Malware Self Defense

Protecting you and your friends from digital monsters

Blue Team is best team - quick pause from actual pres

- Defensive-side of security
  - Very fulfilling
  - Higher demand
- Purpose of Red Team…
- (can be) less frustrating
- Includes:
  - Incident Response
  - Malware Analysis/CTI
  - Defense Engineering
  - Forensics
  - etc

Malware Threat Landscape

- Anyone been infected?

- Types of malware? - constantly evolving

Malware Threat Landscape

- Anyone been infected?

- Types of malware? - constantly evolving
  - Ransomware
  - RATs / C2 Agents
  - Banking Trojans / InfoStealers
  - Cryptominers
  - PUPs
  - Droppers
  - Worms
  - etc

Malware Threat Landscape

- Anyone been infected?

- **Your** threat model
  - Individual user
  - … also in security
  - **Generally** more-technical than average user - **NOT TO BE RELIED ON**

Malware Threat Landscape

- Anyone been infected?

- How infected?

Malware Threat Landscape

- Anyone been infected?

- How infected?
  - phishing / social engineering / “trojans”
  - vulnerability - webbrowser or other server being hosted
  - sketchy software / supply chain / virus
  - compromise / insider threat
  - JavaScript or other code running on top of program
  - spontaneous generation
  - infinite attack vectors

Defenses - **Overview**

- Prevention
  - Awareness (unreliable)
  - Keep devices up-to-date (duh)
  - Investigate sketchy/dubious stuff
  - Tighten defenses - firewall, **disable** macros, isolate environments
- Alert
  - Intrusion Detection System
  - IOCs
- Detection / Removal
  - Anti-malware scanners
  - Manual threat hunting
- Remediation - **frequently** ignored
  - How did the infection occur? and how can defenses be improved?
  - Damage caused…

- How reliable are these?

Investigating Sketchy Stuff…

- When in doubt -> Avoid (or is **absolutely** necc. -> isolate)
- Signatures
  - VirusTotal / Antiscan[.]me
  - Google - be careful when searching URLs
- Sandbox
  - Any.Run / Hybrid Analysis
  - Screenshot Guru
  - VirtualBox / isolated system
- Reverse - will be covered in greater detail later
  - Be **super** careful where/how you do this
  - Research what is there, look for obfuscation/packing or other malicious indicators

- What have ya seen in the past? What do you see in the GitHub?

Anti-malware and Endpoint Detection

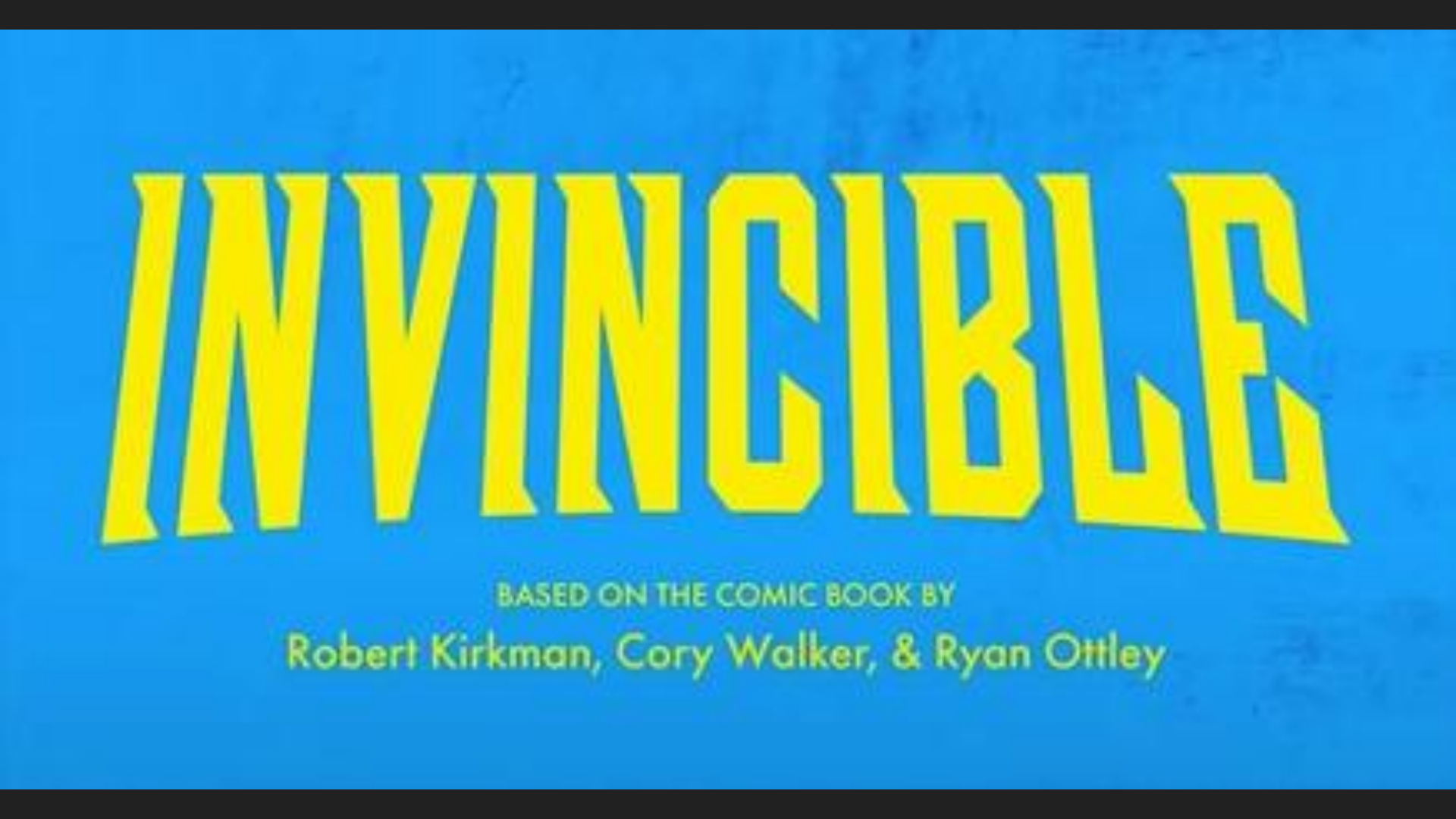
- Thoughts on using AV?

- Static vs Dynamic detection
- WD is not great…
- Top *free* AVs - based on my research and xp
  - Avira
  - BitDefender
  - Comodo
  - Kaspersky?
  - **Roll your own!**

Remediation

- It does matter bc you are **NOT**

- Malware really gone? - pls don’t get too paranoid
- Investigate artifacts
  - VirusTotal
  - Sandbox reports
  - Consult friends
- Change PWs, monitor accounts, **alert others**


INVINCIBLE
BASED ON THE COMIC BOOK BY
Robert Kirkman, Cory Walker, & Ryan Ottley

Remediation

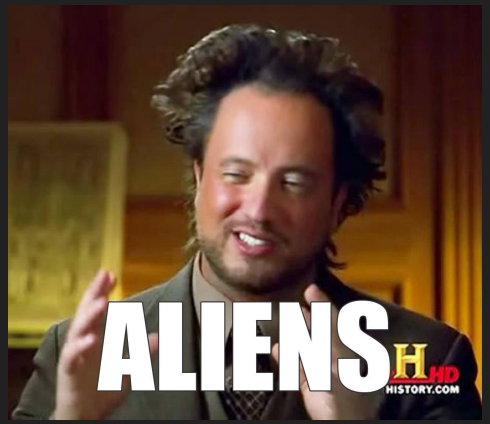
- It does matter bc you are **NOT** invincible

- Malware really gone? - pls don’t get too paranoid
- Investigate artifacts
  - VirusTotal
  - Sandbox reports
  - Consult friends
- Change PWs, monitor accounts, **alert others**

Remediation

- It does matter bc you are **NOT** invincible

- Malware really gone? - pls don’t get too paranoid
- Investigate artifacts
  - VirusTotal
  - Sandbox reports
  - Consult friends
- Change PWs, monitor accounts, **alert others**



Links

- Workshop Repo - https://github.com/Abjuri5t/Malware-Defense_Workshop
- VirusTotal - https://www.virustotal.com/gui/
- Google - https://www.google.com/
- Any.Run - https://app.any.run/
- Hybrid Analysis - https://www.hybrid-analysis.com
- Screenshot Guru - https://screenshot.guru
- OSBoxes - https://www.osboxes.org
- Avira - https://www.avira.com/en/free-antivirus-windows
- BitDefender - https://www.bitdefender.com/solutions/free/thank-you.html
- Comodo - https://antivirus.comodo.com/download/thank-you.php?prod=cloud-antivirus
- Resources for AV script - https://github.com/Abjuri5t/Malware-Defense_Workshop
- phishing@wpi.edu - mailto:phishing@wpi.edu

Security News

- SANS StormCast - https://is.sans.edu/podcast.html
- Off the Record - https://the-record.captivate.fm

Learn Malware Analysis

- **(stay tuned!)**
- Malware Analysis Bootcamp - https://www.youtube.com/watch?v=uHhKkLwT4Mk

Darknet Diaries Episodes

- WannaCry - #73
- Mikko - #74
- Dark Caracal - #38
- STUXNET - #29
- NotPetya - #54