Ransomware as a service

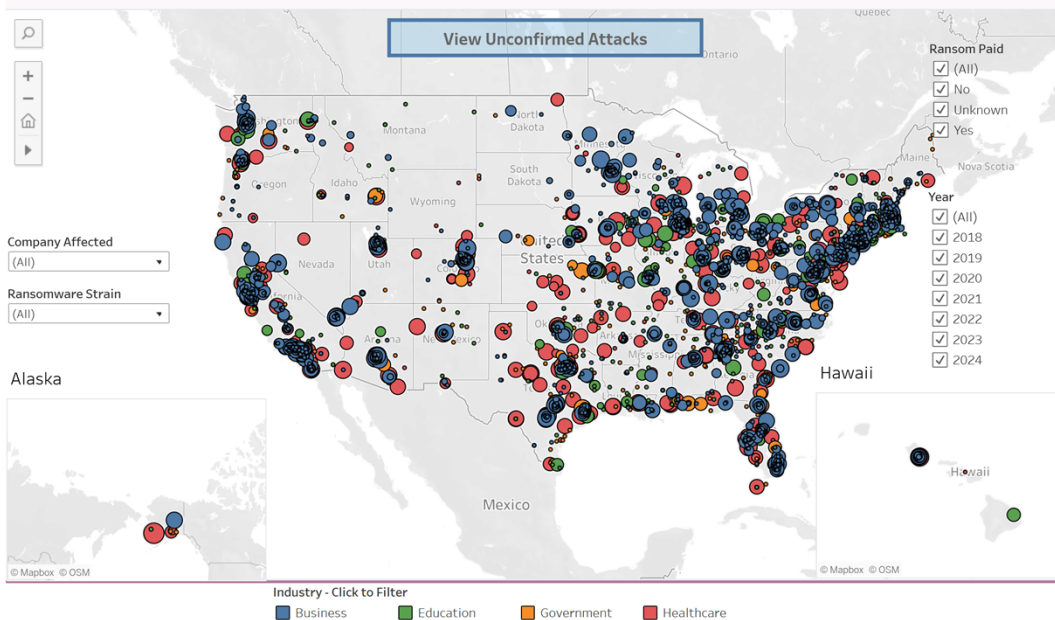
By 2031:

- ransomware attacks may occur every 2 seconds, targeting businesses, critical infrastructure, and consumers
- cost of damage > \$265 billion
- UC, San Francisco (2020)
- Judson school district (2021)
- City of Dallas (2023)
- Sony (2023)
- Las Vegas MGM (2023)
- Hospitals (2023) -- > 299

City governments in Michigan, New York face shutdowns after ransomware attacks

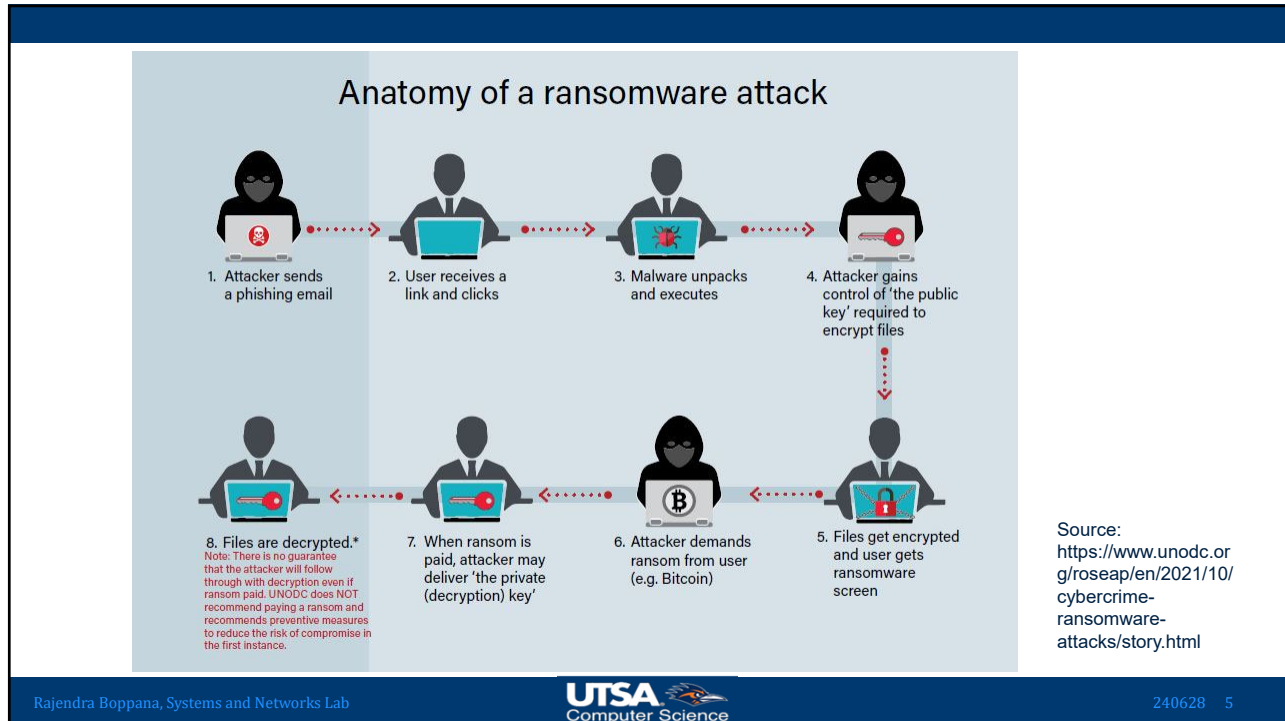
3

Map of confirmed US ransomware attacks from 2018 to present



Source: <https://www.compartech.com/ransomware-attack-map/>

4



5

Distributed Denial of Service (DDoS) Attacks

A flood of bogus requests overwhelm a computer or network and make it unresponsive

Brute force (high volume), exploit network design (low volume)

SYN flood, Slowloris, Goldeneye, ...

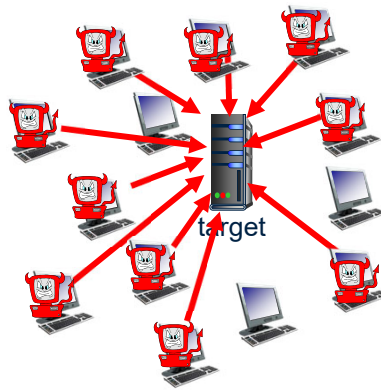
UTSA
Computer Science

240628 6

6

Distributed Denial of Service (DDoS) Attacks

- Compromise and control computers, IoT devices, ... (bots)
- Overwhelm the target with bogus traffic from networks of bots



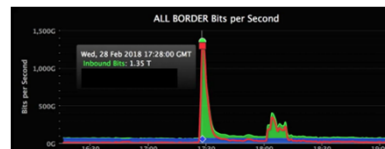
Rajendra Boppana, Systems and Networks Lab

240628 7

7

Famous and Recent DDoS Attacks

- HTTP/2 rapid-reset (2023)
 - Google, AWS, Cloudflare, ...
 - Google attack (2020)
 - 2.5 Tbps traffic (peak) directed at Google for six months
 - AWS DDoS attack (2020)
 - 3 days, 2.3Tbps traffic rate
 - Mirai Dyn DDoS attack (2016)
 - GitHub, HBO, Twitter, Reddit, PayPal, Netflix, and Airbnb were inaccessible
 - \$300k-\$1M/hour in lost productivity
 - GitHub attack (2018)



Source: Wired


Rajendra Boppana, Systems and Networks Lab

240628 8

8

Common Cyberattacks


Malware
Phishing
Man-in-the-Middle

Rajendra Boppana, Systems and Networks Lab  240628 9

9

NSF CyberCorps® Scholarship for Service (SFS)

Faculty: Raj Boppana, Greg White, and Phil Menard

Rajendra Boppana, Systems and Networks Lab  240628 10

10

SFS Program Benefits



Tuition & Fees

Covered for 2-3 years



Stipends

\$27K-37K/year



Supplies

Books, laptops, and other course materials



Networking

SFS Job Fair and conference travel for networking opportunities

+ Professional development and certification opportunities (Security+, CCNA, ...)

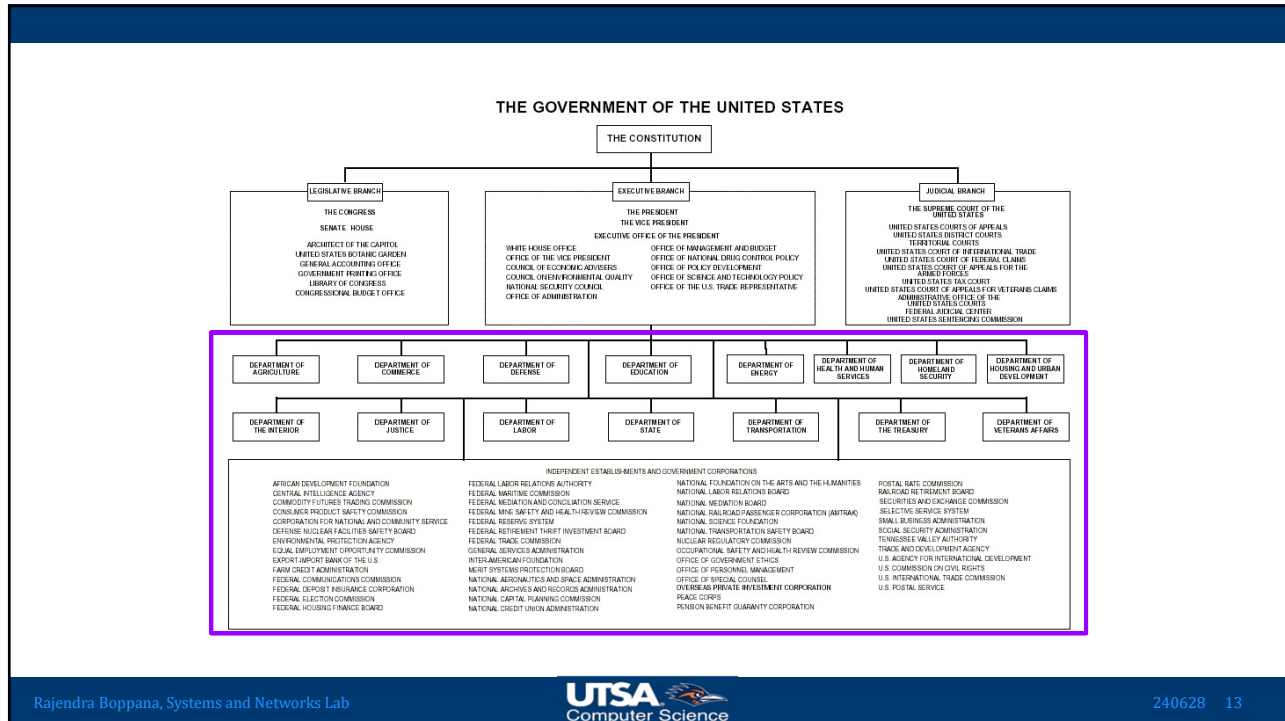
UTSA

11

Important Points

- Must be a full-time student
 - Working while in the SFS program is discouraged
- Work for an executive branch of Fed Gov
 - Intern during summers at an executive branch of the government
- Must be able to obtain “Top Secret” security clearance
- SFS program is flexible 😊

12



13

Striving for Representation

SINCE 2021, UTSA'S SFS PROGRAM HAS RECRUITED APPLICANTS, RESULTING IN...

41%

Female
SFS Scholars

Outpacing national cybersecurity workforce by 16 percentage points¹

43%

URM
SFS Scholars

Outpacing national cybersecurity workforce by 17 percentage points²

URM: underrepresented minority

UTSA 1. <https://cybersecurityventures.com/wp-content/uploads/2022/09/Women-In-Cybersecurity-2022-Report-Final.pdf>
2. <https://www.isc2.org/-/media/Files/Research/Innovation-Through-Inclusion-Report.aspx>

14

NSF SFS Checklist

- Completed application form
- Two letters of recommendation
- College transcripts (unofficial, student versions are OK)
- Personal statement of career interests, goals, and plans
- Resume (up to 2 pages)

<https://sciences.utsa.edu/computer-science/scholarships/sfs.html>



15

Tips for Great Reference Letters

- Select faculty members you took courses with
- Provide them
 - Your resume with GPA, major courses completed, and grades for them
 - A statement of your career interests and your major accomplishments — course projects, certifications, etc.

16

Tips for Writing Personal Statements

- 3 or more paragraphs; 12-point font; ~ 500 words or 1 page
- 1: **establish your interest and suitability for the scholarship**
 - Clearly state you are applying for the scholarship
 - Indicate your interest in cybersecurity
 - Indicate your current academic progress in pursuing cybersecurity concentration/track/degree — GPA, and most relevant courses taken
 - 2: **Make a case for yourself (1 or more paragraphs)**
 - Why are you well qualified for the scholarship, indicate any academic honors/distinctions
 - Why are you interested in working for the government, indicate any relevant prior experience
 - Point out positives that are not obvious from your resume
 - Explain any issues that are obvious from your resume
 - 3: **Summarize and offer to discuss and provide more info**