USE CASE

authUSB SafeDoor in Critical Infrastructures

What is the specific issue of Critical Infrastructures regarding USB flash drives traffic?

According to definitions, Critical Infrastructures are the strategic infrastructures, which provide essential services and whose functioning is indispensable and does not allow alternative solutions, so that their disruption or destruction would have a serious impact on essential services.

Isolated networks (OT) involve the use in both, own and third-party processes (updates etc.) of USB flash drives. Within these C.I, this use is regulated and controlled, currently using in the accesses to them sanitization kiosks , Firewalls and other elements that are dedicated to scanning USB devices malware threats, only at a software level.

Hardware attacks (BadUSB) carried out via USB drives, are very specific, targeted. The attacker knows perfectly the system that is about to breach. Such threats are also undetectable, persistent over time and, in most cases, irreversible.

Finally, there is the Electrical threat (USB Killer). This threat is intended to bring down the first layer of physical security in the organization and thus prevent the use of USB devices that have to access the network to be protocolized. Normally this previous takedown is given as part of a combined attack. Sand would disable the dedicated equipment of the network with the purpose of carrying out a subsequent attack at a Hw level. This is meant to be persistent in time and, what is most serious, undetectable. Nothing scans computer's HW.

What is SafeDoor*?

SafeDoor is a Hw device with embedded SW that acts as a barrier between USB devices and an organization's computers by analysing, blocking, informing, and auditing cyberthreats at three levels:

- Electrical: Identifying and stopping destructive UsbKiller-type surge attacks.
- Hardware: detecting and disabling BadUsb family attacks, HID (rubber ducky and similar) attacks, fake network cards, composite interfaces, etc.
  In such attacks, the scan that SafeDoor performs of the device is based on the behaviour of the device itself, not on attack patterns, which gets that. Even if the threats evolve, SafeDoor will always be able to detect them. This detection is done continuously and in real time.
- Software: With up to two integrated antiviruses, safeDoor performs a pre-download scan of any content.

SafeDoor thus, enables protocolization in the use of USB devices within organizations. Once SafeDoor shows up that no threat is detected, we can manage safely through it all the information inside the USB device.
SafeDoor is certified under the Lince methodology and is part of the CCN, CPSTIC catalogue.
*Protected under patent

How does SafeDoor fit into our work and cybersecurity scheme?

1. ACCESS CONTROLS

Fully autonomous installation of SafeDoor (Only connected to the Electrical network) Through the built-in LEDs SafeDoor tells us whether the connected device is safe or not, performing the scanning at the three types of threats.(HW, SW and electrical)

2. DIRTY/CLEAN PORT

Port 1- (Dirty Port) The user connects to one of the usb ports of the SafeDoor device, the USB drive from outside the organization and whose information wants to safely dump into a new Pendrive. (Border Team)

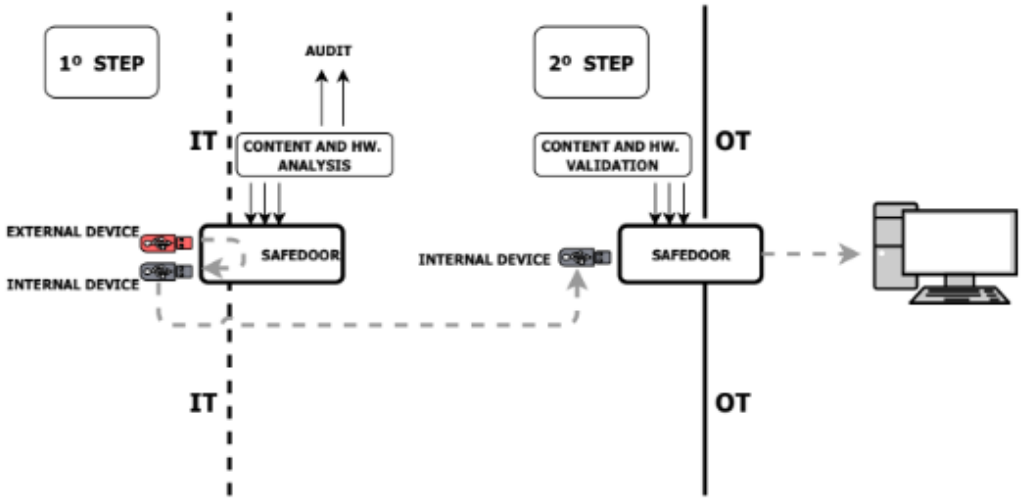
Port 2- (Clean Port) In the second port of the SafeDoor device we connect the trustable prendrive, where we are going to dump the information. We manage to make sure that both , the information contained in it and the hardware itself, doesn't contain a threat of any kind.

It is possible, if necessary, to establish a protocol for the use of **reliable devices** used within the organization.
SafeDoor allows the use of Encrypted USB devices (Bitlocker , Iron Key, Datalocker…)
SafeeDoor also includes the possibility of using digital signature of the files that are downloaded to ensure its integrity.

3. INTERNAL NETWORK

Any USB device that enters ,exits or is used in your organization, is pre-analyzed with SafeDoor and will never be connected directly to corporate devices. This prevents,the different networks and communications between them ,from any Hw, Electrical or Sw attack.

In all cases, the deployment of SafeDoor prevents the leaking of internal information from the organization through USB storage devices. There is a possibility of allowing it, under a strict protocol and always auditing this extraction through our Central Console.



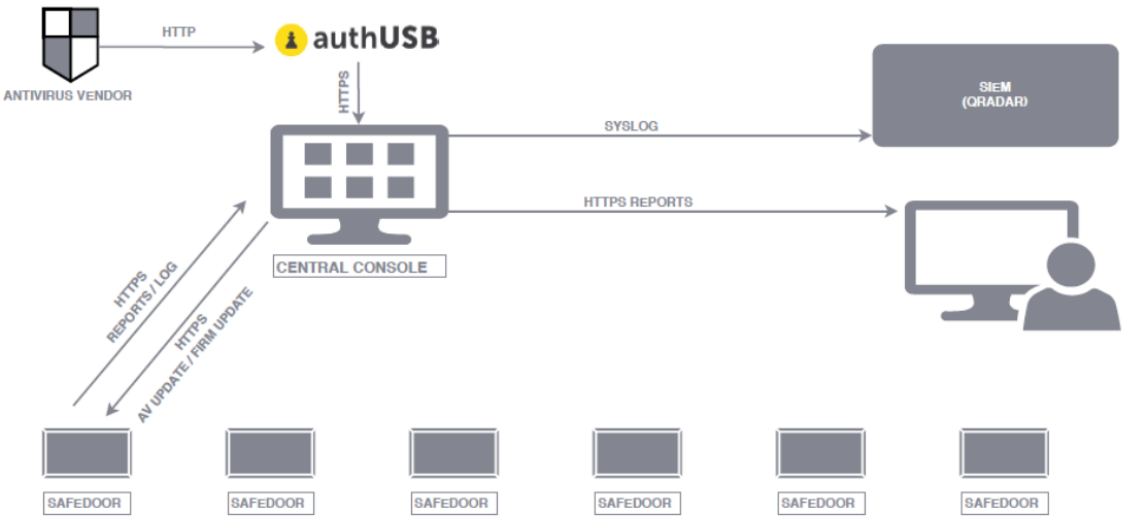
FAQ:

1. **Maximum number of antiviruses embeded on SafeDoor***
Safe Door supports up to two simultaneous antivirus engines. We can log it either to a metadefender machine or sending the files to a Sandbox.
*We can integrate more than two if necessary

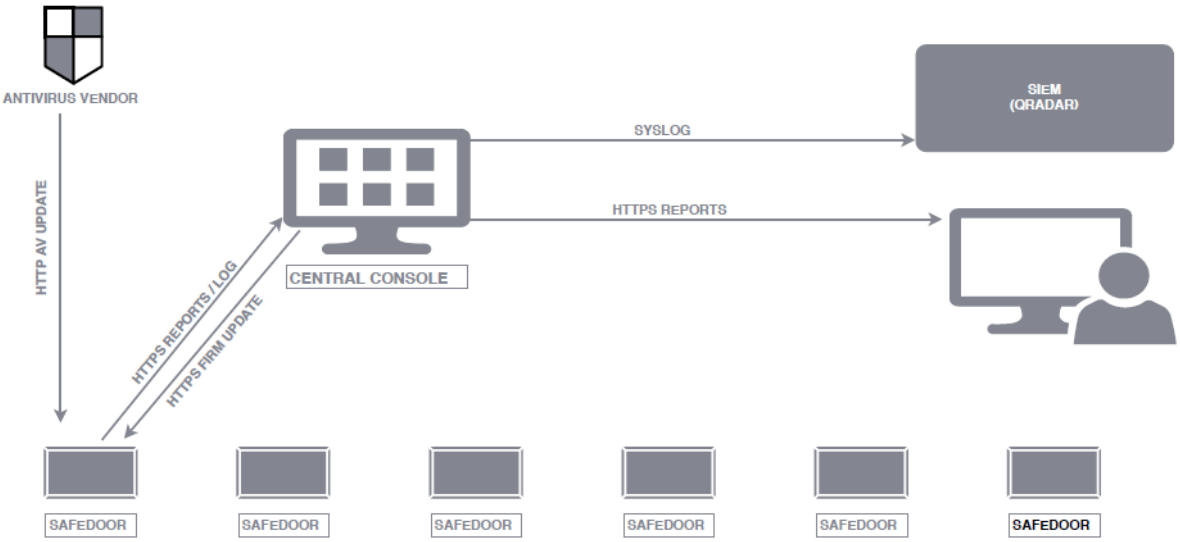
2. AV and our own SW Updates

There are three methods of updating signatures, depending on the environment:

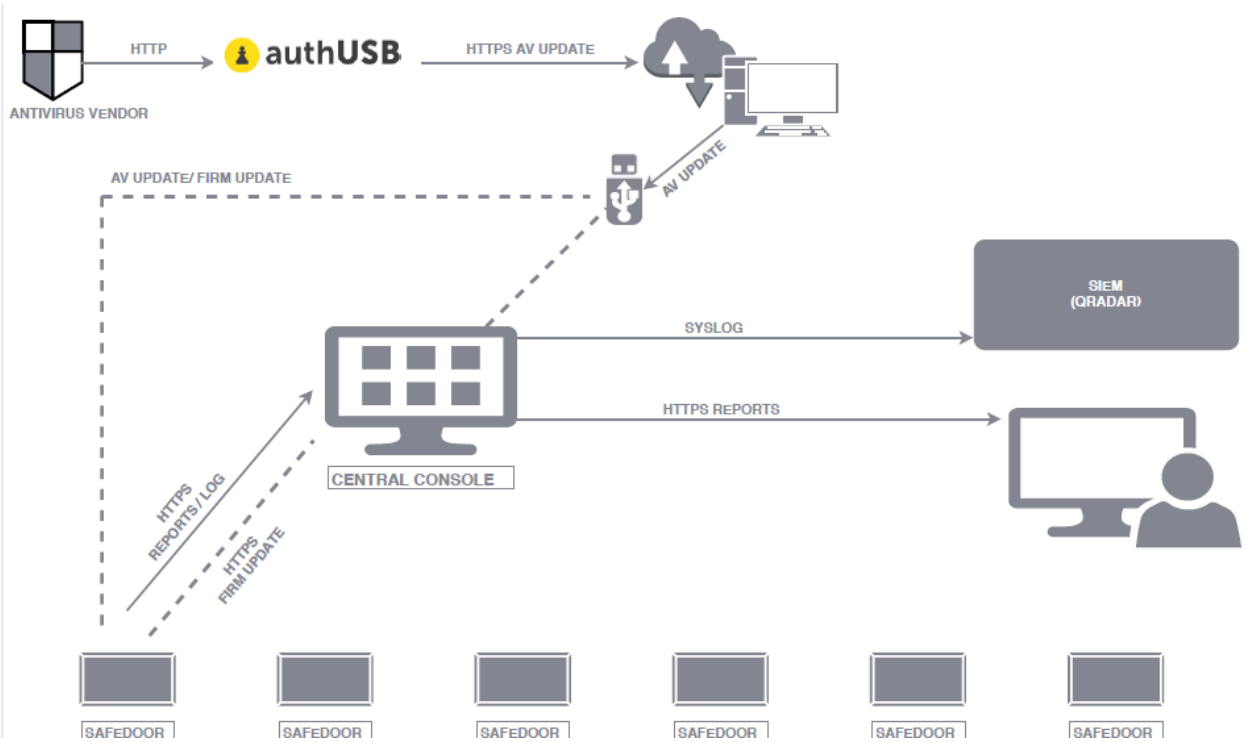
- **Direct**. If SafeDoors are outbound to the internet, either directly or via proxy, they are updated directly against the antivirus provider's server.



- **Indirect.** If the safeDoor does not have internet output but their central console does, they will use this as a mirror for the upgrade.



- **Ofline**. We provide a tool (windows) to run from a computer with internet output, that will obtain the signatures and dump them on a USB stick. This memory can be connected to any safeDoor, which will be used as an update source. It can also be used to dump signatures to the central console (if it is on an isolated network) to act as a mirror for its associated safeDoor.



3. Scan levels to run (fast, full, selective,.)

As soon as a memory is connected to safeDoor, hardware and electrical analysis is performed automatically. This analysis is very fast, just two seconds ,the USB device is continuously being monitored until it is unplugged

For software scanning (antivirus) there are two modes of use:

- **Manual:** From SafeDoor's web browser, the user selects the files/folders to download. On these selected files, analisis is carried out by the antivirus (selective analysis)
- **Automatic**: Anti-virus scans all the contents of the memory reporting through Leds its progress and result. No need to access the web interface. The computer is autonomous (full analysis)

It is also possible to modify the default settings of antivirus engines (maximum size, depth levels in compressed files, extensions to be scanned...)

4. Average USB scanning time.

The scanning time is similar to that of a desktop computer, since the bottleneck is at the reading speed of the USBstick. With modern USB flash drives read speeds of about 35 MB/s can be achieved, while with advertising memories or degraded by usage the speed can drop to 15/20 MB/s.

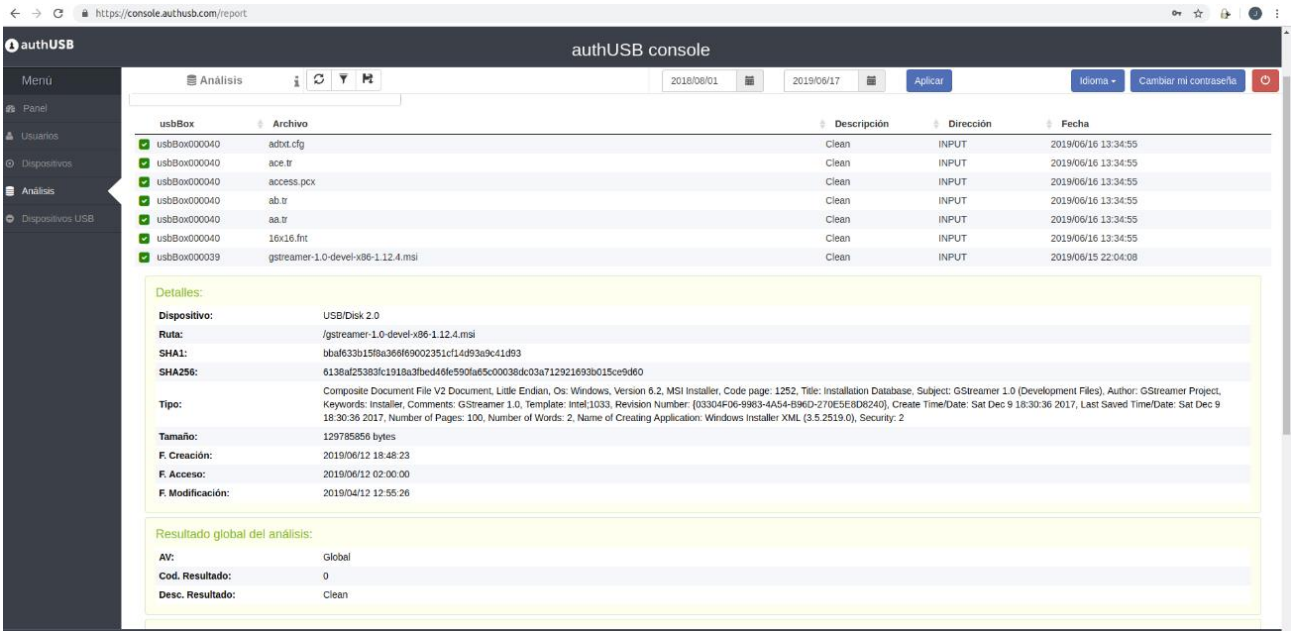
5. Log storage: device, console?

Each action performed on each safeDoor is dumped in real time onto the Center Console. In case of loss of connectivity or isolated computers, these reports will be stored on the device, being possible to download (digitally signed) for subsequent loading to the central console manually through its web interface.

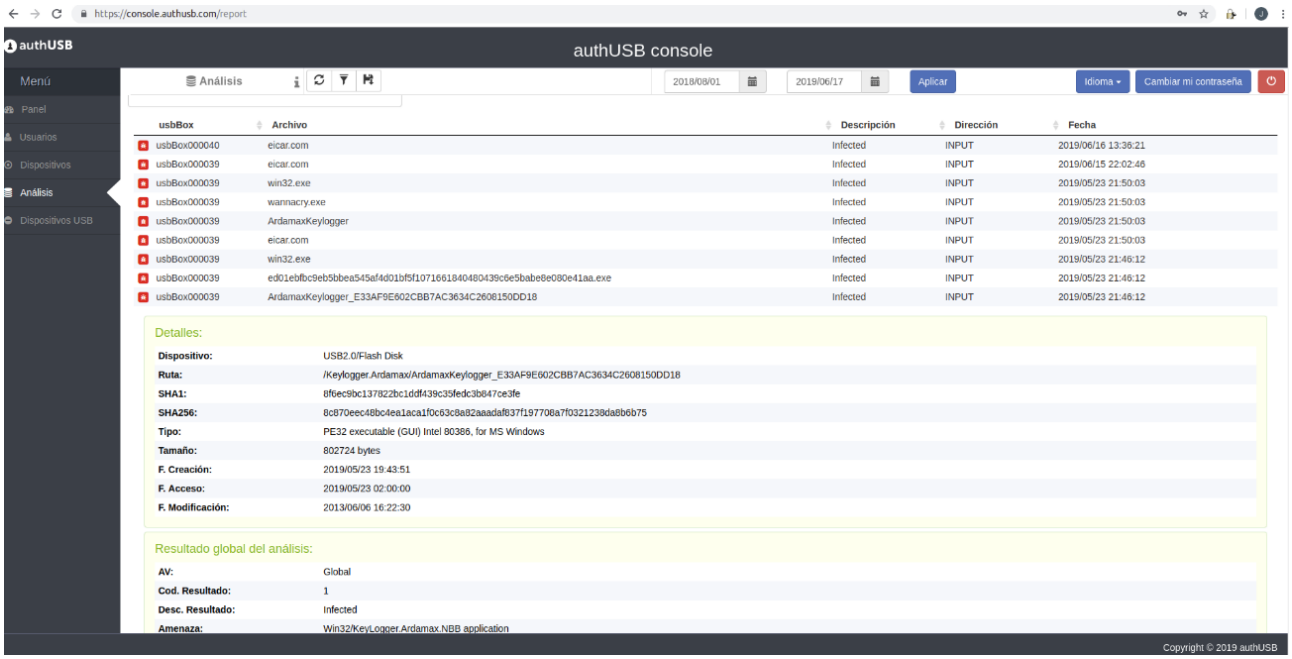
6. **Maximum number of devices to manage from a central console**

It is scalable depending on the hardware or configuration of the virtual machine on which you run. With 2 cores /16GB RAM 50 linked devices are supported

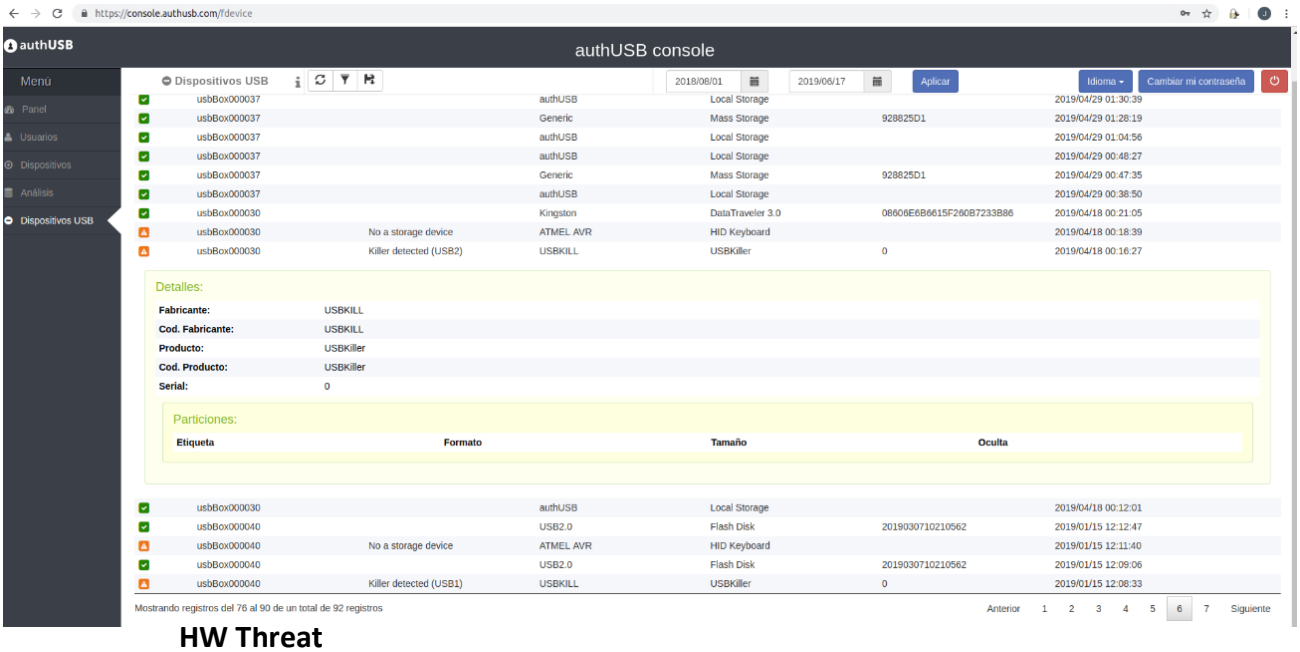
7. Central console screens



clean file capture



SW threat



HW Threat

8. Download of files

The first and mandatory step to download a file is the Software (antivirus) scan. In case of threat detection in any of the files, in no case will the user be able to download that one specificall. In case the rest of files are free of threats,the user could be able to download them:

1) Into the user PC
2) Into a USB flash drive connected to SafeDoor
3) Into a previously configured folder.