USBKILL

For immediate release
For more information contact: Steve BENSON - support@usbkill.com

USBKill V4 Takes Computer Hardware and Smartphone Testing Next Level to Protect Critical Functions Across Law Enforcement and Essential Industries

HONG KONG - - - September 15 2020 - - - Computers are an integral part of modern culture, allowing for previously unimagined advances and relied on by essential organizations around the world. Yet when they fail, the repercussions can be monumental. Even catastrophic. Hardware testing helps ensure that does not happen. That's where USBKill V4 comes in. It's the newest version of the device most relied on for testing and protecting hardware by industries that can't afford to fail.

First introduced in 2016, USBKill has become the global standard in stress testing hardware. It is used to safeguard computers in the aeronautical, law enforcement, public infrastructure, medical and consumer electronic realms. Its clients and partners include megabrands like IBM, hp, CISCO, SAMSUNG, AIRBUS and Panasonic. Version 4 is being touted by the makers as more powerful, with more attack modes, more covert, tests for everything from iPhones to HDMI to USB-C and more; and will not miss targets, even for devices powered down.

"USBKill has evolved beyond the original plug-and-zap device. The new V4 hardware framework not only has more powerful discharges and improved stability, it also has an internal, rechargeable battery, for offline attack tests for where the host device is not turned on," explained Steve Benson, CTO of USBKill. "The Offline Mode even bypasses all known USB-C and Apple/iPhone security protocols. In other words, the V4 is the ultimate device for testing smartphones and modern hardware."

Probably most notable about the V4 device are the advanced attack modes and extensive test accessories and adaptors. Attack modes now include single pulse and continuous pulse options, meaning it will not activate until triggered to give pentesters and law enforcement agencies complete discretion. Likewise, the V4 can be triggered via remote trigger, smartphone trigger, timed attach, magnetic attack, magnetic trigger or classic mode.

As to accessories and adaptors, V4 offers a variety of new choices to help prepare for any situation. Its accessories open a broad attack surface for pentesters, covering all possible types of hardware, including smartphones, computers, laptops, printers, televisions, network equipment, USB drives and external hard drives. The V4 Tester in fact acts as a multi-function shield device, providing high-voltage protection and juice-jacking protection while the V4 Adaptors include both basic and advanced versions. Basic Adaptors apply to USB-C, iPhone, MicroUSB, MiniUSB and USB-A Female; and the Advanced Adaptors apply to USB-B Male, USB-B Female, VGA (DB15), HDMI Male, HDMI Female-Female, DisplayPort Male, DisplayPort Female-Female, RJ45 Male and RJ-45 Female.

"USBKill is always thinking several steps ahead to help organizations prepare for any scenario and avoid profound risks. Critical flight systems, hospital infrastructure, law enforcement, public electronic systems and much more need to be able to rely on their hardware. We help make sure they can with V4," stressed Benson.

For more information and to order USBKill V4, go to usbkillv4.myshopify.com.