University of Colorado **Boulder**

CSCI 3403 INTRO TO CYBERSECURITY

Lecture: 1-1

Topic: Intro

Presenter: Matt Niemiec

Intro

Welcome!

- Introduce myself
- My office: ECOT 743
- Office hours: Wednesday, 2:30-3:30 or by appointment
  - Check Piazza for the most recent office hour times
- Email: Matthew.Niemiec@Colorado.edu
- TAs: Introduce themselves
- CA: Anusha.Gupta@Colorado.edu

What is This Course?

- Theory and implementation
- Learning to defend systems
- Becoming fluent in terminology
  - An attack or threat or exploit?
- Mile wide, inch deep
  - Explore concepts you find interesting!

What is This Course NOT?

- How to hack things
  - Though we may do a little of that!
- In-depth technical explanations of technologies
- Something to be used unethically
- Exclusively for people who want to pursue security

Syllabus

- Go to syllabus for course

Course Feedback

- We're listening!
- This is your experience – make it what you want!
  - Please discern between complaints and critiques
- Survey will be up all semester
- Myself or CM will read them
- Link: https://forms.gle/WRUUbPkmFNsa6q3D6

Weekly Readings

- Each week there are two types of readings
  - Recommended
  - Optional
- A shorter version of slides will be posted in advance
- Your learning is in your hands

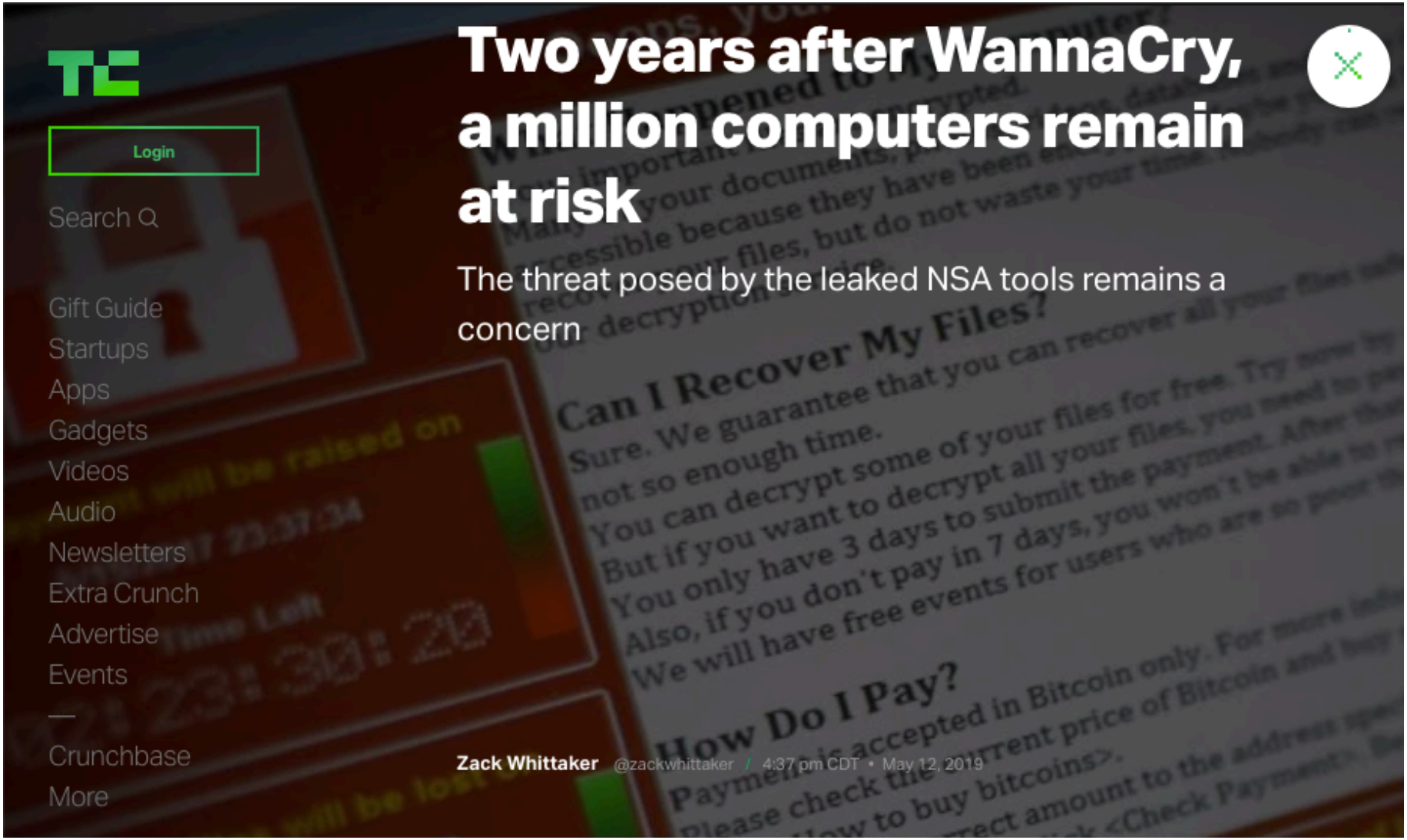
Course Structure

- Two main sections in course
- Introduction to security
  - The first three weeks
  - The “boring” stuff :(
- Everything else
  - The ”cool” stuff! :)

Security Now

Ransomware

- Software that encrypts your files
- Asks for payment to decrypt
- Cross your fingers and hope they decrypt your files


Login
Search
Gift Guide
Startups
Apps
Gadgets
Videos
Audio
Newsletters
Extra Crunch
Advertise
Events
Crunchbase
More
Two years after WannaCry, a million computers remain at risk
The threat posed by the leaked NSA tools remains a concern
Can I Recover My Files?
Sure. We guarantee that you can recover all your files
not so enough time.
You can decrypt some of your files for free. Try now by
But if you want to decrypt all your files, you need to
You only have 3 days to submit the payment. After that
Also, if you don't pay in 7 days, you won't be able to
We will have free events for users who are so poor
How Do I Pay?
Payment is accepted in Bitcoin only. For more
Please check the current price of Bitcoin and buy
How to buy bitcoins>.
And send correct amount to the address
Check Payment>. Be
Zack Whittaker @zackwhittaker / 4:37 pm CDT • May 12, 2019

LILY HAY NEWMAN SECURITY 04.23.2018 08:55 PM

Atlanta Spent $2.6M to Recover From a $52,000 Ransomware Scare

Whether to pay ransomware is a complicated—and costly—calculation.

Yeah, but you CAN pay...

PRIVACY AND SECURITY FANATIC

By Ms. Smith, CSO | MAY 22, 2016 9:00 AM PDT

About

Ms. Smith (not her real name) is a freelance writer and programmer with a special and somewhat personal interest in IT privacy and security issues.

NEWS

Kansas Heart Hospital hit with ransomware; attackers demand two ransoms

Kansas Heart Hospital was hit with a ransomware attack. It paid the ransom, but then attackers tried to extort a second payment.

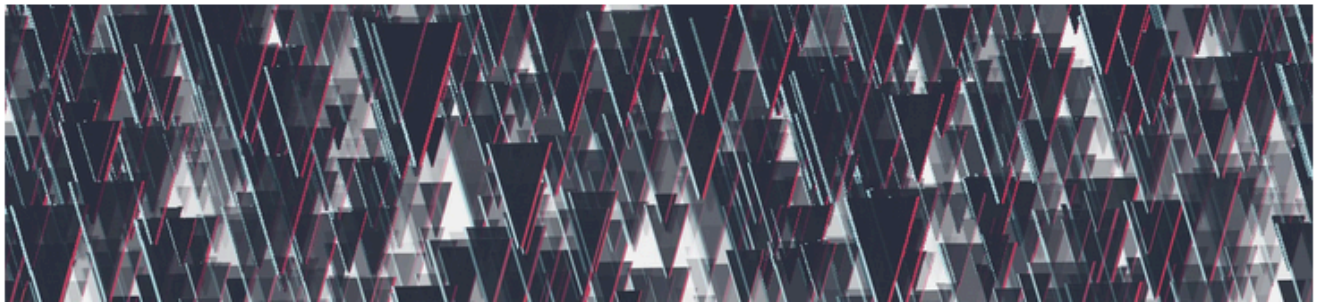
DDoS Attacks

WIRED BUSINESS CULTURE GEAR IDEAS SCIENCE SECURITY TRANSPORTATION SIGN

LILY HAY NEWMAN SECURITY 03.01.2018 11:01 AM

GitHub Survived the Biggest DDoS Attack Ever Recorded

On Wednesday, a 1.3Tbps DDoS attack pummeled GitHub for 15-20 minutes. Here's how it stayed online.



Car Security

WIRED

Hackers Remotely Kill a Jeep on the Highway—With Me in It

Share

SHARE

TWEET

COMMENT

EMAIL

ANDY GREENBERG SECURITY 07.21.15 06:00 AM

Hackers Remotely Kill a Jeep on the Highway—With Me in It

Is This a Joke?

ZDNet

VIDEOS BUILD A WEBSITE WINDOWS 10 CLOUD AI SECURITY TR PREMIUM MORE NEWSLETTERS

MUST READ: How the CIO fought their way back from the edge of extinction

Cryptocurrency-mining botnet uses a Taylor Swift image to hide malware payloads

MyKingz (Smominru) botnet hides the malware it deploys on infected hosts inside a JPEG of Taylor Swift.

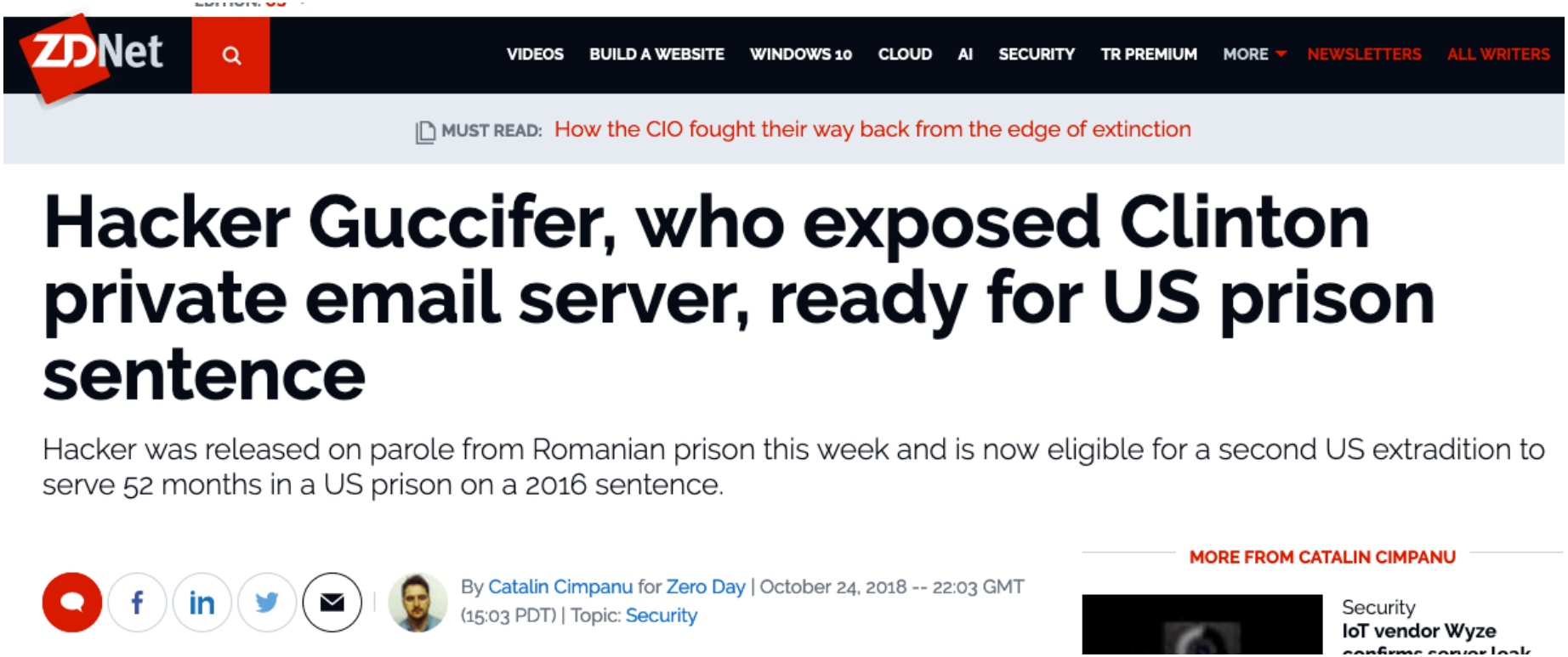
By Catalin Cimpanu for Zero Day | December 19, 2019 -- 05:30 GMT (21:30 PST) | Topic: Security

The operators of a cryptocurrency-mining botnet are currently using an image of pop singer Taylor Swift to hide malware payloads they send to infected computers -- as part of their normal infection chain.

MORE FROM CATALIN CIMPANU

Security
IoT vendor
confirms se

Defending Against Hackers?



What's The Point?

- How do we think about these things?
- We need to analyze the situation
- It's up to us to defend them

Common Security Principles

Humans Are the Weakest Link

- Humans have many “bad” qualities
  - Are sympathetic, gullible, trusting, lazy, biased, etc.
  - These can be exploited
- Can I hack into your system?
- We assume users are worse than ignorant

No System is Perfectly Secure

- What? Do we give up?
- Know who we're protected from
- Know who we're protecting against
- Adversaries have boundaries, too

The Offense Has The Advantage

- We must defend EVERYTHING
- Attackers only need one exploitation
- Not quite the full story

Everything Is Broken

- Computers weren’t made with security in mind
- You can find something wrong with EVERYTHING
- The Internet, computer hardware, secure protocols, etc.

CIA Triad

The CIA Triad

- Confidentiality, integrity, and availability
- The three pillars of computer security
- Everything we do in this ~~course~~ field

Example?

- We're back in third grade
- Alice wants to pass a note to Bob
  - The message: "The answer to question 3 is a"

Confidentiality

- “...The unauthorized disclosure of information”
- Keep “bad” people from seeing message
  - Bad is a matter of policy!
- Different than privacy
- In our example

Integrity

- “...Unauthorized modification or destruction of information”
- Keep people from tampering with the message
- In our example

Availability

- “...the disruption of access to or use of information or an information system”
- We don’t want to be cut off from our service
- How? Why?
- In our example

What Are We Protecting?

- Hardware
- Software
- Data
- Networks

Conclusion

- We want to keep systems secure
- We think of this through the CIA triad
- Protect many types of things
- Questions?