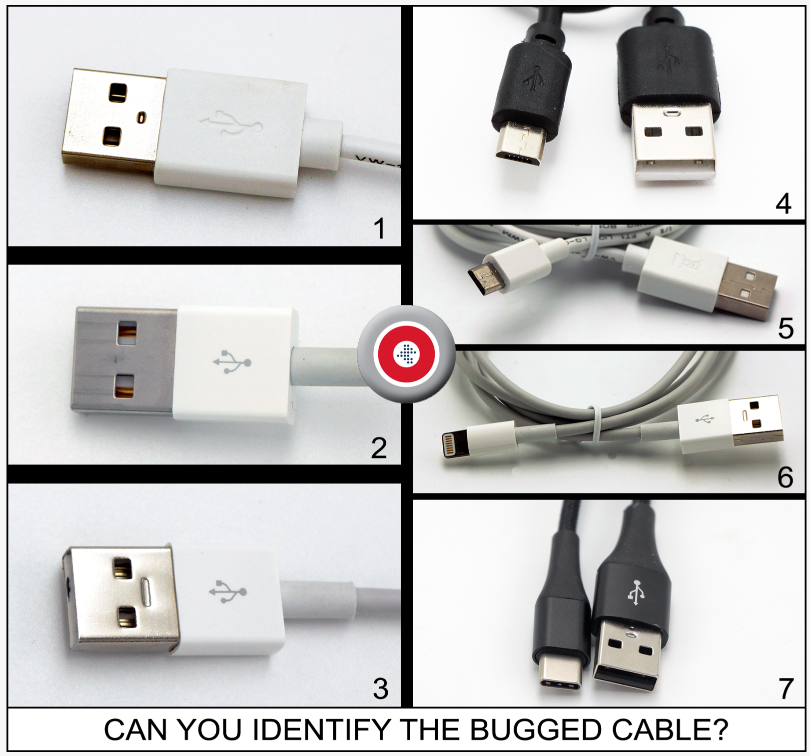
EINPRESSWIRE

Malicious USB Spy Cables Detected by Murray Associates TSCM

Sharp spike in internet sales of USB spy cables has corporate security and IT directors concerned. Murray Associates researched and developed a solution.



OLDWICK, NEW JERSEY, USA, October 20, 2020 /EINPresswire.com/ --
• Malicious USB cables look exactly like the real thing.
• Some act as eavesdropping bugs.
• Some have GPS tracking capability.
• The worst ones take control of a user's cell phone, laptop, or desktop.

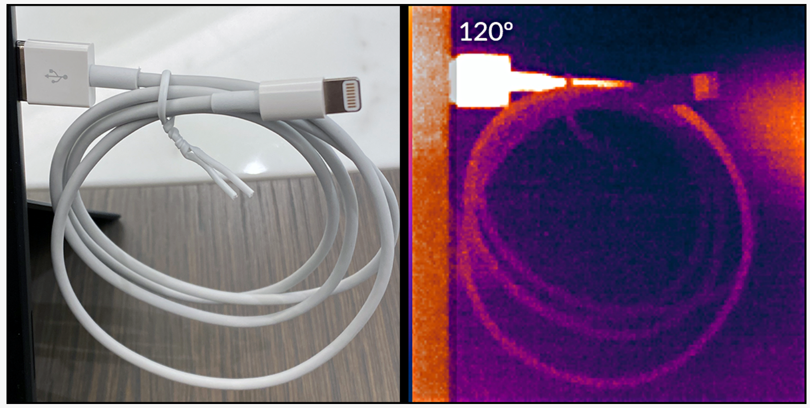
A malicious USB cable is any cable which performs an unexpected, and unwanted function. Data exfiltration, GPS tracking, and audio eavesdropping are the primary malicious functions Murray Associates TSCM discovered in their tests.

Murray Associates, a firm specializing in corporate counterespionage, noticed internet sales of these spy cables spiked this year. "The quality of these spy cables is amazing. Some are absolutely indistinguishable from the real thing just by looking," said Kevin D. Murray, the firm's Director. "Through testing we developed electronic detection techniques. This new protocol is now part of the Technical Surveillance Countermeasures (TSCM) inspections we conduct for our clients."

Spy cables are very dangerous in a business environment. Placement is easy. Once in place they won't be suspected. Discovery is impossible without inspection.

The worst malicious USB cables allow control of a user's cell phone, laptop, or desktop by a remote hacker. This silent spying is of particular concern to corporations because this initial connection is often used as a pivot point to attack other machines and databases on the network. The hacker roams unnoticed on the network. Motives range from corporate espionage to instigating a ransomeware attack.

Some cables have an Achilles Heel. They become slightly warm when plugged into an active USB port. “We can easily see this using thermal imaging. Some people can detect it by touch. However, all USB cables should be considered suspect until we electronically test them,” said Murray.



Infrared Photo of Malicious USB Cable

Malicious USB Spy Cable Internet Ad

The first malicious USB cables began life as an NSA-created spy tool under the code name [COTTONMOUTH] in 2008. The government paid a lot for them. Their cost for a spy cable was $1,015.00 each, in quantities of 50. Now, malicious USB spy cables are universally available at a fraction of that cost; some costing less than $10.

Can’t identify the bugged cable? No worries. You can’t tell just by looking. That’s why we put a small black mark on it. It is Cable 3.

> “
> Electronic eavesdropping and corporate espionage are covert activities. You need to inspect to detect. TSCM inspections are cheap insurance, but better. Insurance can't prevent the loss.”
>
> *Kevin D. Murray, CPP, CISM, CFE*

Malicious USB spy cables are only one corporate espionage trick spies use. There are many more. If your organization is concerned about electronic surveillance, information loss, or intellectual property theft, the counterespionage specialists at Murray Associates can help you.

In case you are interested in actually seeing malicious USB cables for sale, here are a few links… The o.mg cable. Alibaba

——

Kevin D. Murray CPP, CISM, CFE is a business counterespionage consultant and TSCM specialist with over four decades of experience.

Murray Associates is an independent security consulting firm, providing eavesdropping detection and counterespionage services to business, government and at-risk individuals.

Headquartered in the New York metropolitan area, a Murray Associates team can assist you quickly, anywhere in the United States, and internationally.

Kevin D. Murray
Murray Associates - TSCM
908-832-7900
tscm@counterespionage.com
Visit us on social media:
LinkedIn
Twitter
