**Rootkit Seek & Destroy**

**Anything with any electronic intelligence, has firmware and therefore subject to firmware rootkits**

Firmware has full access over the system

IOT devices are especially something to be careful of when it comes to this

Open-source hardware is a good attempt at combatting this

**Mitigation (UEFI / BIOS)**

* Enable secure boot
* UEFI SecureFlash is enables
* Update BIOS whenever there is a security patch
* Set a strong BIOS or UEFI password
* Re-flash your firmware if you suspect a problem

**Virustotal**

* Extract firmware using the below tools and check

Darwindumper

* MacOS
* Dump firmware

Flashrom

UEFI firmware

* Python

ChipSec

Make sure private info like Wi-Fi passwords are removed before uploading BIOS to virustotal

**End-Point Recovery & Remediation**

A lot of approaches to malware is to prevent and detect malware from doing what it wants but there isn’t enough focus on being able to clean the system and restore to a good condition which is just important

Containment should be considered allowing you to record all end-point events and activities, allowing it to undo what a hacker has done

* Snapshots
* Disk-cloning (restore to good state)
  + Rollbackrx
  + Macrium Reflect
  + CarbonCopy
  + TimeMachine
  + DriveImage
  + CloneZilla
  + TrueImage
  + **Terabyte**
  + AWS
  + TurnKey

**The faster and quicker you can respond to a threat, the less it’ll cost you in terms of resources, time and impact**

**Effective response and recovery is the final layer in effective end-point protection**