USE CASE

authUSB SafeDoor for Financial sector

What is the specific problem of Financial Sector 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 is SafeDoor?

SafeDoor is a Hw device with embedded SW that acts as a barrier between USB sticks and an organization's computers by analyzing, blocking, informing, auditing and managing threats 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 behavior 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

SafeDoor is certified under the Lince methodology and is part of the CCN, CPSTIC catalog.

*Protected under patent

How does SafeDoor fit into your work scheme?

1. SENIOR MANAGEMENT

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.

In the case of branches, as in the Central departments, SafeDoor is the ONLY WAY OF ENTRY of USB devices into the organization. SafeDoor carries through a triple analysis at the three levels (Electrical, Hw and Sw) of the USBs managed by the staff,(both, for internal use and those that customers delivered with their information)

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 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. Way to update antiviruses.

There are three methods of updating signatures, depending on your 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.
- **Offline**. 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, 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.**

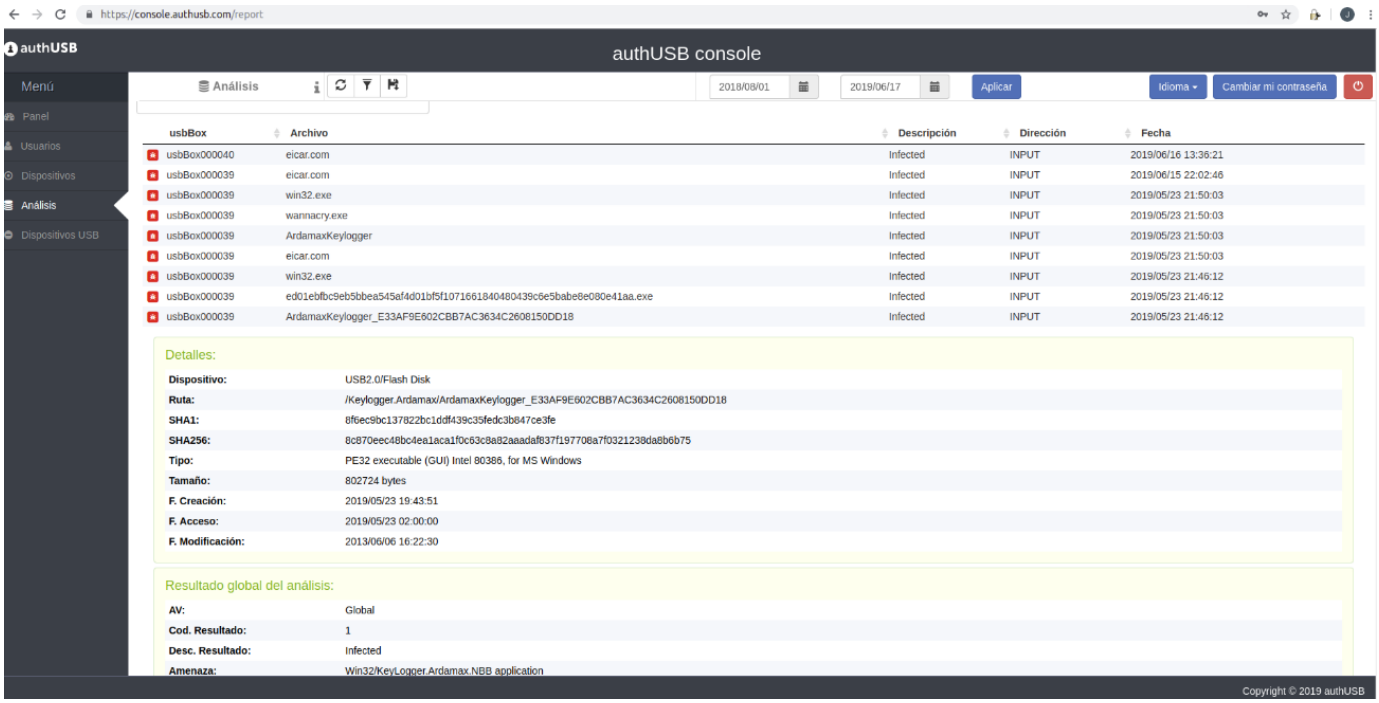
The scanning time is similar to that of a desktop computer, since the bottleneck is at the reading speed of the USBstick. With modern memory read speeds of about 35 MB/s can be achieved, while with advertising memories or degraded by usage the speed can drop to 15/20 MB/s.

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

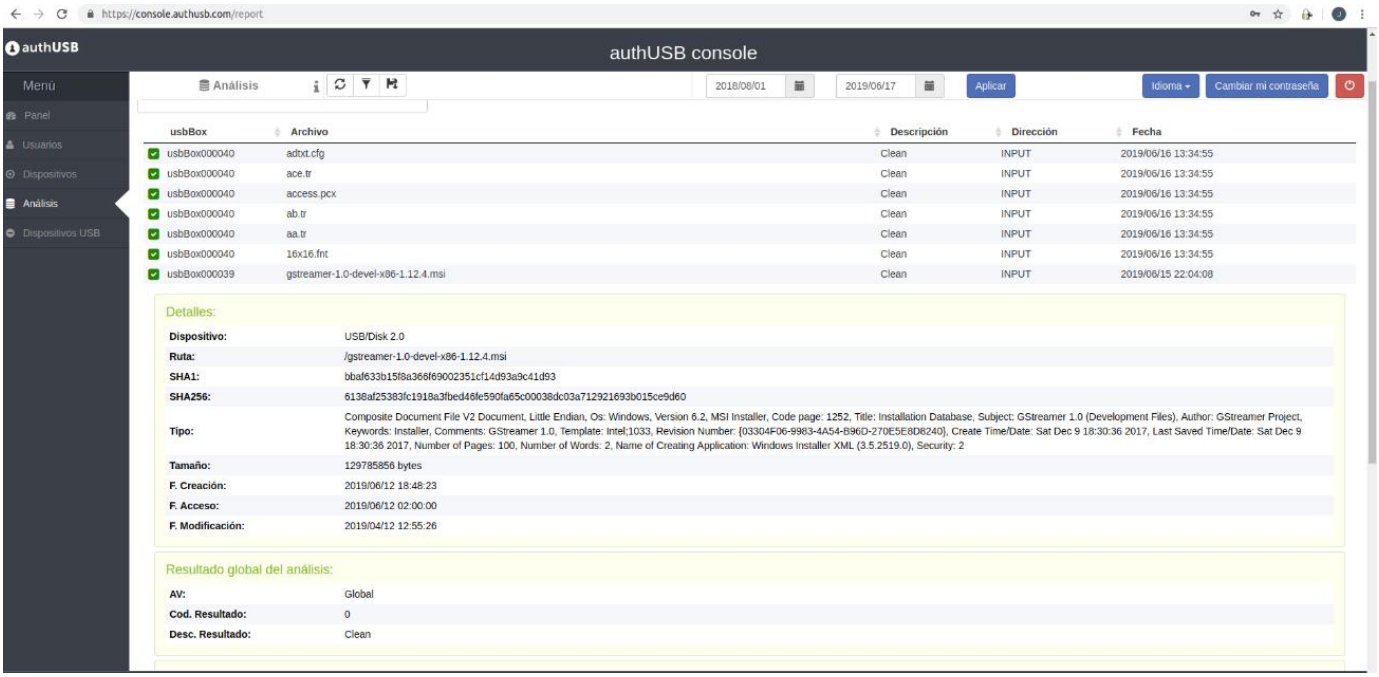
Each action performed on each safeDoor is dumped in real time onto the Center Console. In case of loss of connectivity or isolated computers these reports will be stored on the device, being possible to download (digitally signed) for subsequent loading to the central console manually through its web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

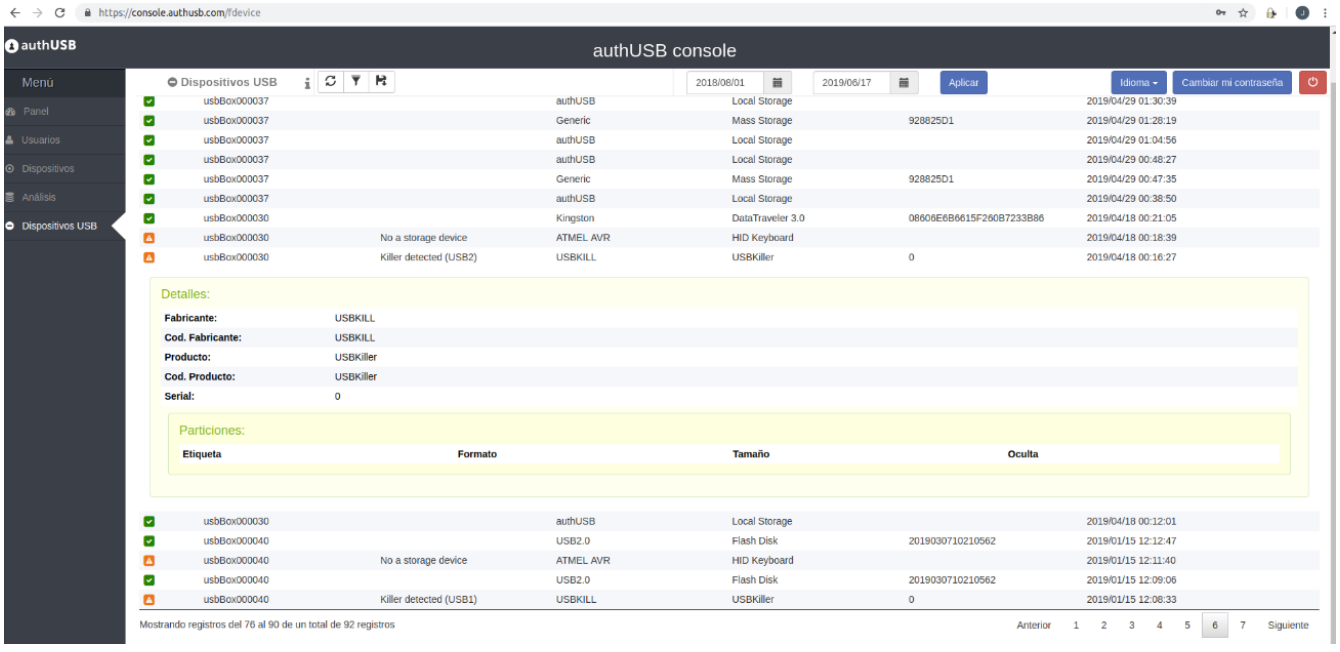
7. **Central Console screens**



CLEAN FILE



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.