Intro to Cybersecurity_

@UT.ISSS

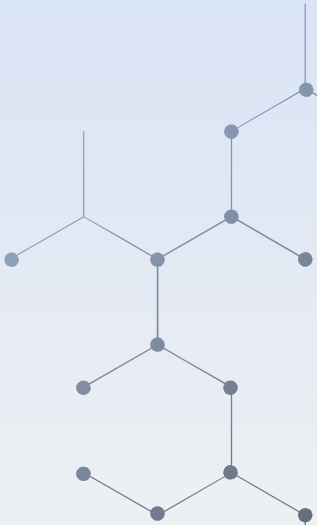
September 11, 2024 | The Information & Systems Security Society

INFORMATION AND SYSTEMS SECURITY SOCIETY

Cyber in the News_

INFORMATION AND SYSTEMS SECURITY SOCIETY

Table of contents_



INFORMATION AND SYSTEMS SECURITY SOCIETY

Upcoming Events_

September 12

5 - 6pm CT, WCP 2.210

Women in Cybersecurity (WiCyS) Fall Kickoff

September 13

11:59pm CT

Cyber Scholars Program Application closes at 11:59pm CT

September 18

5 - 7pm CT

Fundamentals Series: Talk I

September 19

6 - 8pm CT; TBD

Hash Association of Student Hackers Fall Kickoff

September 25

5 - 7pm CT

Fundamentals Series: Talk II

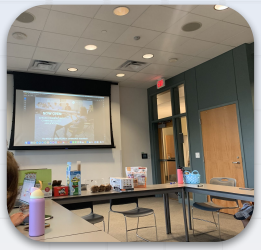
September 28

Tentative; TBD

[Exclusive] Cyber Scholars Program Social

ISSS
INFORMATION AND SYSTEMS SECURITY SOCIETY

Women in Cybersecurity (WiCys)



- **Recruit, retain and advance** women in cybersecurity to build a robust and diverse cybersecurity workforce
- **Fall Kickoff (5-6pm) WCP 2.210**

Accomplishments:

- Sent 2 members to 2024 International WiCyS Conference (at Nashville, TN)
- Volunteered at UT STEM Girl Day
- Collaboration with WiCS (Intro to Cybersecurity)
- Grew membership by 133%
- Member in Top 10 for WiCyS x Target Cyber Defense Challenge

INFORMATION AND SYSTEMS SECURITY SOCIETY

Hash Association for Student Hackers

Compete with UT at national cybersecurity competitions!

Everyone is welcome to join in-person, weekly in Dobbie and virtually in Discord.

- Distinct from ISSS, but we share missions
- You can compete at in-person events
- Join our Discord for meetings and signups!
- If you want to join the CPTC team, fill out the signup form TODAY (9/11)!

ISSS
INFORMATION AND SYSTEMS SECURITY SOCIETY

What to expect_

Phase I

September - October. Wednesdays, 5-7 pm CT

Fundamentals Series Talks (subject to change)

Networking, Cryptography, Web Exploitation, Reverse Engineering, Digital Forensics and Incident Response, and Open Source Intelligence

Phase II

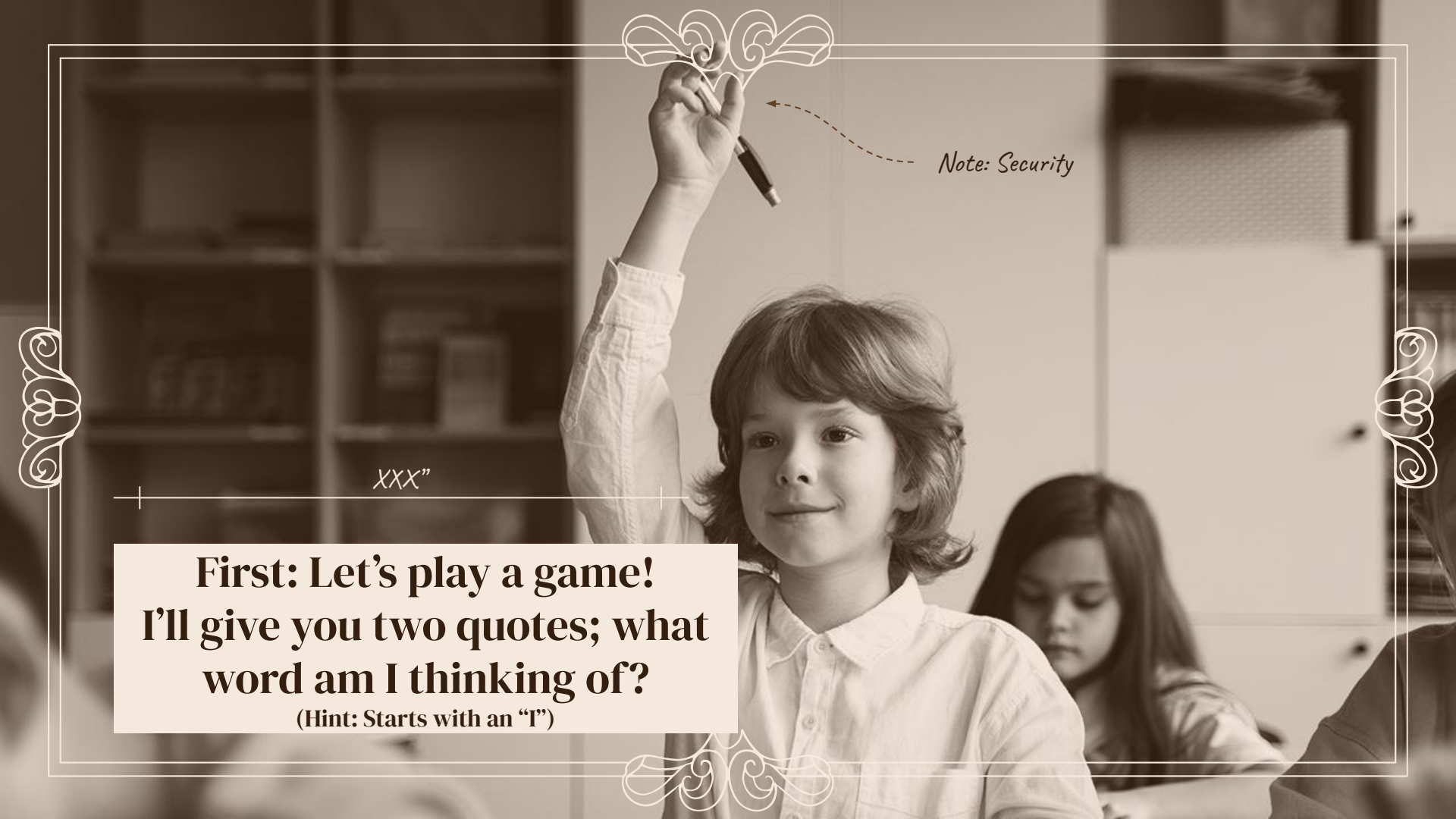
November - December. Wednesdays, 5 -7 pm CT

Specialty Series Talks

Free range talks covered by officers and guest speakers

Format: Lecture-Based (Learn) → Hands-On (Apply)

INFORMATION AND SYSTEMS SECURITY SOCIETY



First: Let’s play a game! I’ll give you two quotes; what word am I thinking of?

(Hint: Starts with an “I”)

"One who knows the enemy and knows himself will not be endangered in a hundred engagements."

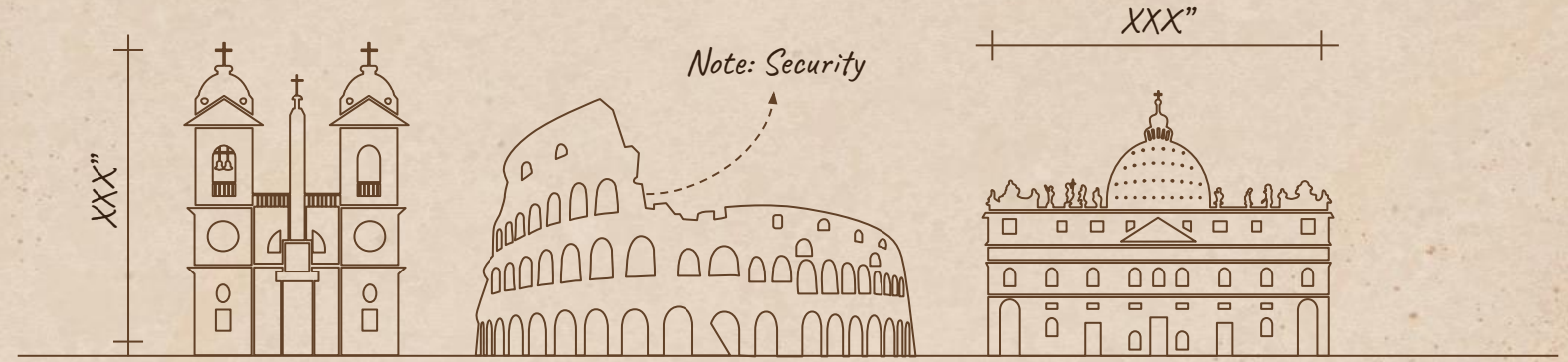
— SUN TZU

"I _ _ _ _ _ _ _ _ _ _ _ _."

"Knowledge is power."

— FRANCIS BACON (?)

INFORMATION!



The goal of this talk is to provide you context.

- **Security:** What exactly are we protecting? How are we protecting it?
- *Basic terminology:* industry lingo that you'll begin to hear often
- Concepts: information security, cybersecurity, national security
- *Note: we're going to try to be a little bit interactive c:*

03

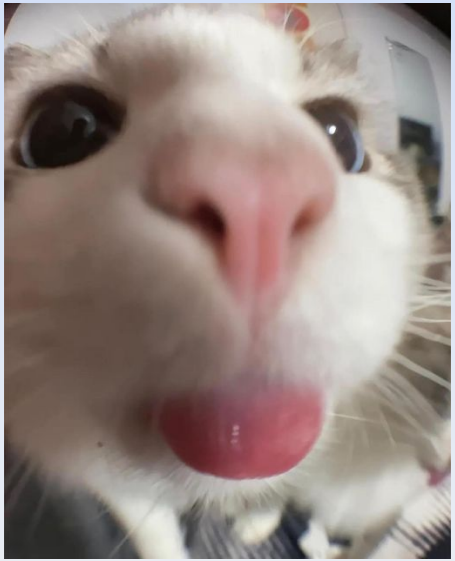
Security; A Background_

to answer this question…

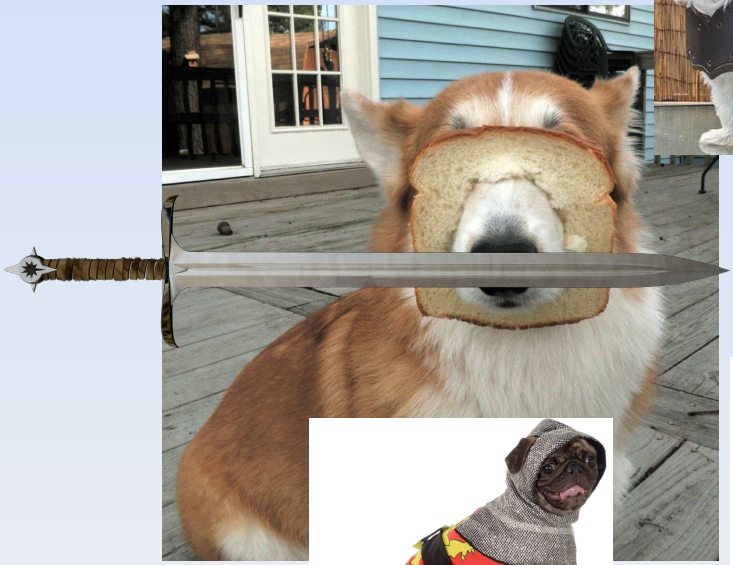
let’s go on a journey!


here’s where we’ll begin

A



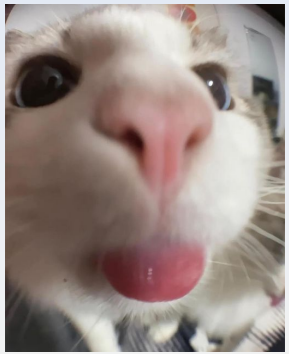
B

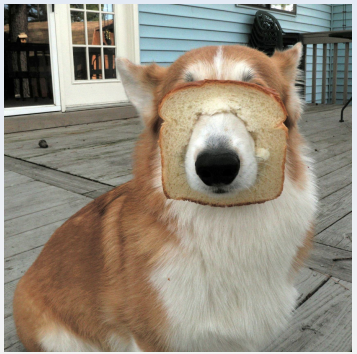


Intelligence

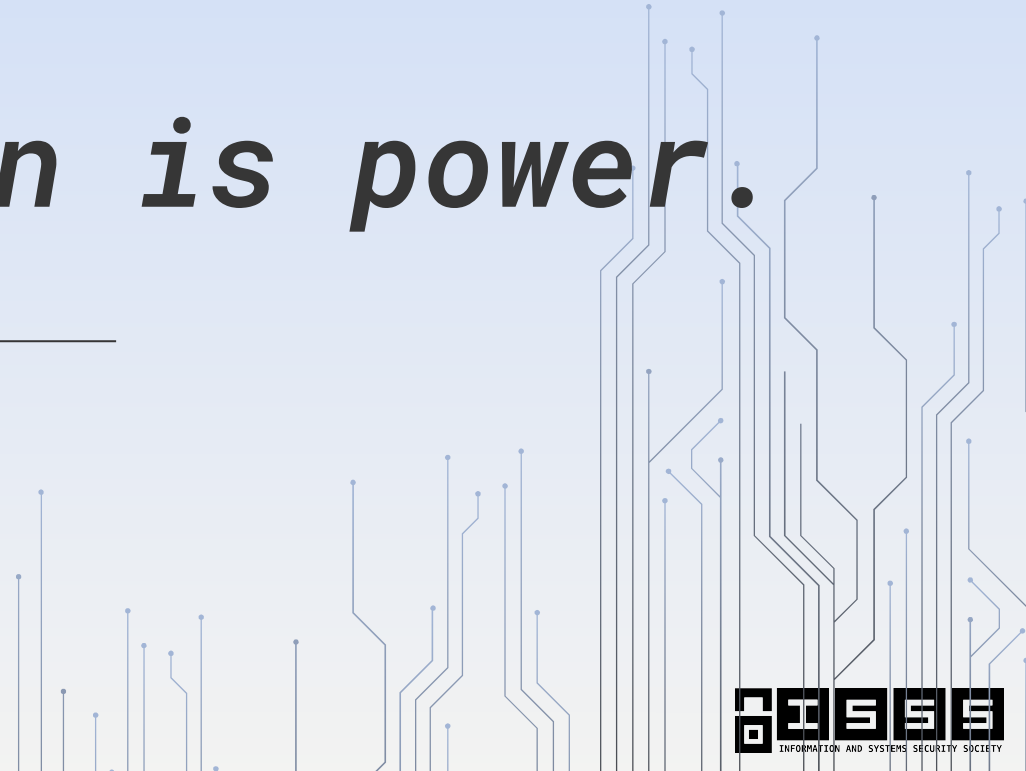
national security

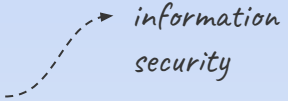
- Gathering **intelligence and spying** on one's enemy is essential to determine the political and military direction of the state, especially during times of conflict
- Governments needed the means to collect intelligence to **enable them to make informed decisions**





Information is power.





Information has been used since the first times of the history of humanity as **social and economic value**,

and it has always been **prevented from being disclosed** to the people who were not supposed to have it

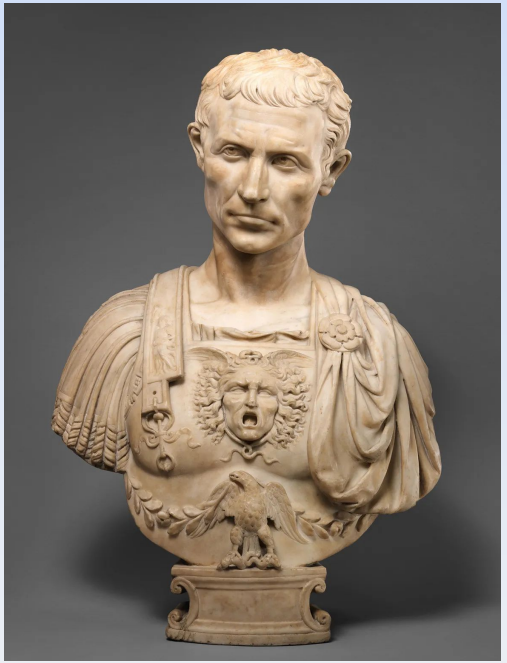
the discovery of writing provided the ability to store information and experiences and transfer it to others and use again

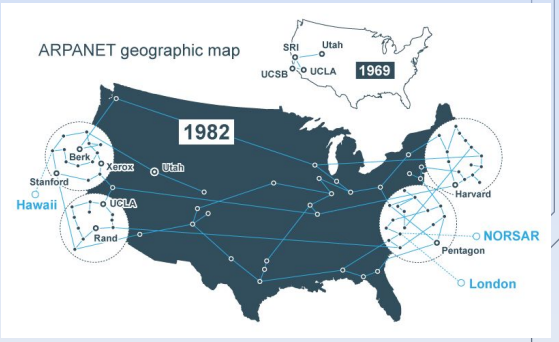
‘ancient humans achieved to keep the power of information within certain group or class in society, by creating “information monopoly”’

— Harnold Innis, Canadian historian

*“If he had anything **confidential** to say, he wrote it in cipher, that is, by so changing the order of the letters of the alphabet, that not a word could be made out. If anyone wishes to decipher these, and get at their meaning, he must **substitute the fourth letter of the alphabet**, namely D, for A, and so with the others."*

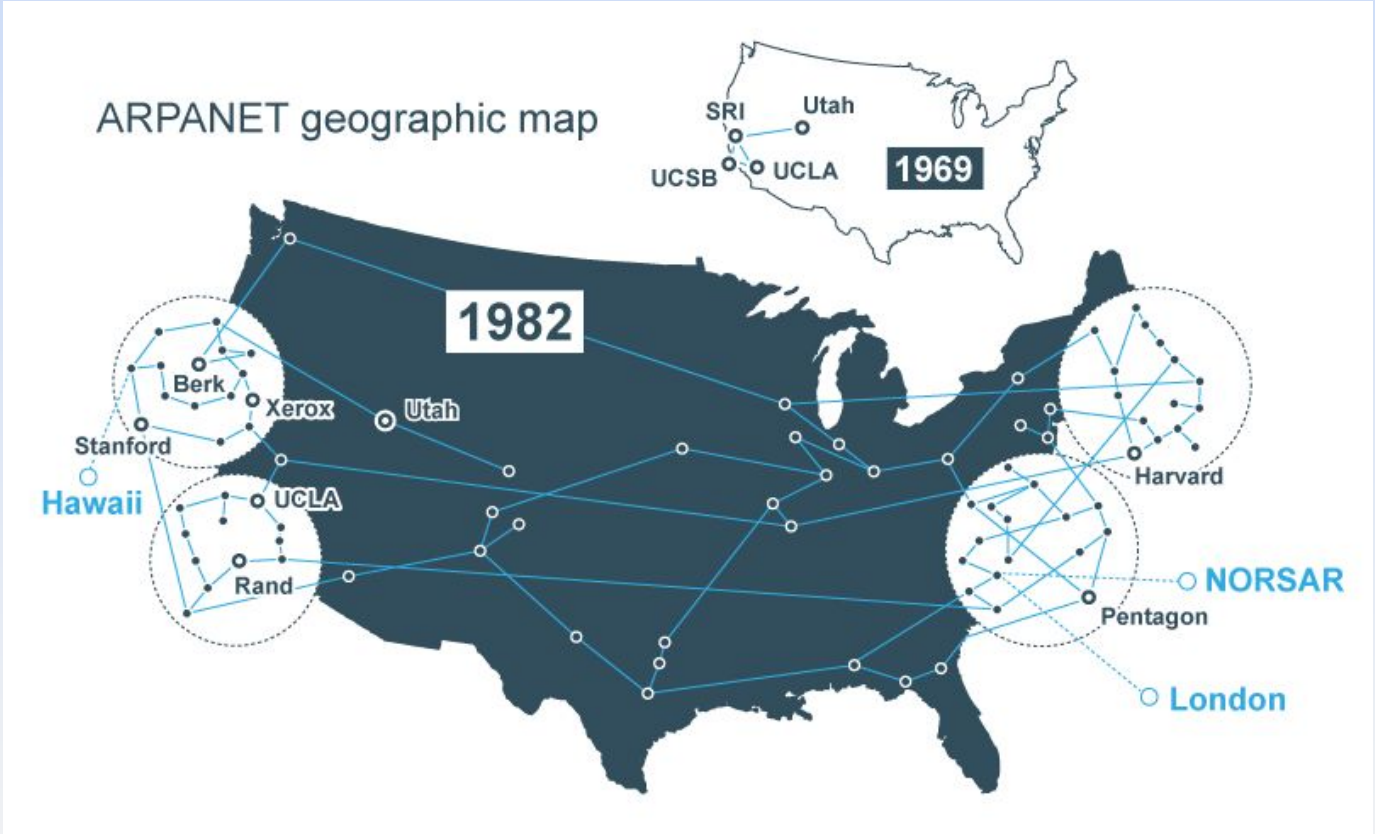
—Suetonius, Life of Julius Caesar 56

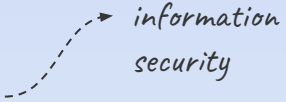



ARPANET geographic map
SRI
Utah
UCSB
UCLA
1969
1982
Berk
Xerox
Utah
Stanford
Hawaii
UCLA
Rand
Harvard
NORSAR
Pentagon
London

INFORMATION AND SYSTEMS SECURITY SOCIETY


IBM
IBM
IBM





Information has been used since the first times of the history of humanity as **social and economic value**,

and it has always been **prevented from being disclosed** to the people who were not supposed to have it

Break!

04

Security; Today_

What is hacking?

“Access, disrupt, manipulate, or damage a system in an unauthorized way”

Who and Why do people hack?

sophisticated, amateurs, state-sponsored, non-state organizations, individuals, criminals, spies, show-offs, for the lols, vendetta, competitive advantage, for the greater good, to cause harm

INFORMATION AND SYSTEMS SECURITY SOCIETY

“CIA” Triad

Culinary Institute of America

Integrity

Ensuring information is not altered or destroyed in an unauthorized way.

Confidentiality

Protecting sensitive information against unauthorized access.

Availability_

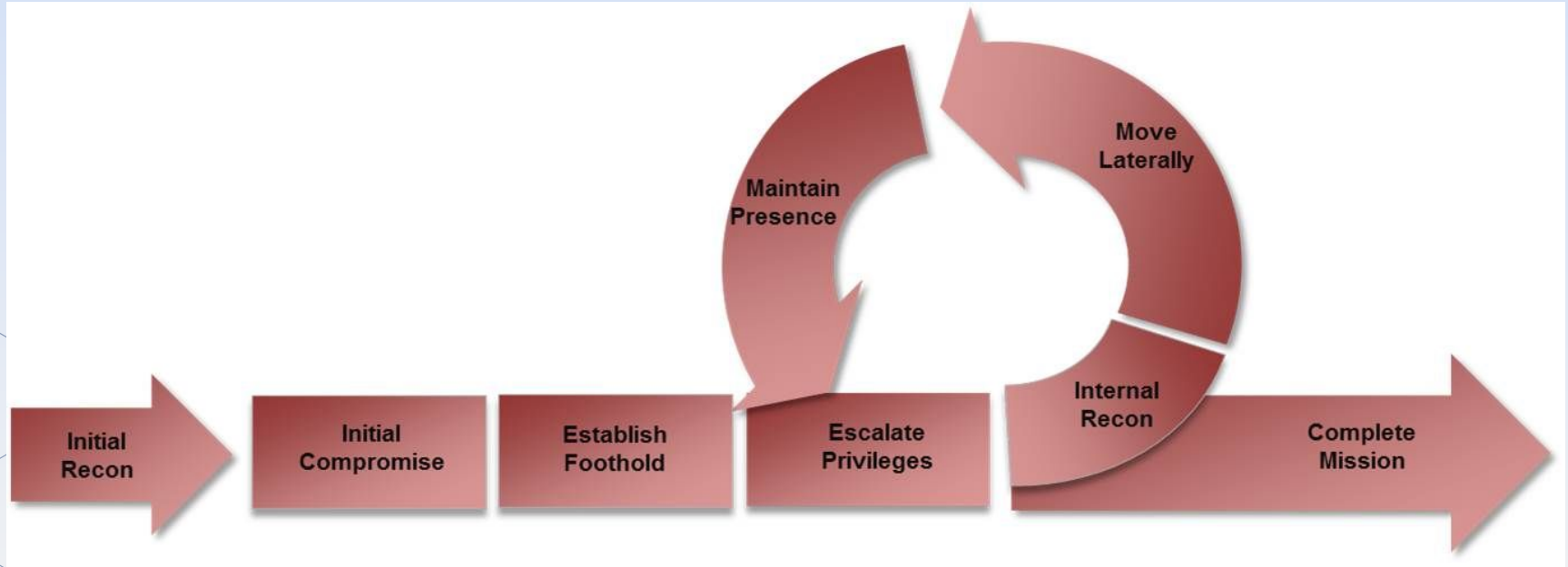
Ensuring information remains available for its intended use

Goal: (from defensive POV) prevent or minimize unauthorized, harmful actions

Vulnerabilities, Exploits, and Patches

Vulnerabilities: latent weaknesses

Cyber Attack Lifecycle



Case Study

solarwinds

SolarWinds Security Advisory RE: CERT Emergency Directive

Recent as of January 4, 2021, 6:00pm CST

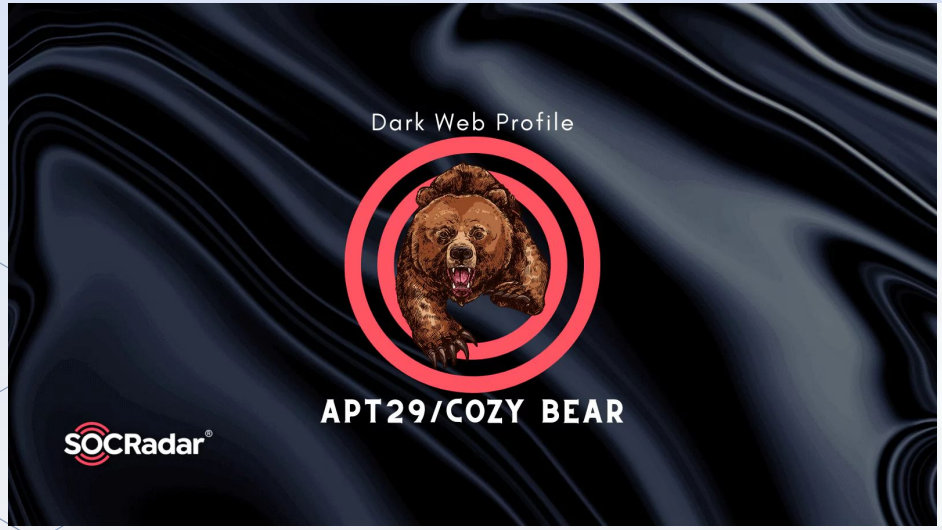
SolarWinds was the victim of a cyberattack to our systems that inserted a vulnerability (SUNBURST) within our SolarWinds® Orion® Platform. We believe that this attack impacts Orion Platform build versions **2019.4 HF 5, 2020.2 with no hotfix installed**, and **2020.2 HF 1** as referenced in **Cybersecurity and Infrastructure Security Agency (CISA) Computer Emergency Readiness Team (CERT) Emergency Directive 21-01** issued December 13, 2020, and updated December 18, and December 30, 2020.

CERT issued **Alert (AA20-352A)**, titled **Advanced Persistent Threat Compromise of Government Agencies, Critical Infrastructure, and Private Sector Organizations**, as an update to ED 21-01 on December 17, 2020, based on our coordination with the agency, and

Solarwinds

- Network management
- **ORION:** network monitoring software package
- *Why and who would this information be of interest to?*

Russia’s Foreign Intelligence Service (SVR)



Step 1: Accessing the SolarWinds “build environment”

- Need to compromise update system possibly by:

spear phishing, password spraying, vuln or config errors

Step 2: Inject malware (SUNSPOT) into Orion update

if Visual Studio Code:

if particular Orion build:

Monitor when Visual Studio is used to access Orion source code → inject file → `SolarWinds.Orion.Core.BusinessLayer.dll`

- .dll: malware package called SUNBURST (backdoor)
- victims included: Dept of Treasury, State, Commerce, Energy, and Homeland

Step 3: Deciding where to inject SUNBURST

- No action for 2 weeks

if security products in system:

disable or shutdown product

communicate with C2 server (masqueraded as “Orion Improvement Program”, legit traffic flow)

Step 4: Injecting tools

TEARDROP (*dropper*) *:* programs that have hidden malware payloads

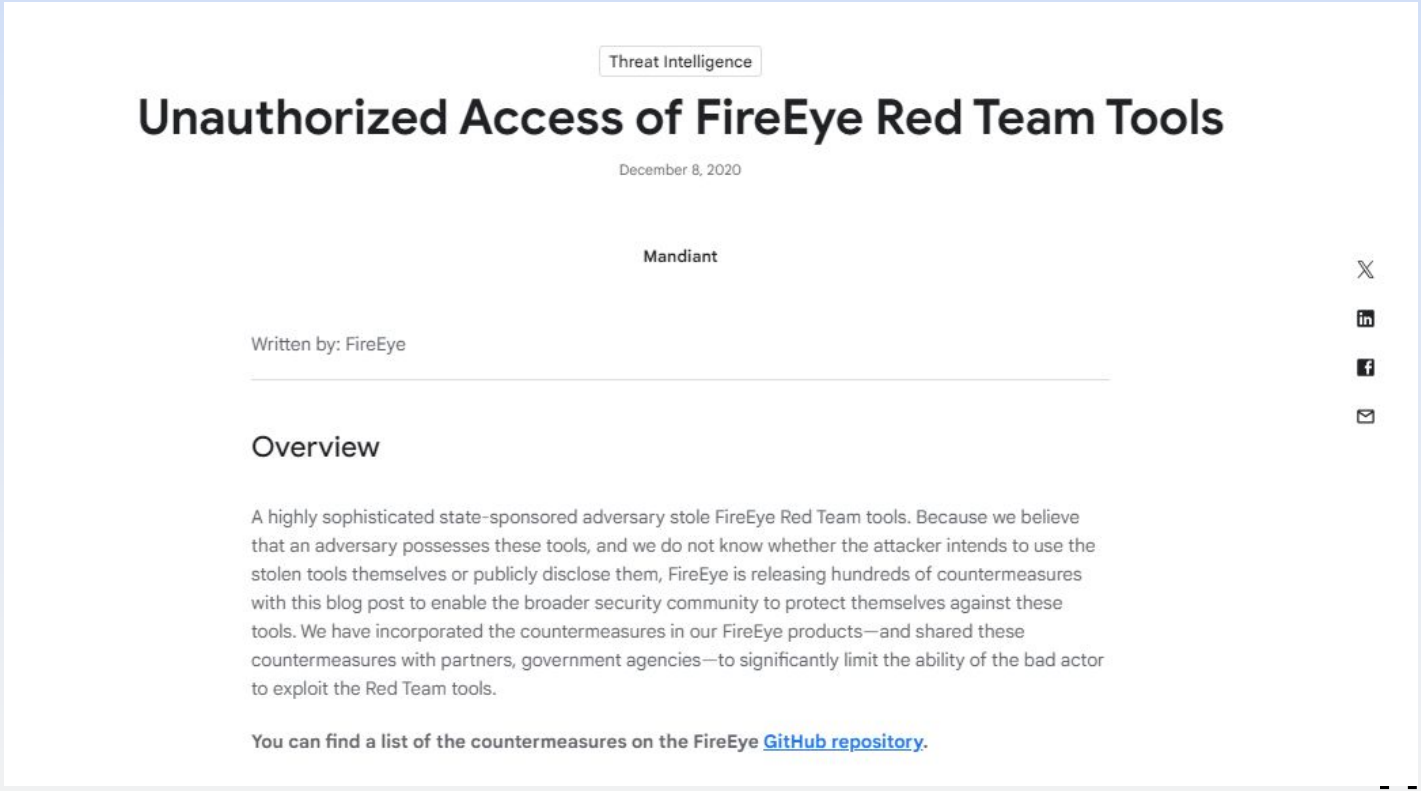
RAINDROP (*loader*): programs that provide means to download from external sources

- Inject Cobalt Strike beacon
- To execute file, temporarily replace legit file with malicious one, execute it, then restore original

Step 5: To the cloud!

- Information in Cloud (M365)
- Sometimes SUNBURST not needed
- Alternative ways of access

Step 6: Be sneaky



Threat Intelligence

Unauthorized Access of FireEye Red Team Tools

December 8, 2020

Mandiant

Written by: FireEye

Overview

A highly sophisticated state-sponsored adversary stole FireEye Red Team tools. Because we believe that an adversary possesses these tools, and we do not know whether the attacker intends to use the stolen tools themselves or publicly disclose them, FireEye is releasing hundreds of countermeasures with this blog post to enable the broader security community to protect themselves against these tools. We have incorporated the countermeasures in our FireEye products—and shared these countermeasures with partners, government agencies—to significantly limit the ability of the bad actor to exploit the Red Team tools.

You can find a list of the countermeasures on the FireEye GitHub repository.

05

Intro to CTFs

Time to register! https://forever.isss.io/

INFORMATION AND SYSTEMS SECURITY SOCIETY

Hands-On

https://overthewire.org/wargames/bandit/

06

Careers in Cyber

Check-In Form

OR

https://bit.ly/isss-cyber

INFORMATION AND SYSTEMS SECURITY SOCIETY

Thank You!

Any questions or comments?

INFORMATION AND SYSTEMS SECURITY SOCIETY