USE CASE

authUSB SafeDoor for Financial and related sectors

What is the specific problem of these Sectors regarding USB devices?

" Banks are focusing more resources and attention than ever on cybersecurity. However, cybersecurity issues continue to grow, fuelled by determined, well-funded, sophisticated adversaries—and by a world that is increasingly interconnected and digital."

This true affirmation is an extract from, 2020 Banking Regulatory Outlook paper by Deloitte.

In the financial sector, compliance with specific regulations, as well as another more cross-cutting type, affecting any sector such as the GDPR, are critical.
It is very important to take into account, given the confidentiality of the data that is handled, the cases of data extraction by internal actors .In some cases this is due to negligence or internal neglect and in others to an attempt to use it in a new work or for sale.
Financial analysts need to move critical information both internally and outwards, not forgetting the need to keep it protected and under control.
In this sector there are types of highly sensitive information, which are critical to keep under control. Examples include:

- **Customer Data:** Financial services clients assume that their confidential information is secure in the hands of financial firms. Any leakage of this information can seriously damage the customer.
- **Regulated Information:** Data that must be audited mandatory.
- **Internal reports, confidential financial analyses** of a strategic nature for the organization.
- **Management Documentation, Executive Board** that is restricted to a specific group within the organization.
- **Information related to high critical money laundering** and access to which must be thoroughly controlled.

In both central offices and bank branches, USB devices are used not only for internal use. There is not a precise protocol for its use. On many occasions on those organizations ,the decision of disabling the bios of the USB ports is taken, wrongly believing that once the data clips of the USB ports have been disabled, the threats doesn't exist anymore . Nothing further from reality.

HW (badusb) and Electrical (Usb killer) threats remain active.

What does SafeDoor provide?

SafeDoor is a solution that analyses, protects and detects cyber 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 your work scheme?

1. MANAGEMENT POSITIONS

SafeDoor directly connected to the computer equipment, exercising the single entry point of any USB storage device. It also prevents any information from being extracted by this means without prior authorization. In this case, this extraction is audited through the Central Console, stating who, when, where it occurs, and what kind of information is being leaked.

2. CENTRAL OFFICES AND BRANCHES.

Networked, the SafeDoor serves each department, consisting of a previously determined number of workplaces. The administrator mode will allow to individually register the users or it may be able to integrate the organization's LDAP. Once this is made, the administrator may also manage the two USB ports of SafeDoor, stablishing one of them for each group of users. SafeDoor will perform the analysis of the USB storage devices used by the staff.

For its shared use, by different user, the system supports the explicit reservation in advance of each of the ports, so that the confidentiality of data content is guaranteed.

In all cases, the deployment of Safe Door also prevents internal information leaks through USB storage devices. There is the possibility of allowing it, under a strict protocol and with the appropriate permissions within the organization and this extraction is always audited through our Central Console.

ANSWERS TO SPECIFIC QUESTIONS

1. **Maximum number of antiviruses* to install on device**

   Safe Door supports up to two simultaneous complete antivirus engines

   *We can integrate more than two if necessary

2. **Way to update antiviruses.**

There are three methods of updating signatures, depending on the place where is deployed:

- **Direct**.
- **Indirect.**
- **Offline**.

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, although it continues to be continuously monitored until it is extracted. As for software scanning (antivirus) there are two modes of use:

- **Manual:** From a web browser, the user selects the files/folders to download. On these selected files, analysis is carried out by the antivirus (selective analysis)
- **Automatic**: Anti-virus scanners all the contents of the memory reporting through Leds 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 memory 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.

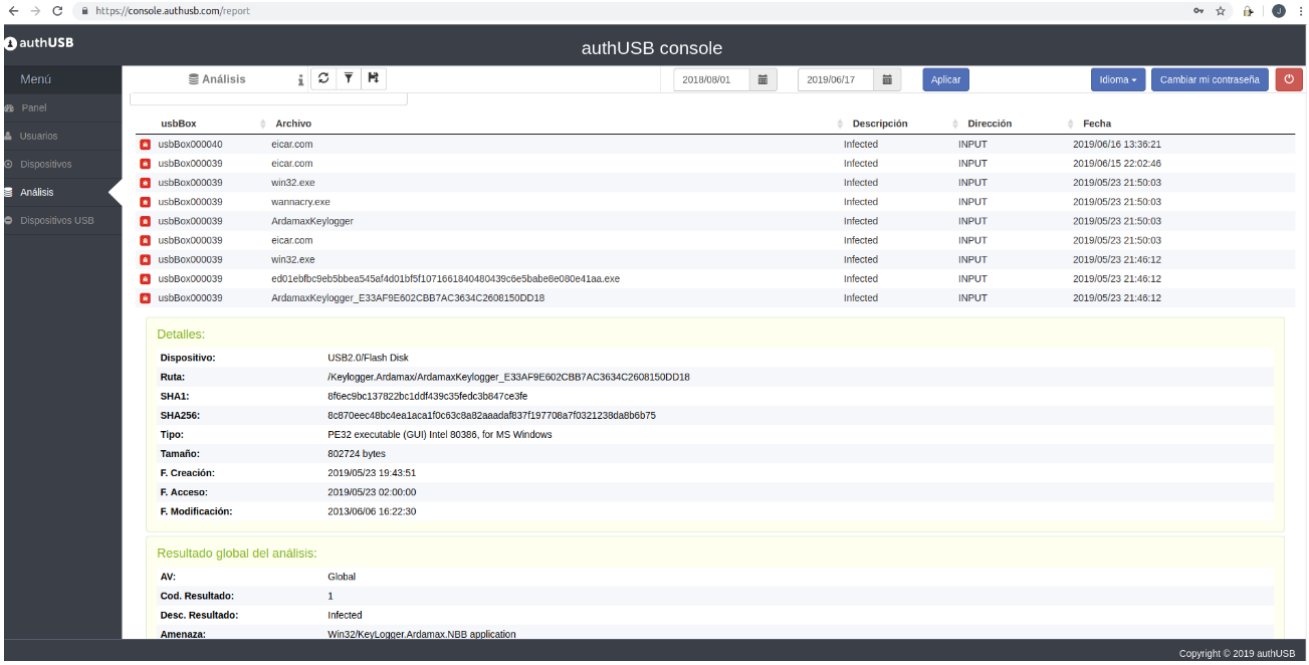
5. **Log storage: device, console**

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

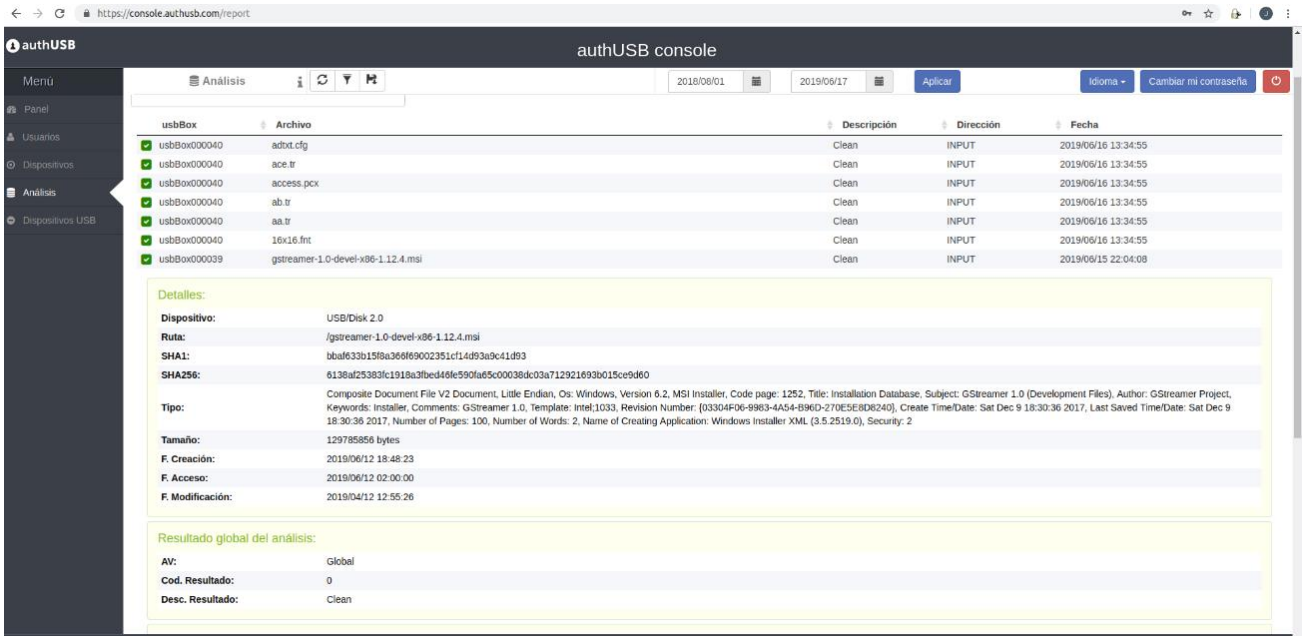
- It receives the audit reports (detailed registry of the devices and files analyzed) digitally signed via the SafeDoor through an HTTPs channel.
- Through the same channel it provides firmware updates and automatic setup for all the SafeDoors. If needed it can also act as a mirror of the latest antivirus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

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.

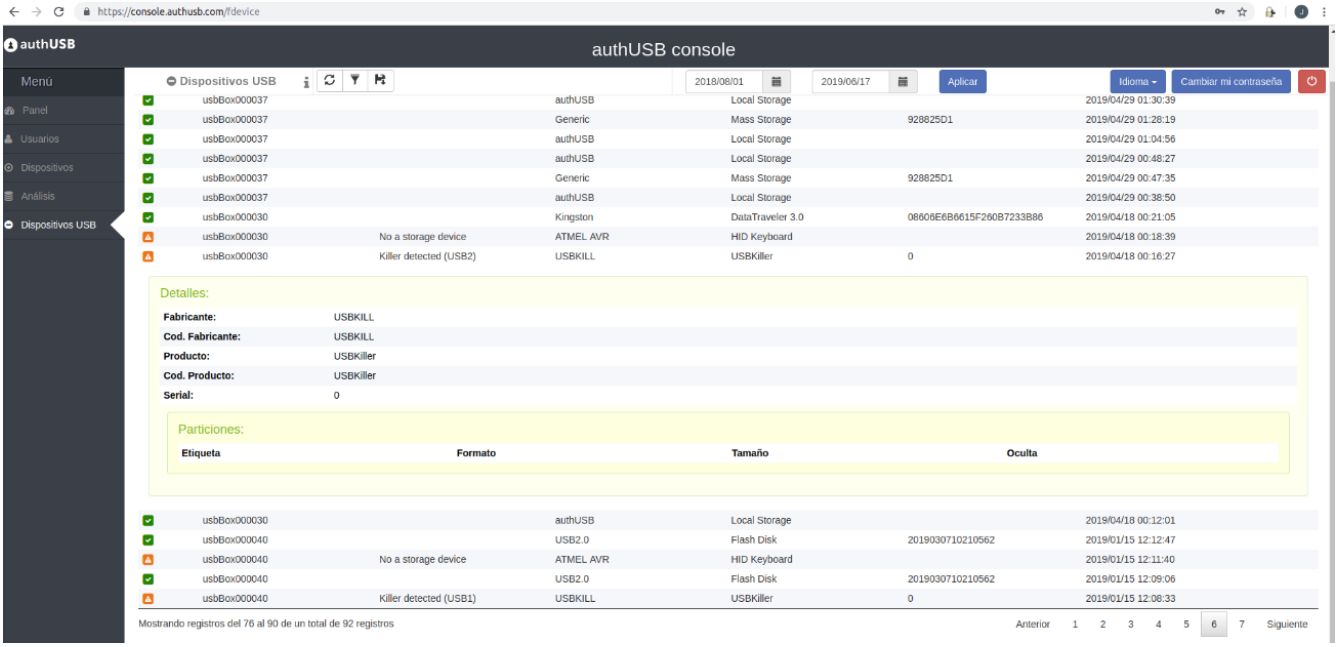
7. **Central Console screens**



CLEAN FILE



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.