Infosec 101 and Faulty Assumptions in the Field

Introduction to the 101 Track

Deana Shick
CERT Coordination Center (CERT/CC)

Software Engineering Institute
Carnegie Mellon University
Pittsburgh, PA 15213

This material is based upon work funded and supported by the Department of Defense under Contract No. FA8702-15-D-0002 with Carnegie Mellon University for the operation of the Software Engineering Institute, a federally funded research and development center.

DM19-0496

Agenda

- Introduction
- What is the Field
- Compromising C,I,A
- If you are just beginning…
- Concluding Remarks
- Questions

Who Are We?

- Information Security was born at the Software Engineering Institute (SEI), which is part of Carnegie Mellon University
  - The SEI is a Federally Funded Research and Development Center (FFRDC) as part of Carnegie Mellon University
  - Only FFRDC with “cyber” in the charter
- Morris Worm outbreak in 1988 – birth of the CERT Coordination Center (CERT/CC)
  - Work with members of the Intelligence Community (IC), Computer Network Defense (CND) communities, and Law Enforcement
  - Spun up US-CERT at DHS post 9/11
  - Coordinates vulnerabilities on behalf of DHS for the general public

Who Am I?

- I've been at CERT for ~6 years
- I work on the Threat Analysis team as a Vulnerability Analyst within the CERT/CC
  - Analyze the intersection of vuls, malware, and threat actors
  - CVE, Vul Severity, OASIS
  - Taught CERT/CC's Vulnerability Response Capability Development class for CERT/CC
- Pioneered the Information Security Program at Duquesne University in Pittsburgh
  - Joint program with IR and Computer Science for undergrads
- Moonlighted at Carnegie Mellon's Heinz College in their Information Security Policy and Management Master's program

What is the Field?

Disclaimer

- This presentation is intentionally broad
- It is going to be from my perspective as someone who loves, teaches, and breathes threat-stuff every day
- I’m going to do a little bit of a dive into certain topics. I hope these things resonate with you.
- This could be a ~3-4 hour lecture

Information Security

- **"Information security**, sometimes shortened to **InfoSec**, is the practice of preventing unauthorized access, use, disclosure, disruption, modification, inspection, recording or destruction of information. The information or data may take any form, e.g. electronic or physical."

- Surrounding the protection of information:
  - Confidentiality
  - Integrity
  - Availability
  - Non-repudiation

https://www.law.cornell.edu/uscode/text/44/3542

Faulty Assumption #1

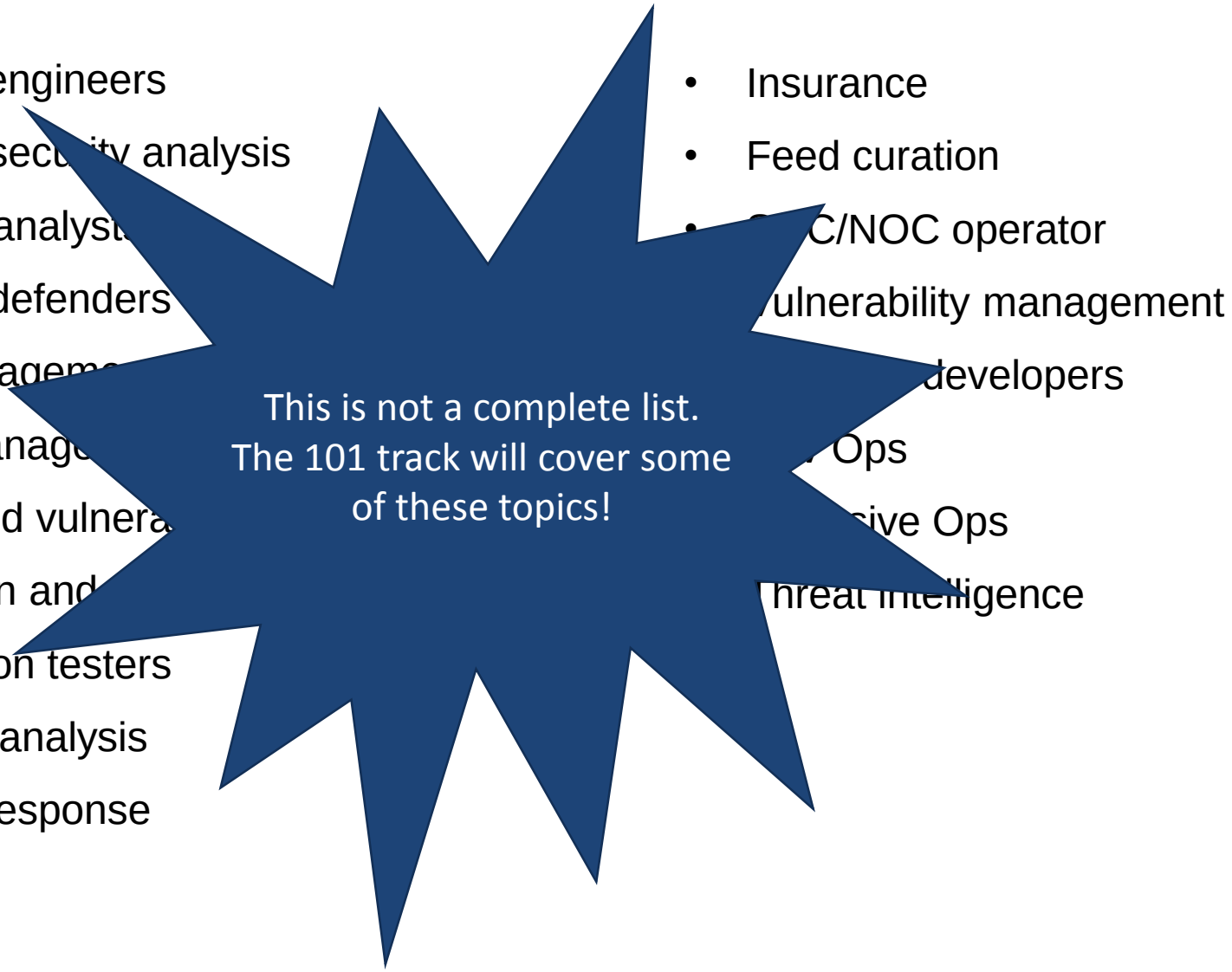
There is a ”right” answer to how secure you should be.

Faulty Assumption #1

- Risk tolerance
- No one-size-fits-all solution
- There are probably things you shouldn’t do
- Sliding scale based on risk of the things you should do

Where do you fit in?

- Security engineers
- Network security analysis
- Malware analyst
- Network defenders
- Risk manageme
- Policy manage
- Threat and vulnera
- Simulation and
- Penetration testers
- Strategic analysis
- Incident response
- Lawyers
- C-Suite



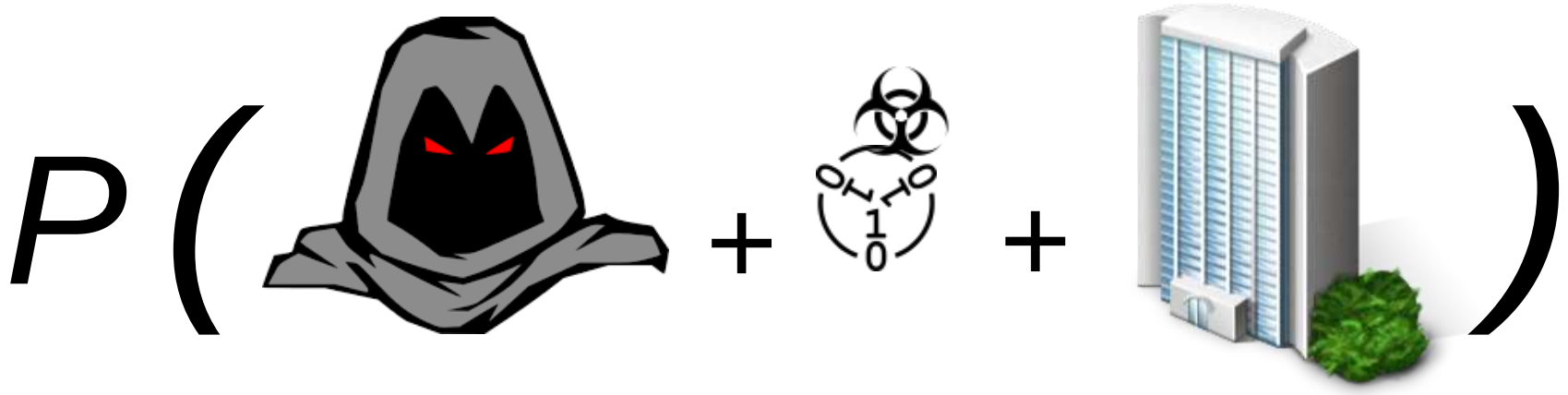
- Insurance
- Feed curation
- C/NOC operator
- ulnerability management
- developers
- Ops
- ive Ops
- hreat intelligence

Infosec 101 and Faulty Assumptions in the Field

Compromising C,I,A

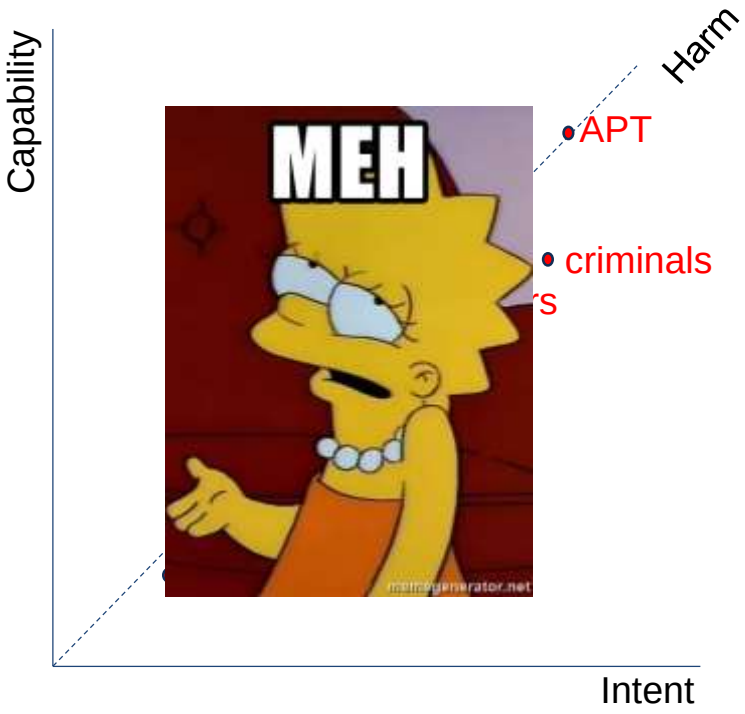
Threats

- A lot of the field revolves around how we understand ways CIA is compromised. This means a little bit of threat analysis (also my view of the world)
- People involved in this are risk management, procurement, policy creation, reverse engineering, vul management, etc.
- Your C-Suite operates on information provided to them by the aforementioned parties.

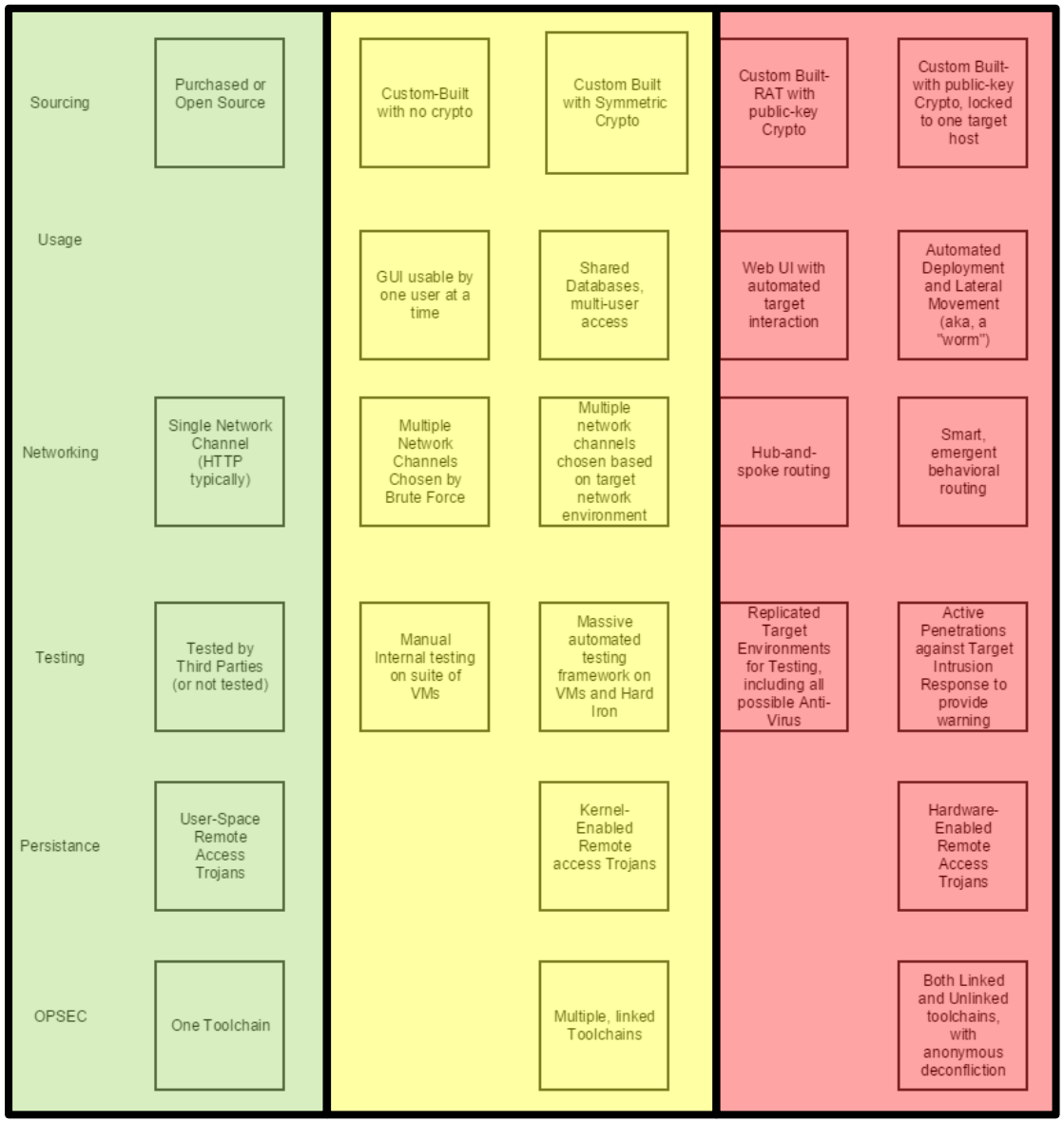


Actor

- The person/s behind the keyboard perpetuating harm
- The actor must have a motivation to do harm (old model)
  - Newbies (script kiddies), mess your day up
  - Hactivists, “political” agenda
  - Terrorists, “political” agenda
  - Insiders, make $$
  - Criminal organizations, make $$
  - Nation states, save $$
  - APT, save $$

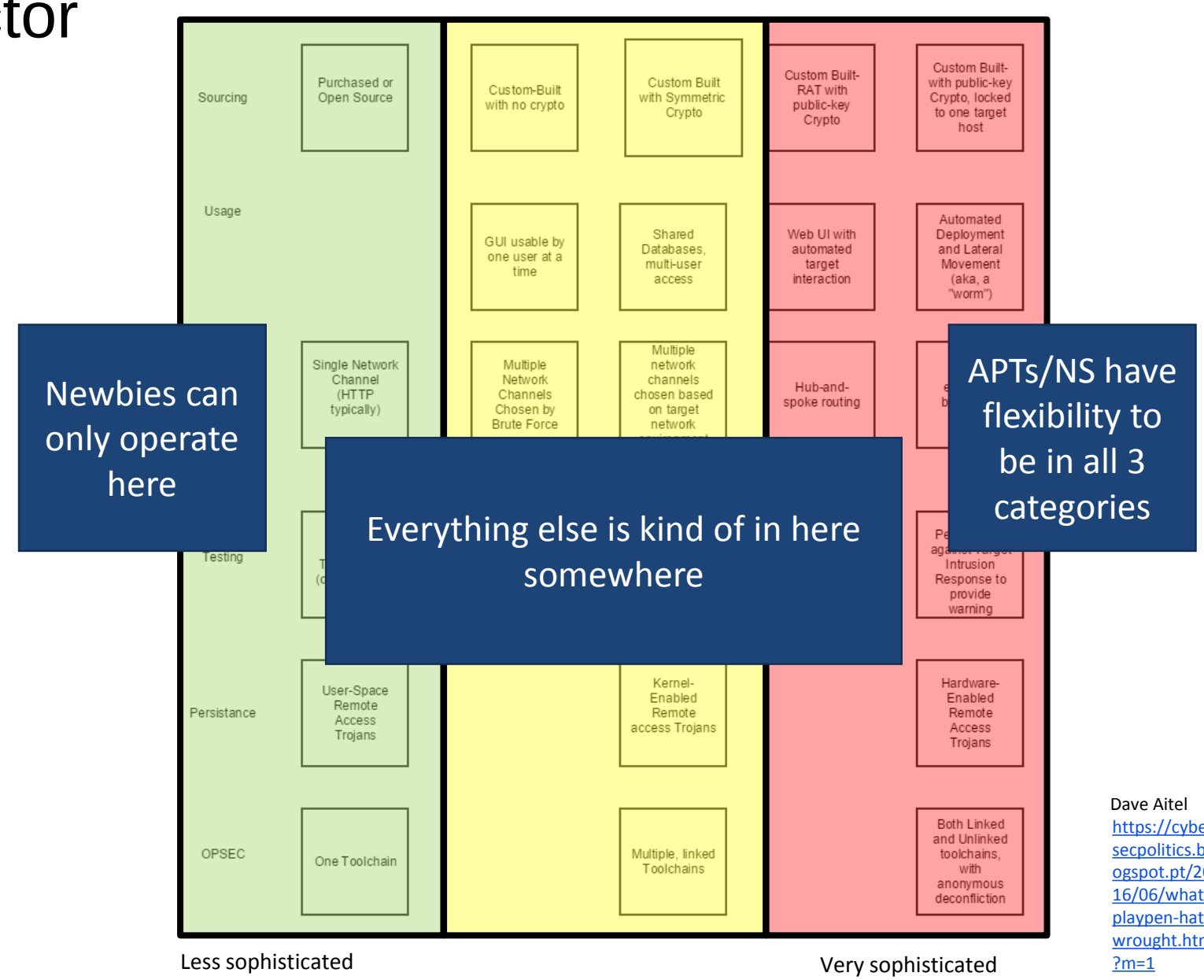


Actor



Dave Aitel
https://cybersecpolitics.blogspot.pt/2016/06/what-playpen-hath-wrought.html?m=1

Actor



Dave Aitel
https://cybersecpolitics.blogspot.pt/2016/06/what-playpen-hath-wrought.html?m=1

Faulty Assumption #2

The APT and/or Nation State is the biggest threat to me.

Faulty Assumption #2

- No organization is 100% secure all of the time
- It is really hard to do attribution
- APTs and/or Nation States are your 1%. If they want to get in, they probably will
- You have 99% of things to worry about
  - Shore up against those things

Tools

- What the actor uses during their operations. Think of this like any other tool
- Includes:
  - Vulnerabilities – weakness in code. “code is data and data is code”
  - Exploits – the code used to take advantage of a vul
  - Native utilities built into your OS
  - IP address and domain names
  - Delivery mechanisms – infection vectors (physical/virtual)
  - Malware – does and doesn’t use vuls.
  - Overall trickery/social engineering

Tools

- Network defense operates here to protect against threat actor tools
  - SOC operators should pivot on these findings
  - Threat intelligence can also operate here
- Keep in mind that tools alone are useless without an actor and target
- There are a ton of sub fields in the Tooling category, so I am going to try and keep it as broad as possible.

Faulty Assumption #3

If I patch my machines, I'm definitely safe from actor tools. My scanner gave me no results, so ¯_(ツ)_/¯

Faulty Assumption #3

- There are a lot of issues with this one…so here we go…
- Patching may not be the magic bullet. It certainly helps, though!
  - You should test patches
  - Prioritization is a real issue for organizations
- Vulnerability scanners sometimes operate on vulnerability identification (like CVE, for example), headers, etc.
  - CVE is working on it, but it's not 100% wholistic of the vuls that are out there
  - Not referring to only the "zero-day" either
- Anti-virus isn't perfect
- **TL;DR the tools you use may not be as good as you think.**

Victims

wtop NEWS TRAFFIC WEATHER LISTEN

Home » Baltimore, MD News » Cyberattack cripples Baltimore's government...

Cyberattack cripples Baltimore's government computer servers

AP By The Associated Press
May 7, 2019 6:29 pm

BALTIMORE (AP) — Baltimore's government on Tuesday rushed to shut down most of its computer servers after its network was hit by a ransomware virus. Officials believe it has not touched critical public safety systems.

Agents with the FBI's cyber squad were helping city technology employees try to determine the source and extent of the cyberattack. Baltimore Mayor Bernard "Jack" Young said police, fire and EMS dispatch systems have not been affected, but other layers of the mid-Atlantic city's network have been "infected with a ransomware virus."

"At this time, we have seen no evidence that any personal data has left the system," Young tweeted Tuesday afternoon.

While the scope of the problem wasn't immediately clear, email and phone outages hobbled parts of the city's network. Public works officials told customers that "for now we're unable to take calls to discuss water billing issues." Finance department employees said they could only accept checks or money orders.

The Tuesday problems come just over a year since another ransomware attack hit Baltimore's 911 dispatch system, prompting a worrisome 17-hour shutdown of automated emergency dispatching. The March 2018 attack required the transition of the critical 911 service to manual mode.

Following last year's attack, which came days after ransomware staggered the city of Atlanta's computer network, officials in Baltimore disclosed that its systems were made vulnerable by an "internal change to the firewall" by a technician who was troubleshooting within the automated dispatch system.

Ransomware typically exploits known software vulnerabilities. Cybersecurity experts say organizations that fall victim to such attacks often haven't done a thorough job of patching systems regularly.

Russia-Linked Hackers Responsible for Vast European Cyber Attacks, Says Microsoft

Read More

Russian Hackers Attempted to Br... DNC After the 20...

Russian Hackers Reportedly Been... Orthodox Christi...

Here Are Some H... From Facebook a... Twitter's Senate...

A Russian Hacke... Confessed to Ha... DNC During the E...

By LUCAS LAURSEN February 20, 2019

Russia-linked hackers have attacked over 100 accounts linked to European think tanks and civil society NGOs, Microsoft said Wednesday. The victims include the German Council on Foreign Relations, European branches of the Aspen Institute, and the German Marshall Fund.

Victims

- The person, place, or organization where C, I, A is compromised in one way or another
  - C: PII, credit card numbers, super secret flight information is taken without your consent
  - I: an actor changes your super secret airplane schematics, financial records, or any other data without your consent
  - A: The system by which you process customer credit cards, or the machine you use to build your plane is down
- Financial impacts of these are determined by the organization itself
  - A bank may have more interest in availability than an engineering firm, for example
  - Risk tolerance is also determined from org to org

Faulty Assumption #4

No one will target me. I have nothing to hide.

Faulty Assumption #4

- Your organization has some asset you want to protect (I'd hope)
  - Data
  - Humans
  - Machines
- You may be targeted purely as a byway for something else
  - Computational power – cryptocurrency mining
  - Insecure DNS server – hop point
- Maybe you showed up on Shodan, and someone is targeting you because they can

If you are just beginning…

Pick something!

- You can't be good at EVERYTHING
- If you are a career changer, infosec can use your unique perspective
- Pick something you really like if you are just starting out
- If you are transitioning between sub fields, remember the big picture
- Infosec cares about C, I, A. Figure out where you fit in.

Challenge Assumptions

- If you are seasoned in the field, you have probably heard the four assumptions (and then some)
- Progress can be made by challenging these things
- Learn from others in the field
- Continue to go to these types of events!

Infosec 101 and Faulty Assumptions in the Field

Concluding Remarks

To Wrap Up

- We went over the definition of infosec and how it centers around C, I, A, and Non-repudiation
- We discussed C, I, A can be impacted by discussing how threats work
  - Probability (Actor + Tool + Target)
- We discussed four faulty assumptions in infosec that people make all of the time:
  - Information security is binary in terms of making “correct” decisions
  - I should only care about APTs
  - My security tools will save me
  - No one will target me

RVASec has an awesome lineup

The 101 track is going to cover the following:

- What is Cyber Insurance: Are you covered?
- Vulnerability Assessments and Penetration Tests
- Social Engineering, Physical Security, & USB attacks
- Risk Assessments: The Heart of Risk-based Security
- Network Security 101
- Being Secure Doesn’t Mean You Are Managing Risk
- RVASec 101 Panel

Contact

Deana Shick

Member of the Technical Staff

CERT/CC

@deanashick (Twitter)

dshick@cert.org

Questions?