Don't trust that storage medium

Tatu Erkinjuntti

11/28/2024

So, what is a storage media?

- A physical device that can store data.
- In IT, these are commonly:
  - Hard disc drives (HDDs)
  - Solid-state drives (SSDs)
    - USB mass storage devices are commonly SSDs
  - Magnetic-tape drives
  - Floppy discs
  - Optical media
    - CD’s
    - DVD’s
    - Blu-ray’s

What are the areas we are interested in?

- USB mass storage devices
- Optical media
- Hard disc drives (HDD) & Solid-state drives (SSD)
  - Excluding USB devices

What is out of scope for this presentation?

Floppy discs

- To be considered legacy.
- Not used in consumer electronics anymore.
- Windows 10 / 11 no longer offer device drivers by default.
- Linux should offer support in the stock kernel.

Magnetic-tape drives

- Mainly used for long-term storage and archiving.
- Doesn’t really have a place in consumer electronics at the moment.

What should we consider when dealing with storage media?

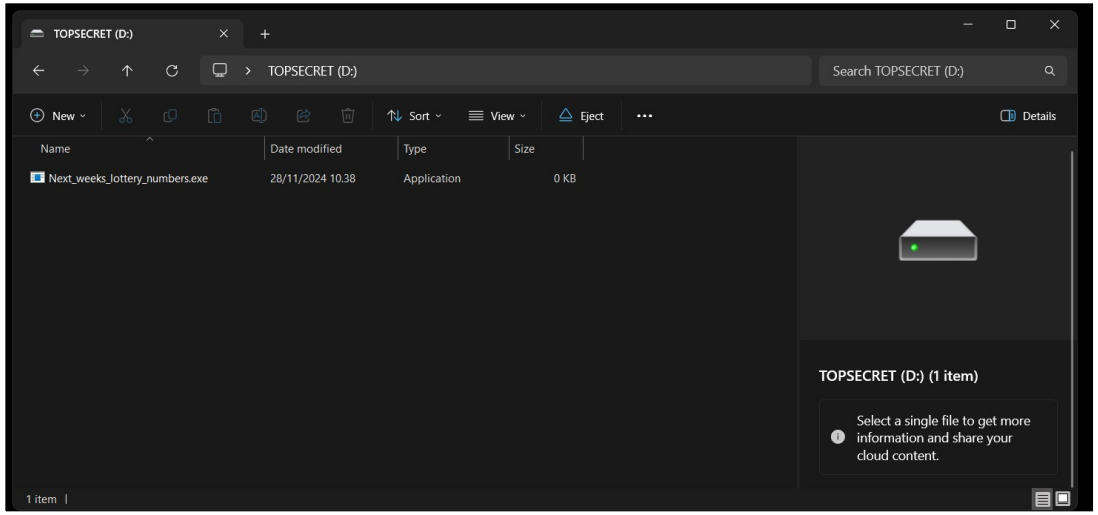
- Generally, If you do not know the device origin, don’t use it.
  - If you must check an unknown storage medium, sandbox it.
    - Virtual environment.
    - Nonessential computer with no network access.
- Even up to date virus protection might not protect your system.
- “Curiosity killed the cat”, just inserting the device might be enough to get compromised.
- In some cases, even formatting the device does not offer protection.

So, what should we be worried about when dealing with storage media?

- May contain malicious software (Malware), examples are:
  - Worms
  - Trojan horses
  - Ransomware
  - Spyware
  - Scareware
  - Wipers
- Payload can be delivered/executed by various ways:
  - User interaction
  - Infected boot sector
  - USB device enumeration
  - Autorun / Autoplay on insertion
  - Corrupted disc firmware
  - Payload hiding in an overprovisioned part of the SSD (theoretical)

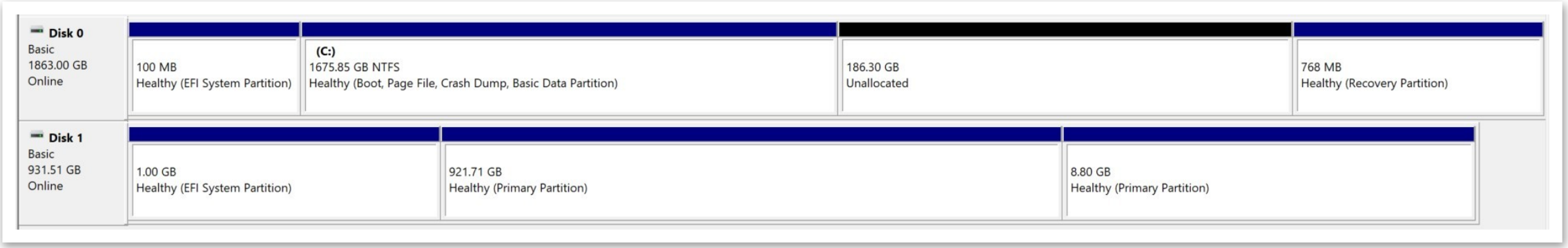
User interaction, a universal way of executing a payload.

- Regardless of device type or attack vector, getting the user to execute the malicious payload is the most convenient way to infect the target host.
- This can be achieved by trickery
  - Swapping a device or file with a something similar
- This can be achieved by social engineering
  - Raising curiosity
  - Pass on as a legitimate article
  - Inducing fear and panic



Infected boot sector, the silent killer

- Boot sector is an area located usually in the first partition of a disc.
- At boot, computers look at the active partitions and checks if they are bootable.
  - Does it contain code that the computers firmware (BIOS / UEFI) can execute.
- This is a normal procedure and is how operating systems are loaded.
- An infected boot sector loads malicious code to RAM, altering or replacing the computers original boot code.
  - After this the malware is loaded every time the computer boots.



USB mass storage devices

- By far the most convenient way to deliver a payload on a physical device
- Devices are cheap, can be produced in mass
- A common and familiar storage device for people
- Since USB (Universal Serial Bus) is an industry standard, this creates an intriguing attack vector for payload delivery.
- Computers use USB enumeration on device insertion to determine what device was inserted, malware can be delivered without user interaction.
- Examples:
  - BadUSB: Can act as a human interface device (Emulates a Keyboard for Keystroke Injection) or a storage device
  - KillerUSB: Aims to harm or destroy the computer that it’s attached to by discharging electricity to it.

Optical media

- Optical discs aren’t that widely used as in the past, but they still have a place in IT.
- Efficient malware delivery relies on operating system autorun/autoplay function in insertion.
- Today, this functionality is usually disabled by default, but some operating systems (example Windows) gives the users a popup dialog on what to do with the inserted disc.

Hard disc drives (HDD) & Solid-state drives (SSD)

- HDD’s and SSD’s offer more persistence for an attack.
- This attack vector usually requires much more effort from the attacker and after successful insertion, are harder to mitigate.
- Two examples for HDD’s and SSD’s related vulnerabilities.
  - Corrupted disc firmware.
  - Malware hiding in an overprovisioned part of the SSD.

Hard disc drives (HDD) & Solid-state drives (SSD)

Corrupted disc firmware.

- Hard drive firmware (“device operating system”) is an essential part of HDDs and SSDs, without it, it they can’t operate.
- Unseen to the user, since its not apart of the disc partitioning table.
  - Because of this, normal disc formatting will not remove the malicious content
- Corrupted disc firmware can execute malicious code on host device boot (like infected boot sector).

Hard disc drives (HDD) & Solid-state drives (SSD)

Malware hiding in an overprovisioned part of the SSD

- *Note! Issue reported by IEEE, I could not find a real-world example of use.*
- SSD overprovisioning is a method to extend SSD longevity and improve performance by reserving a portion of the disc.
- Malware could be hidden in an overprovisioned area of the disc and accessed by resizing the disc overprovisioning
  - This could be done by the attacker
  - Unintentionally by the device user

What recomendations are there to mitigate storage media related threats?

- User training and increased awareness

- Securing computer from BIOS / UEFI
  - Enable Trusted Platform Module (TPM)
  - Secure device boot
    - Using secure boot
    - Limiting bootable devices
      - Can only boot from operating system disc
        - Limit boot priority or boot order
      - Disable unneeded boot devices or locations
        - Network (HTTP(S) or PXE for example), USB, Optical drives

What countermeasures are there to mitigate storage media related threats?

- Use up to date virus protection
- Restrict system administrator rights

Thank you!