Press Release
Paris, 22 March 2018

Orange Cyberdefense launches new mobile decontamination terminal for USB flash drives

- USB flash drives are second most dangerous source of cyber-threats
- Mini-terminal Malware Cleaner detects "BadUSB" threats that are undetectable with traditional anti-virus software
- Malware Cleaner is available around the world

Seventy percent of employees use USB flash drives from outside the company and connect them to the company network, and 68 percent take no precautions before inserting them into their work computer[1].

USB flash drives, whether they are new or used, are major sources of infection for company IT systems. They are in widespread use, particularly in certain sectors such as in industry, education and healthcare, both for sharing documents and for updating software.

A new mobile terminal to remind people to decontaminate USB flash drives
Available until now as a fixed 70kg booth or as a software version installed on computers, the Malware Cleaner solution is now available in a “mini-terminal” version. Thanks to this cheaper, mobile version, businesses can facilitate the decontamination of users’ USB flash drives. This portable version can be found at a reception desk, in meeting rooms or even shared between different sites as needed.

Five integrated anti-virus search engines to detect threats
Orange Cyberdefense experts and their “ethical hacking” teams developed Malware Cleaner. Quick and easy to use, all you have to do is insert the USB flash drive to find out if it is has been infected. If it has, the user can choose to delete the file or put it into quarantine. It is also possible to print off a report for a more detailed analysis of the flash drive: infected files details, signature of detected attack, and the name of the anti-virus search engines that detected the infected file.

Malware Cleaner simultaneously uses five anti-virus search engines to optimize and combine the extent and performance of detection. These search engines are automatically updated on a daily basis when the terminal is connected to the internet via the network or using 4G. By the end of the year, two additional anti-virus search engines will be added to Malware cleaner.
It also has an embedded detection engine for BadUSB type attacks that are undetectable by traditional anti-virus software, which can take control of the computer.

[1] source: Ponemon Institute, 2014

In addition, Malware Cleaner includes an admin platform to remotely manage the terminals. This allows to check they are running accurately and being updated, to receive usage statistics in real-time, find out the number of infected files and the types of attack detected. All this precious information helps to improve the company's cybersecurity.

Industry, an exposed sector

In the industry sector, the computers used to control production lines are not connected to the internet for security reasons. The USB ports on these machines are therefore regularly used to carry out maintenance diagnostics and recover SCADA logs, or to carry out updates. This makes them particularly vulnerable to attacks via USB flash drives. Thanks to the Malware Cleaner software solution installed on a computer located at the entrance of the production area, and the addition of a security protocol that makes it compulsory to check all USB devices on this specific computer, the production line is protected from USB flash drive attacks.

"USB flash drives are a real danger for IT security within companies. Even if these attacks are more complicated to set up than attacks by e-mail, for example, they are nevertheless to be feared. Introducing USB flash drives into the heart of the company makes it possible to spread malicious code, paralyze machines, destroy sensitive data and even workstations. Ransomware can be installed on an industrial system simply by inserting a USB flash drive, with no need for the user to do anything at all," says Alexis Richard, Product Manager at Orange Cyberdefense.

Best practices for USB flash drive use

- Never connect a USB flash drive of unknown origin to a workstation
- Renew employees' USB flash drives to avoid the propagation of malware
- Provide employees with USB flash drives to prevent the use of external equipment
- Systematically check USB flash drives when they have been connected to an unsecured environment
- Only connect decontaminated flash drives to industrial computers

Press contact:

Orange : Nathalie Chevrier : + 33 1 44 44 93 93 ; nathalie.chevrier@orange.com
Orange Business Services: Caroline Cellier ; + 33 1 55 54 50 34 ; caroline.cellier@orange.com