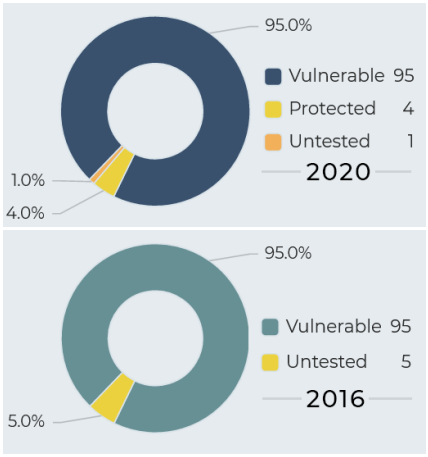
USBKill.com releases V4: Optimised for penetration testing, law-enforcement.
https://youtu.be/N-gsVm817Pc

Since 2016, USBKill devices have been used by security, industrial and law-enforcement clients world-wide to test, harden and protect hardware and infrastructure across multiple industries:

- Aerospace: In-flight entertainment systems, critical flight systems
- Infrastructure: Electronic systems to critical public infrastructure
- Consumer Electronics: Personal computing, mobile telephones, televisions, etc
- Medical Hardware: Critical support systems, hospital infrastructure
- Law-enforcement: LEA and government clients across 25+ countries
- Penetration Testing: White-hat auditing of commercial and industrial electronic systems

Insight: Devices with USB Vulnerabilities, 2016 vs 2020



Notable USBKill clients and partners include:

The USBKill is a device that stress tests hardware. When plugged in power is taken from a USB-Port, multiplied, and discharged into the data-lines, typically disabling an unprotected device.

The USBKill V4 caters specifically to industry needs: significantly more powerful, more flexible, more covert and more compatible - providing multiple modes of operation, fully-wireless functionality and field-kits tailored to meet the requirements of professional clients. More information can be found here: https://youtu.be/N-gsVm817Pc

Notably, the USBKill V4 has the ability to bypass current USB-C and Lightning security measures - both Samsung and Apple flagship devices still have vulnerabilities via their USB ports.

The USBKill V4 devices are made available through **USBKill.com**