USE CASE

authUSB SafeDoor in Critical Infrastructures

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

According to the CNPIC's own definition, Critical Infrastructures are strategic infrastructures, which provide essential services and whose operation is indispensable and does not allow for alternative solutions. Therefore, their disruption or destruction would have a serious impact on essential services.

In a large part of these infrastructures where there are isolated networks (OT), they involve the use, both for their own processes and for those of third parties (updates, etc.) of USB flash drives. Within these IICCs, this use is regulated and controlled, and various solutions such as sanitization kiosks, firewalls and other elements are currently being used to comply with this control in accesses to the same.

With these solutions, USB devices are scanned at two levels, Sw and Hw

At the SW level, a static scan of the USB devices is performed, i.e. if the USB stick contains a delayed threat, they would not be able to stop it.

On the other hand, the threats at the HW level that are detected by these solutions are always based on white lists. They will not be able to detect any new threat.

In this environment, attacks on hardware (BadUSB) carried out via USB flash drives are particularly significant. This type of threat is also undetectable, persistent over time and, in most cases, irreversible.

Finally, there is the electrical threat (USB Killer), which aims to destroy the first layer of physical security in the organization and prevent the use of USB devices accessing the network. Nothing scans the computer's Hw.

The control at all levels of these devices is vital for the security and operation of the industrial chain.

What does SafeDoor*provide?

SafeDoor is a solution that analyses, protects and detects attacks via USB devices. It acts as a barrier between these and the computer equipment of an organization, taking action against the three attack vectors:

- **Electric**: It continually monitors the behaviour of the USB device at the electrical level, identifying and halting attacks by overvoltage of the usbKiller type.

- **Hardware**: It continually monitors the behaviour of the USB device at the hardware level, spotting and deactivating attacks from the BadUsb family, HID threats (rubber ducky and similar ones), false network cards, complex interfaces, etc.

- **Software:** With an integrated antivirus motor (compatible with various manufacturers) with which it carries out an analysis previous to the download or transfer of any content.

The behaviour of the USB device is monitored at all times until the extraction, avoiding in this way attacks activated via time or the number of connections, which would have passed unnoticed in an initial analysis. Because of these reasons, amongst others, a foreign USB device never should be directly connected to the organization’s equipment.

In addition to the protection of the system, it also offers audition and traceability of all the connected devices and the analyzed files.

SafeDoor offers two type A female connectors for the insertion of USB devices to analyse and an ethernet port for its connection to the web or point-to-point connection directly to a computer. Through this web connection it offers a web interface for the interaction with the user.

How does SafeDoor fit into our work and cybersecurity scheme?

1. ACCESS CONTROLS

Fully autonomous and automated 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. "FRONTERA- FRONTERA/ADUANA" USE

FRONTERA

This model allows for the dumping of the content of an untrustworthy external device in an internal trustworthy inventoried device that is authorized for its for its later connection to the internal equipment of the organization. In this way it is guaranteed that there will not be HW or electric threats and that the contents have been analysed via antivirus, providing traceability of all the files interchanged via USB.
Two different types of dedication can be given as a Frontera team:

-Automated: the scanning is carried out in a totally automatic way, both firmware and of the whole of the files contained in the USB device.
-Interactive: The check is made at Hw and Electric level and, through the web console of SafeDoor, we can choose those files that we want to analyse before downloading them.

FRONTERA/ADUANA

This model allows for the upholding of the Airgap between IT/OT networks or networks with different levels of safety rating. At the same time it also maintains the tracking of folders introduced via an internal network.

The SafeDoor equipment that is located in the internal network, will only accept inventoried USB devices that previously must be scanned by the external SafeDoor. This last one will create a digitally signed folder with a list of files ,scanned and authorized, in the inventoried USB device. During this process, the internal SafeDoor will guarantee, with a previous verification of the digital signature, that only these files are transferred. With this model, the antivirus updates for the internal SafeDoor (a laborious process in isolated networks) are no longer necessary, even when interchanging information between networks located in several sites.

3.-REMOTE TRANSFER

This model allows for a secure transfer of files to a remote location through the central console, download and dump in an inventoried USB device.

Specially designed for maintenance operations and remote configuration, it makes available to the technical experts the necessary files for its activity in a specific location. This way ensures the confidentiality, traceability, integrity and security of the information, as well as the probate of the process minimizing the possibility of human error.

SafeDoor allows the use of Encrypted USB devices at a HW level ,wich we strongly recommend, (DataLocker, Iron Key) and also Bitlocker and Luks encrypted devices SafeeDoor also includes the possibility of using digital signature of the files that are downloaded to ensure its integrity.
The traceability of the processes is total.

FAQ:

1. Maximum number of antiviruses embeded on SafeDoor*

Safe Door supports up to two simultaneous antivirus complete engines.
*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**.
- **Indirect.**
- **Ofline**.

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...)

3. 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.

4. Log storage: device, console?

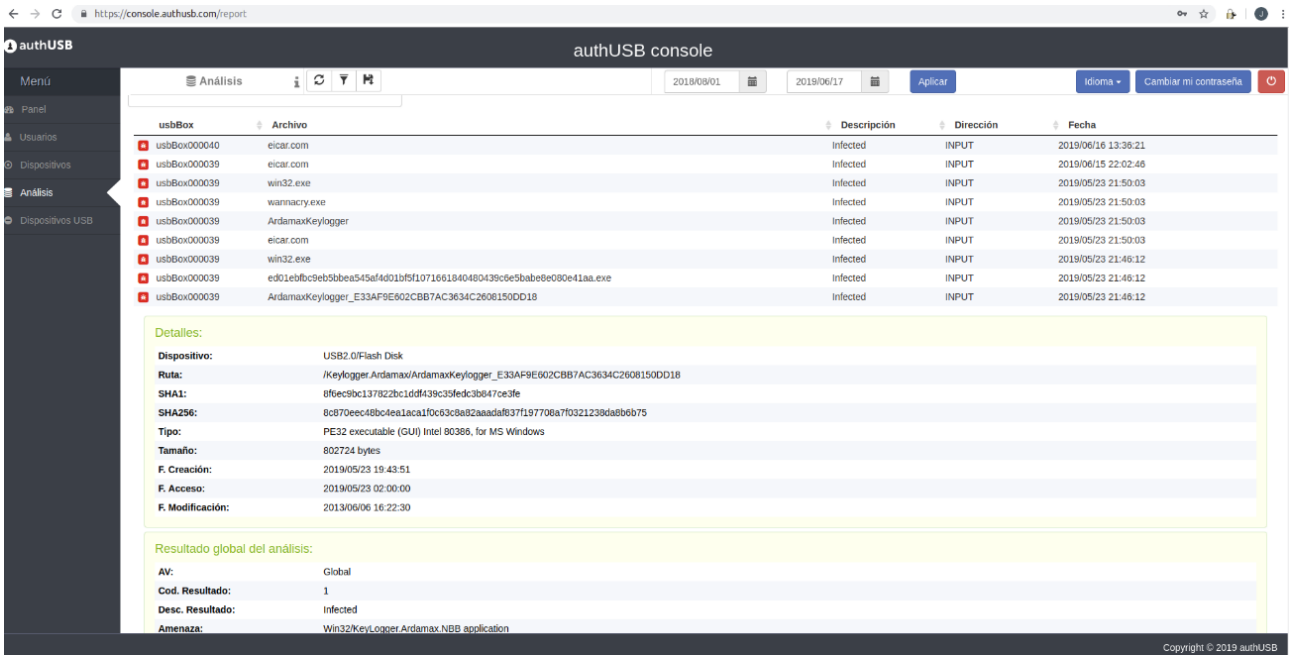
Each of the events that take place in the safedoor devices are reflected in the Central Console

- It receives the audit reports (detailed registry of the devices and files analyzed) digitally signed via the SafeDoor through an HTTPs channel.
- Through the same channel it provides firmware updates and automatic setup for all the SafeDoors. If needed it can also act as a mirror of the latest antivirus updates.
- Embeddable with an external SIEM via syslog.
- It offers a web interface to the administrators for the interaction with the system.

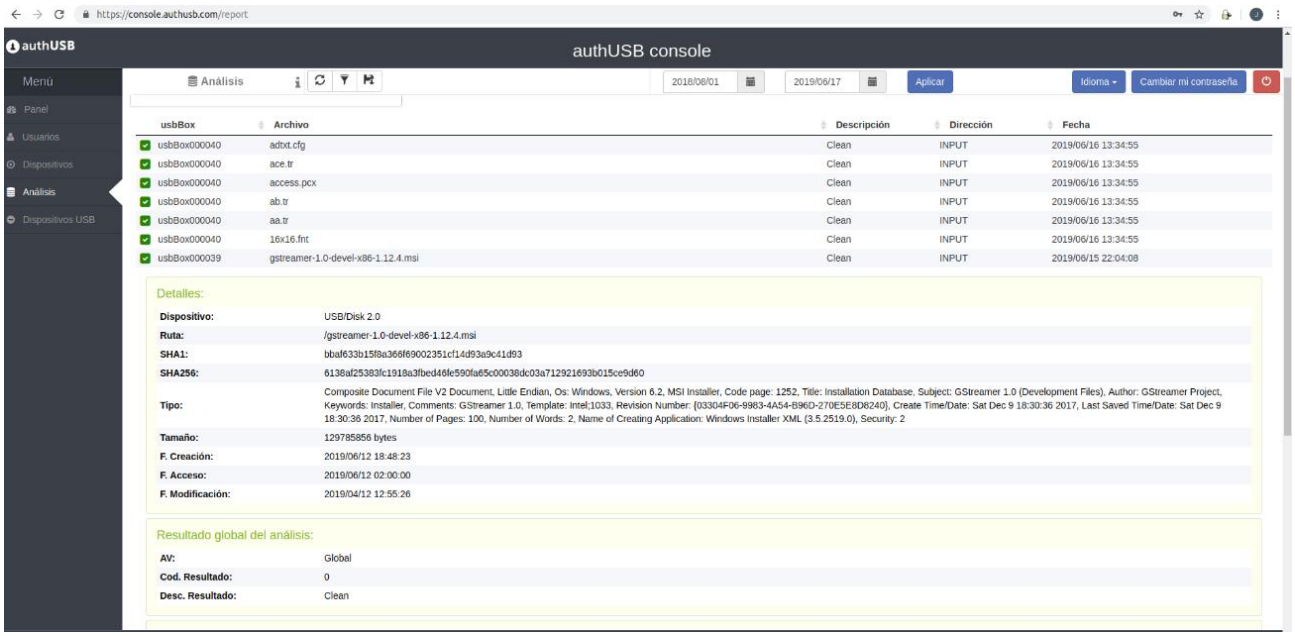
5. Maximum number of devices to manage from a central console

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

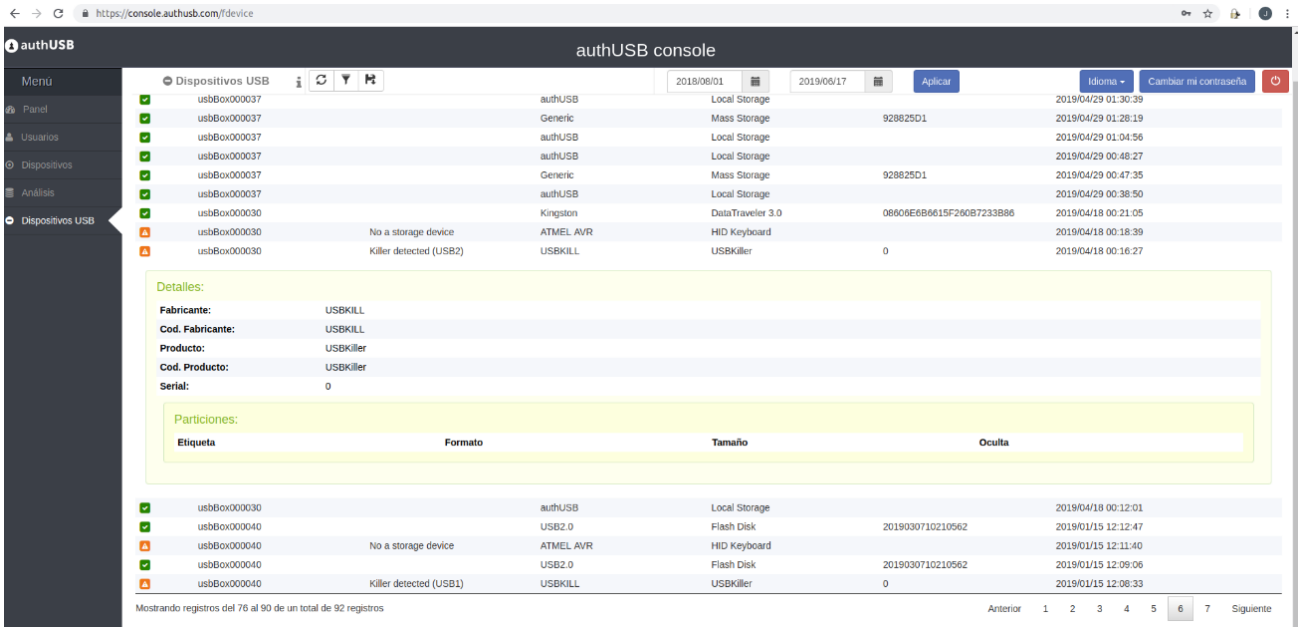
6.Central console screens



clean file capture



SW threat



HW Threat

7. 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.


PRODUCTO SEGURIDAD TIC
CCN
CUALIFICADO
ens
ALTA