Murray Associates | Security Report

Malicious USB Cables

by Kevin D. Murray, CPP, CISM, CFE

Definition

A malicious cable is any cable (electrical or optical) which performs an unexpected, and unwanted function. The most common malicious capabilities are found in USB cables. Data exfiltration, GPS tracking, and audio eavesdropping are the primary malicious functions.

Background

The first malicious USB cables began life as an NSA-created spy tool under the code name COTTONMOUTH in 2008.[1] The government paid a lot for it. The cost for their spy cable back then was $1,015.00, in quantities of 50. Now, they are a fraction of that cost.

Capabilities

The general expectation is that a cable performs no other function than to transfer energy and/or information (electrically or optically) between two points.

Malicious USB cables do much more.

- **Some act as eavesdropping bugs** which can automatically record calls. Or, call a pre-programmed phone number, whenever voices are heard. They draw their power from whatever they are plugged into, and use the cellular phone system to make the call.
- **Some also have GPS tracking capability**; perfectly crafted for vehicle surveillance.
- **The worst malicious cables take control of a user's cell phone, laptop, or desktop.**

User names and passwords are the first bits to go. Next, the connected device's storage is emptied.

Next, pre-loaded penetration tools spring into action. The connection is used as a pivot point to attack other machines and databases on the network.

All of this is controlled remotely by an outside hacker, via Wi-Fi to internet or nearby smartphone. The hacker roams unnoticed on the network, motives unknown.

Once the hacker has infiltrated the network. More data can be extracted, viruses planted, or a ransomware attack staged.

This is dangerous in a business environment.

All this from an innocent-looking USB cable!

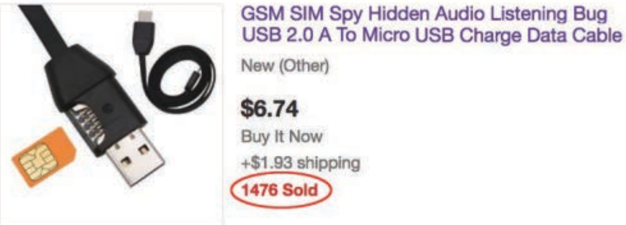
[1] https://nsa.gov1.info/dni/nsa-ant-catalog/usb/index.html

Malicious USB Cables

by Kevin D. Murray, CPP, CISM, CFE

Threat Assessment

1. Most look ***exactly*** like regular USB cables.
2. They are openly sold on the internet.
3. Costs range from $6.74 to $119.99.



GSM SIM Spy Hidden Audio Listening Bug USB 2.0 A To Micro USB Charge Data Cable

New (Other)

$6.74

Buy It Now

+$1.93 shipping

1476 Sold

4. Placement in an office environment is easy.
5. Once in place they won't be suspected.
6. Discovery is impossible without inspection.

Sometimes these "value added" cables are sold as legitimate *penetration testing* tools. Unfortunately, sales are not restricted to just legitimate cybersecurity practitioners. Other times they are openly advertised as *spy cables.*

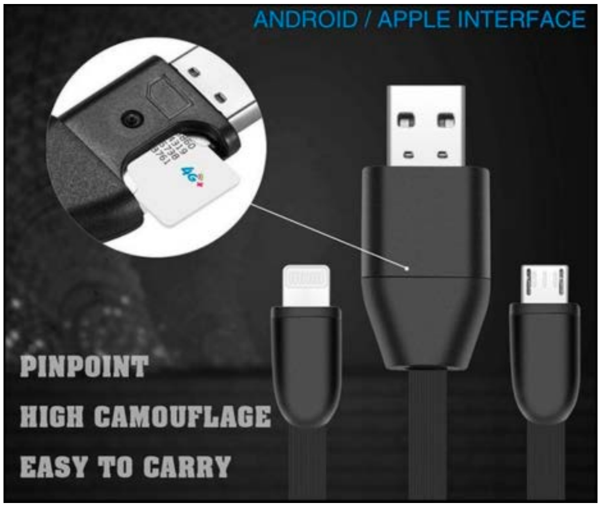
Our Solution

In light of today's serious ransomware attacks and corporate espionage attacks, businesses need a way to inspect for this threat.

1. Murray Associates researched the problem.

2. We purchased and tested several malicious USB cables. From what was learned during these tests our technical staff developed several new inspection protocols.

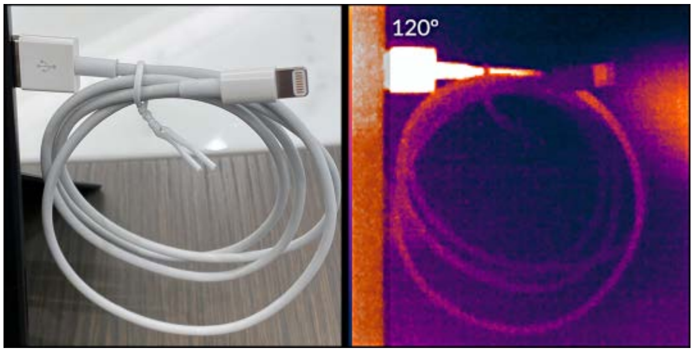
   One of our inspection methods uses an infrared camera to detect heat. As shown on the right, the heat given off by an active malicious USB cable can be easily seen using this detection technique.



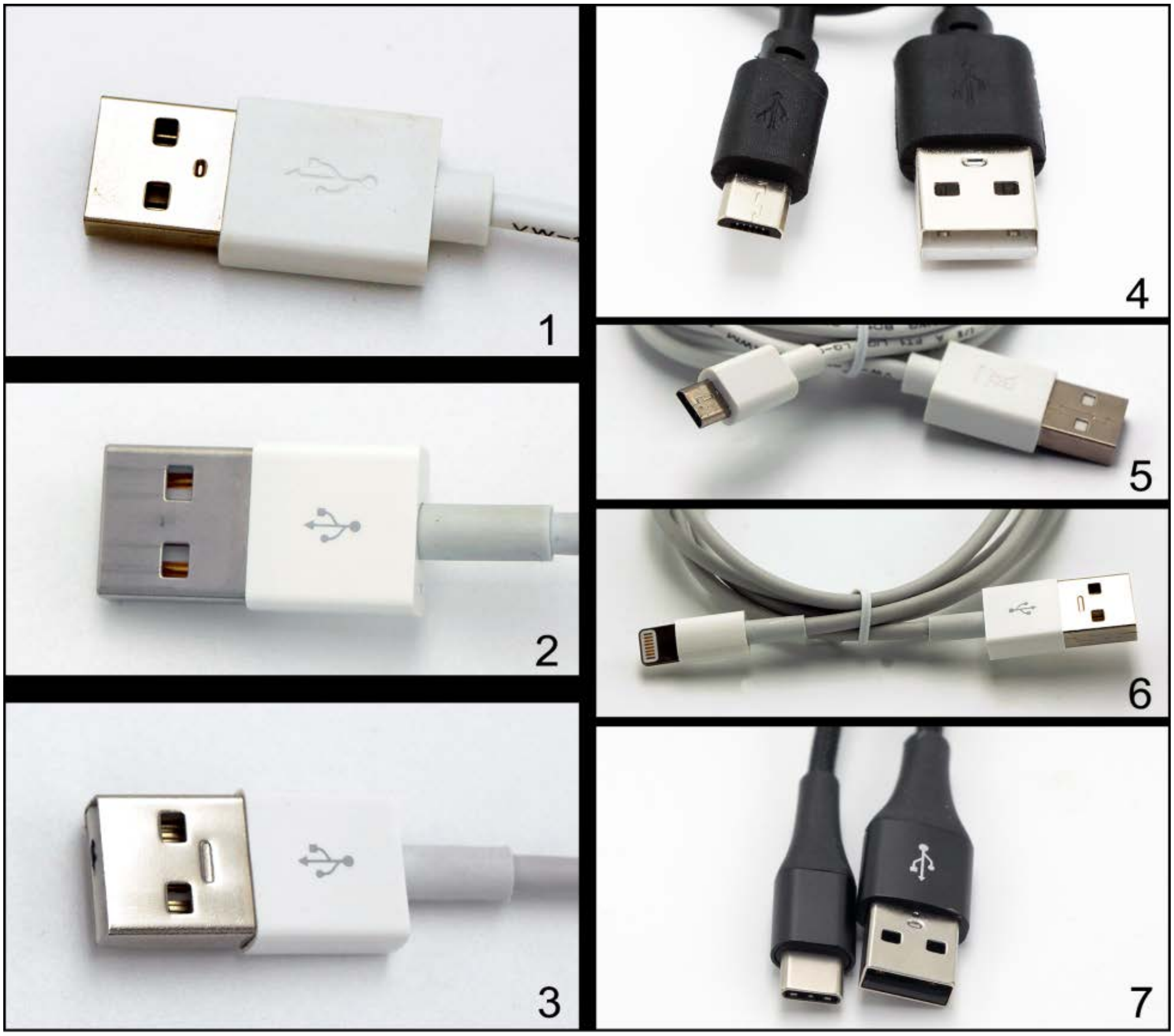
3. **Cables plugged into devices which are turned off, or are just laying around, require our alternate test procedures.**

4. The testing procedures we developed have been added to our Technical Surveillance Countermeasures (TSCM) inspection process.

5. Upon completion of a TSCM evaluation we teach clients how to quickly vet new USB cables entering their environments in between our visits.



Note: Malicious USB cables do not have to be attached to anything other than an active USB port or power supply to do their dirty work.



CAN YOU IDENTIFY THE BUGGED CABLE?

No worries. You really can't tell just by looking, even we can't. That's why we had to put a small black mark on it. It is Cable 3.

Kevin

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

Murray Associates[2] is an independent security consulting firm, providing eavesdropping detection and counterespionage services to business, government and the at-risk individual.

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

[2] https://counterespionage.com/about-murray-associates/electronic-eavesdropping-detection/