BusKill Cable Starts a Self-Destruct Routine on Stolen Laptops

By **Ionut Ilascu** January 4, 2020 01:05 PM 6

A USB cable and some scripting can save sensitive data on your laptop from grab-and-go thieving situations when working in a public place.

Linux system administrator and software engineer Michael Altfield designed a kill-cord called BusKill that can trigger a specific action when it gets disconnected from the laptop.

He came up with the idea after searching for a simple, low-tech solution to cause the computer to lock, shut down, or self-destruct when it is physically separated from the owner.

In essence, BusKill is a cable with a USB drive at one end that attaches to your body and your laptop at the other. When the drive disconnects, it acts on a predefined 'udev' event, which can be anything from locking the computer, shutting it down, or wipe data on it.

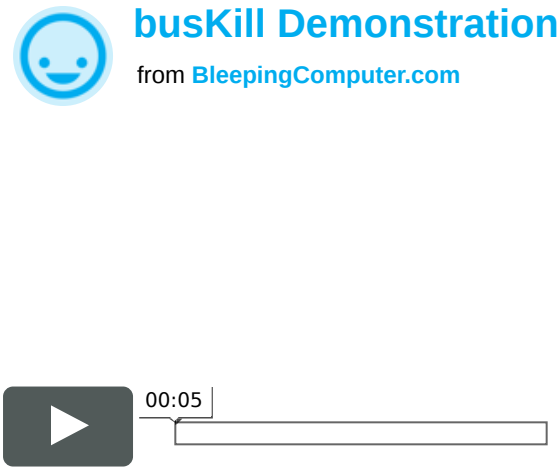
Altfield spent about $20 to build BusKill but this depends on the quality of the items you choose. A USB drive, a magnetic adapter, a carabiner, and a USB extension cable are the hardware essentials.

source: Michael Altfield

Nothing needs to be stored on the USB storage since only its presence is required for the kill cable to do its job; so it can be a cheap device as long as the system recognizes it.

A script that triggers the action is the software part. It can spring into action only when a specific drive is removed by adding uniquely identifiable properties (manufacturer, filesystem UUID, model).

Below is a video showing BusKill in action:



The scenarios Altfield envisages for using BusKill involve working on your laptop in a public space and being logged into services that offer access to sensitive information, like online banking or the company VPN connection.

Altfield argues that despite taking precautions like two-factor authentication, VPN, or password managers, someone that steals your laptop after having authenticated is a plausible risk that some individuals should consider.

BusKill is not available for sale but Altfield provides all the details needed to build your own.

The project sparked a rich discussion on Reddit about how the scenarios thought by Altfield are not at all far fetched and do happen in real life.

The community also came up with other solutions that would protect the data on the laptop. More elaborate ones could destroy the encrypted files on the storage drive when a specific password was entered and boot normally into the operating system.

Following these discussions, the Linux sysadmin is now thinking of writing a follow-up tutorial on expanding the BusKill capabilities to run a destructive wipe of the content in

the computer memory and the LUKS (Linux Unified Key Setup) header instead of the entire encrypted disk.

This approach would make the process faster and more effective because the LUKS header contains the symmetric keys required for decrypting the entire disk. "Wiping the whole drive is unnecessary and would take too long," Altfield told BleepingComputer.

Related Articles:

Linux warning: TrickBot malware is now infecting your systems

KDE archive tool flaw let hackers take over Linux accounts

Sneaky Doki Linux malware infiltrates Docker cloud instances

Windows 10 Desktop Windows Manager crashes due to DirectX bug

Linux-based malware analysis toolkit REMnux 7 released

BUSKILL LAPTOP LINUX UDEV USB USB DRIVE

IONUT ILASCU

Ionut Ilascu is freelancing as a technology writer with a focus on all things cybersecurity. The topics he writes about include malware, vulnerabilities, exploits and security defenses, as well as research and innovation in information security. His work has been published by Bitdefender, Netgear, The Security Ledger and Softpedia.

PREVIOUS ARTICLE NEXT ARTICLE

Comments