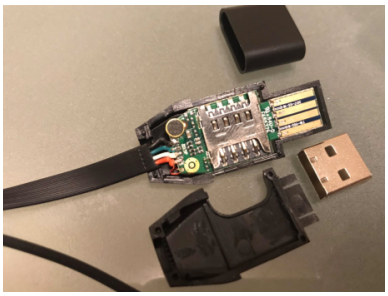
# WireBadger

Malicious Cable Detector User Manual 1.3

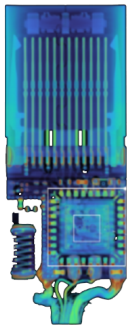
Table Contents

**Overview: Malicious USB Cables and Modern Threats**



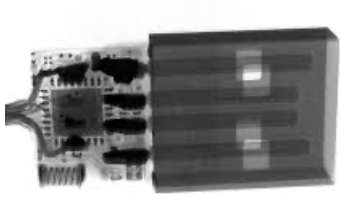
USB technology was designed to be simple, trusted, and universal. When a cable or device is connected, computers and mobile devices automatically establish communication and grant access without user approval. This convenience, however, creates a significant security risk. Over time, attackers have learned to exploit the inherent trust built into USB protocols, transforming ordinary looking cables into effective attack tools.

Early USB-based threats such as CottonMouth relied on infected flash drives and operating-system features such as autorun. While those specific vulnerabilities were reduced, the fundamental problem remained: systems trust USB devices by default. In 2014, researchers publicly demonstrated Bad USB-class attacks, proving that USB devices could be modified at the firmware level to impersonate keyboards, network adapters, or other trusted peripherals. These attacks required no software exploit and could execute commands or install malware within seconds of connection.



As awareness of malicious USB drives increased, attackers shifted to a more covert approach, embedding attack hardware directly inside USB cables. These malicious cables are visually indistinguishable from standard charging or data cables, yet internally contain microcontrollers capable of delivering scripted payloads, altering system settings, installing backdoors, or exfiltrating data. Some variants include wireless capability, allowing remote activation or control after the cable is connected.

Today's malicious cables are smaller, cheaper, and more capable than earlier versions. They can target laptops, desktops, mobile devices, and embedded systems across USB-A, USB-C, and Lightning connectors. Because they operate at the hardware and protocol level, many attacks bypass traditional antivirus and endpoint protection and leave little forensic evidence.



The risk is amplified by common practices such as borrowing chargers, using promotional cables, or charging devices in public spaces. Security organizations, including the National Security Agency, have issued warnings about untrusted USB accessories, and commercially available penetration-testing tools from companies such as Hak5 have demonstrated how easily these attacks can be deployed.

Malicious USB cables represent a credible threat to government, law enforcement, corporate, healthcare, and consumer environments. Effective mitigation requires awareness and hardware-level inspection of cables and connections. In modern threat environments, a USB cable should no longer be assumed to be a passive or harmless component.

**Who buys malicious USB cables (legitimate use)?**

Penetration testers (pentesters)

Usually working under a **written authorization and scope** for a company, government agency, or regulated environment.

---

They test:

- Physical security controls
- User awareness and behavior
- Endpoint hardening and EDR response
- USB device control policies

Their goal: **prove risk, not exploit for damage**.

---

Red teams

Red teams simulate **real adversaries** over longer campaigns.

They test:

- How attackers gain *initial access*
- How long it takes defenders to detect unusual behavior
- Whether physical access + social engineering beats technical controls

Their goal: **measure detection and response**, not just vulnerability

## Introduction

WireBadger is a portable cable tester that detects malicious cables containing malware payloads and wireless access points hidden inside the cable housing. WireBadger offers a simple touchscreen interface with bright and audible alerts allowing penetration testers and security personnel to rapidly test multiple cable configurations. In addition, WireBadger also detects Wi-Fi and Bluetooth signals possibly emanating from the cable itself. These wireless signals indicate hidden access points and BT/BLE devices embedded within some malicious cables. The following cable types are supported:

USB-A cable
USB-B cable
USB-C cable
USB-Mini cable
USB-Micro cable
Lightning cable

## Operation

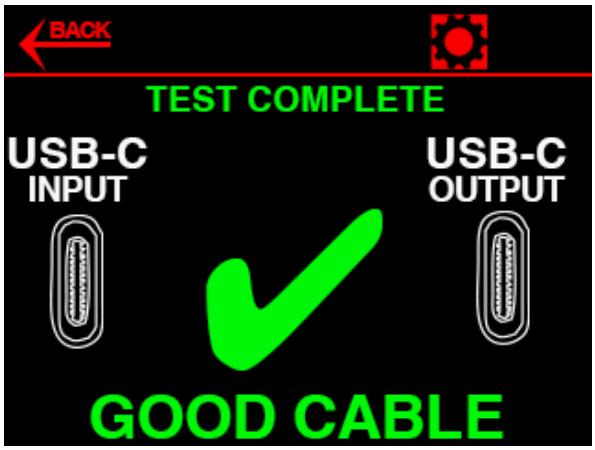
WireBadger is powered using the included AC power adapter and turned on by a button on the side of the unit. Once powered up, the unit's touchscreen allows all necessary adjustments for a full array of cable testing. Each cable tested must be plugged into both input and output sides to be detected and analyzed. Once detected, WireBadger takes a few seconds to analyze the cable and then delivers an on-screen alert displaying either a green check mark (cable is safe) or a skull and crossbones (cable is malicious). Audible alerts in the form of sound effects or voice announcements can also be selected. Under the base of WireBadger, bright LEDs illuminate green (good cable) or red (bad cable) in various patterns such as strobing or pulsing. All of these features can be adjusted by the user in the settings menu.

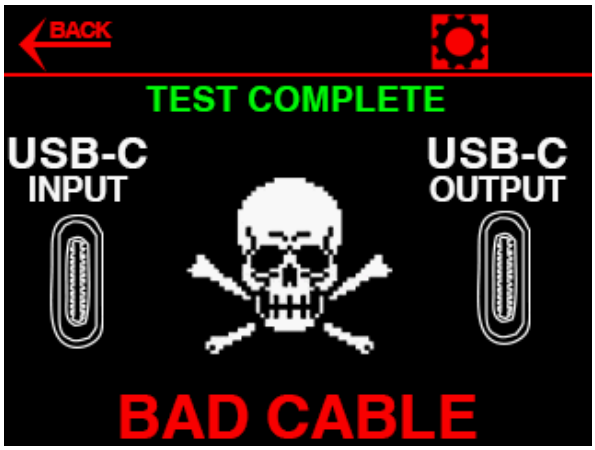
## Unpacking Your Unit

WireBadger ships complete with the (1) WireBadger unit, (1) AC power adapter and (1) rugged transport case. This user manual is in digital format on www.bvsystems.com. Scan the QR code on the shipping box to go directly to the product page containing user manual, quick start guide and tutorial videos. If you want to see the difference between a good cable and genuine malicious cable detection, be sure to order our optional WireBadger test cable kit that includes (3) safe cables and (3) malicious cables.

**Main Screen**

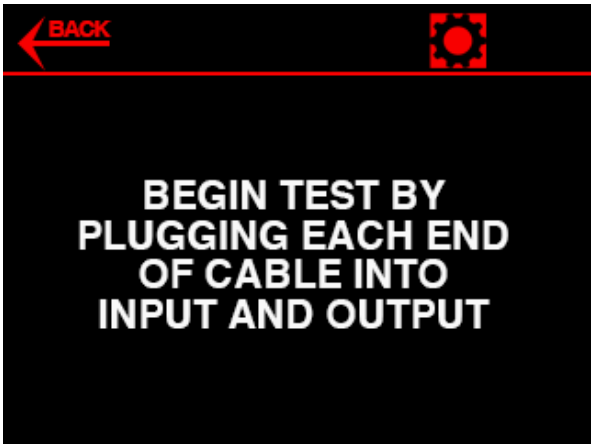
Press the toggle button to power up your WireBadger. Once you connect both ends of the cable in question into their respective ports, WireBadger will analyze the cable. These main scanning screen examples appear when a cable has tested positively or negatively for malicious payloads. There are 36 possible outcomes total for cable testing.



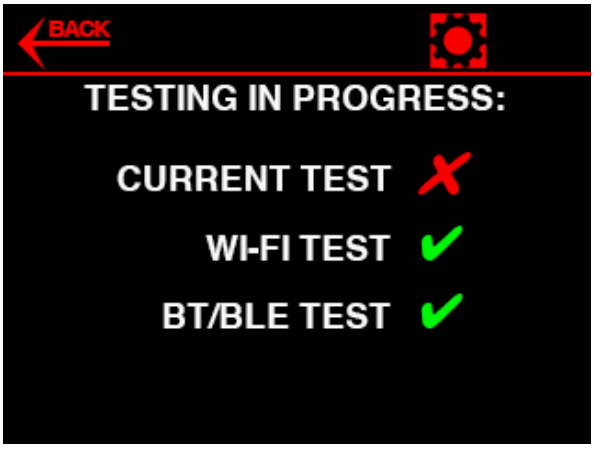
**Before You Begin**

When you first power up WireBadger, before you plug any cable into it, you will be prompted with this message. By default, as soon as you plug one end of the cable into the output and one end into the input, WireBadger will begin to test that cable.



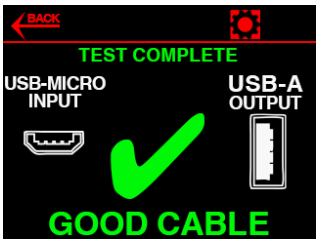
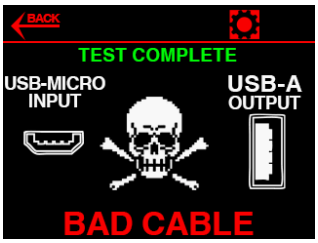
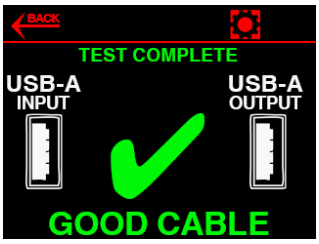
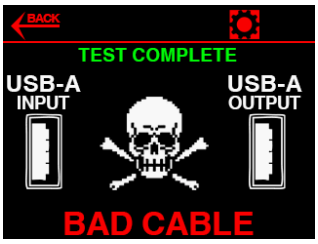
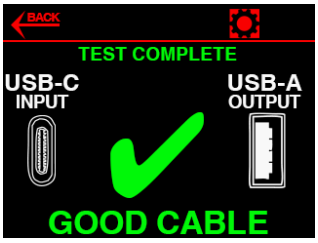
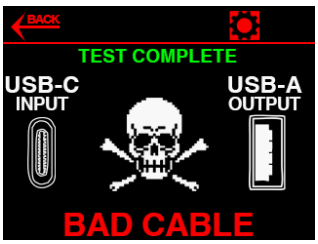
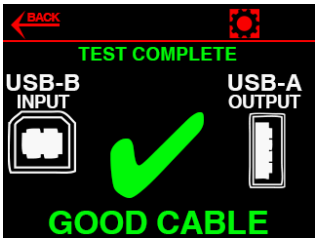
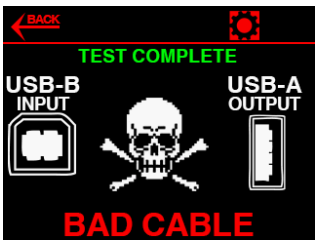
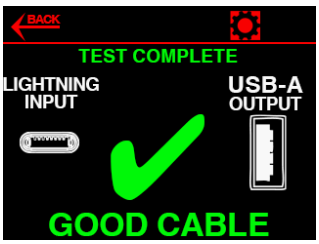
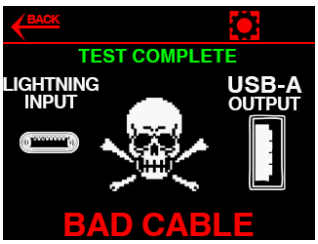
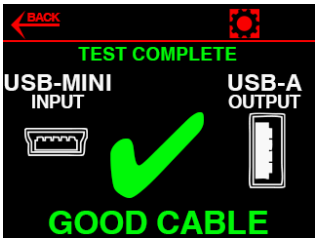
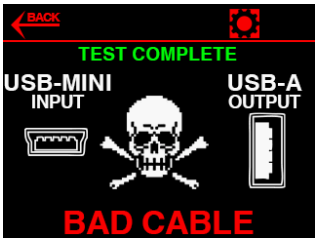
**Testing In Progress**

By default, WireBadger tests the current of all cables. It also tests for Wi-Fi, Bluetooth and BLE signals that could eminate from a malicious cable. These tests are detailed on this screen as they occur. The LED lights under the unit light up differently as each test initiates. The wireless tests can be turned off and the LED lights can also be adjusted in settings.



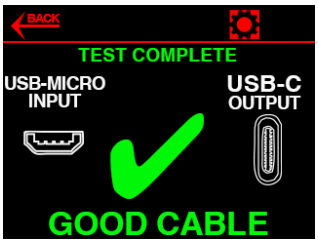
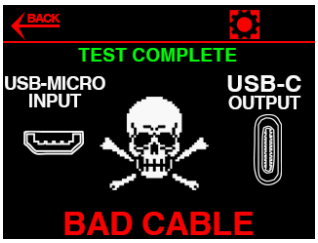
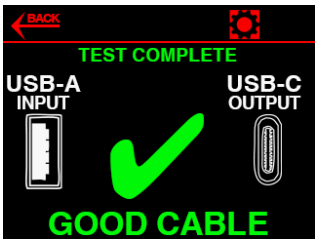
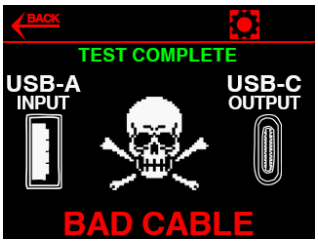
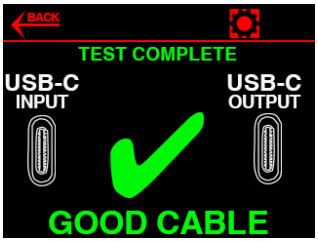
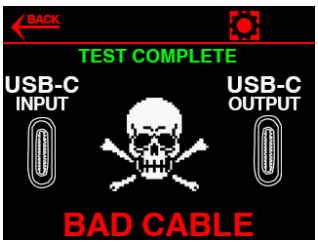
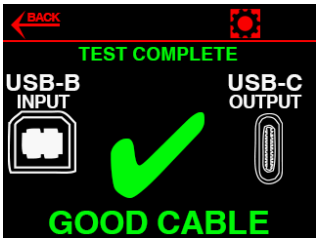
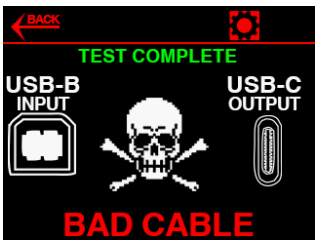
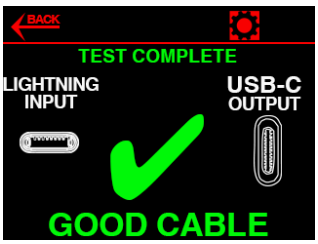
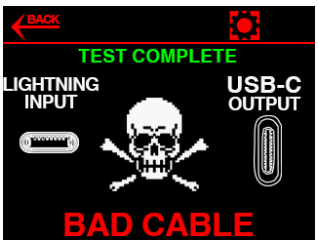
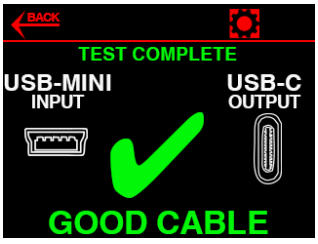
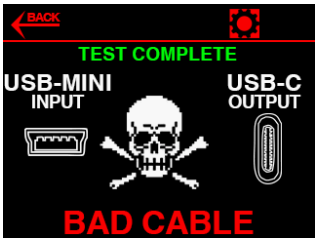
**USB-A Cable Tests**

These cables all include USB-A connector on at least one end of the cable.

| NO MALWARE DETECTED | MALWARE DETECTED |
| --- | --- |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |

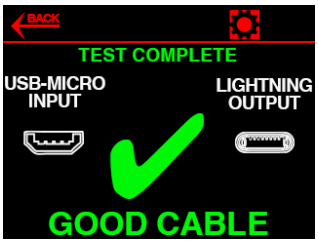
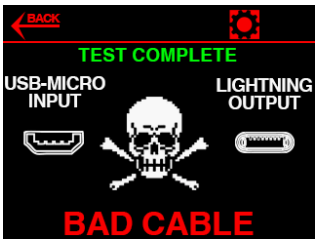
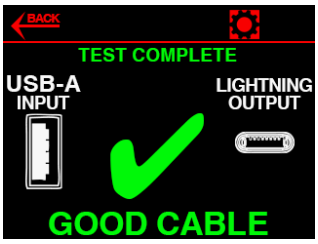
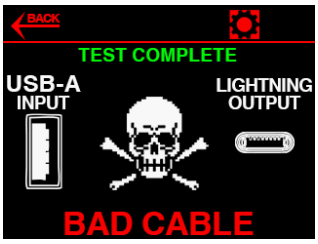
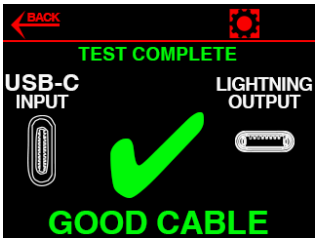
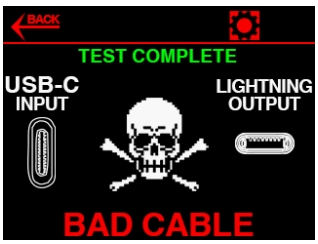
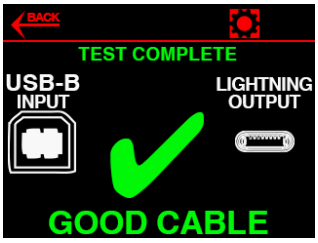
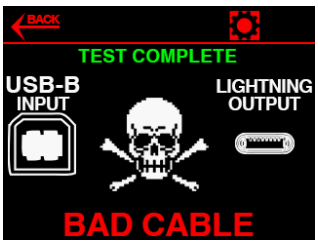
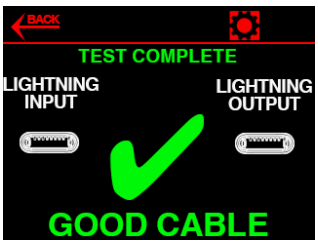
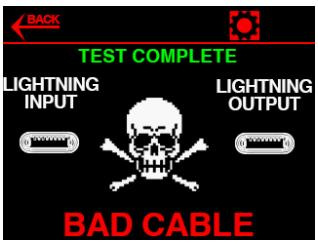
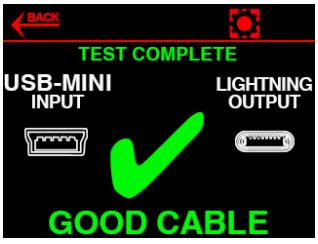
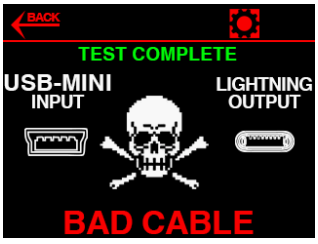
**USB-C Cable Tests**

These cables all include USB-C connector on at least one end of the cable.

| NO MALWARE DETECTED | MALWARE DETECTED |
| --- | --- |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |

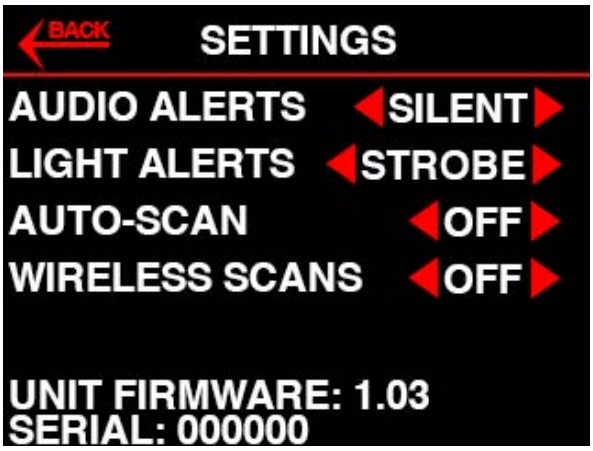
**Lightning Cable Tests**

These cables all include Lightning connector on at least one end of the cable.

| NO MALWARE DETECTED | MALWARE DETECTED |
| --- | --- |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |

**Settings Menu**

Touch the gear icon on the top of any screen it appears to access these settings.





AUDIO ALERTS – Pressing left or right red arrows choose between audio alerts which are SILENT, VOICE (vocal alerts) and TONES.


LIGHT ALERTS - Pressing left or right red arrows choose between visual lighting alerts that appear at 3 of the 4 bottom sides of the unit as a STROBE, PULSE and OFF. Red light indicates a bad cable is detected and green light indicates a bad cable is not detected.

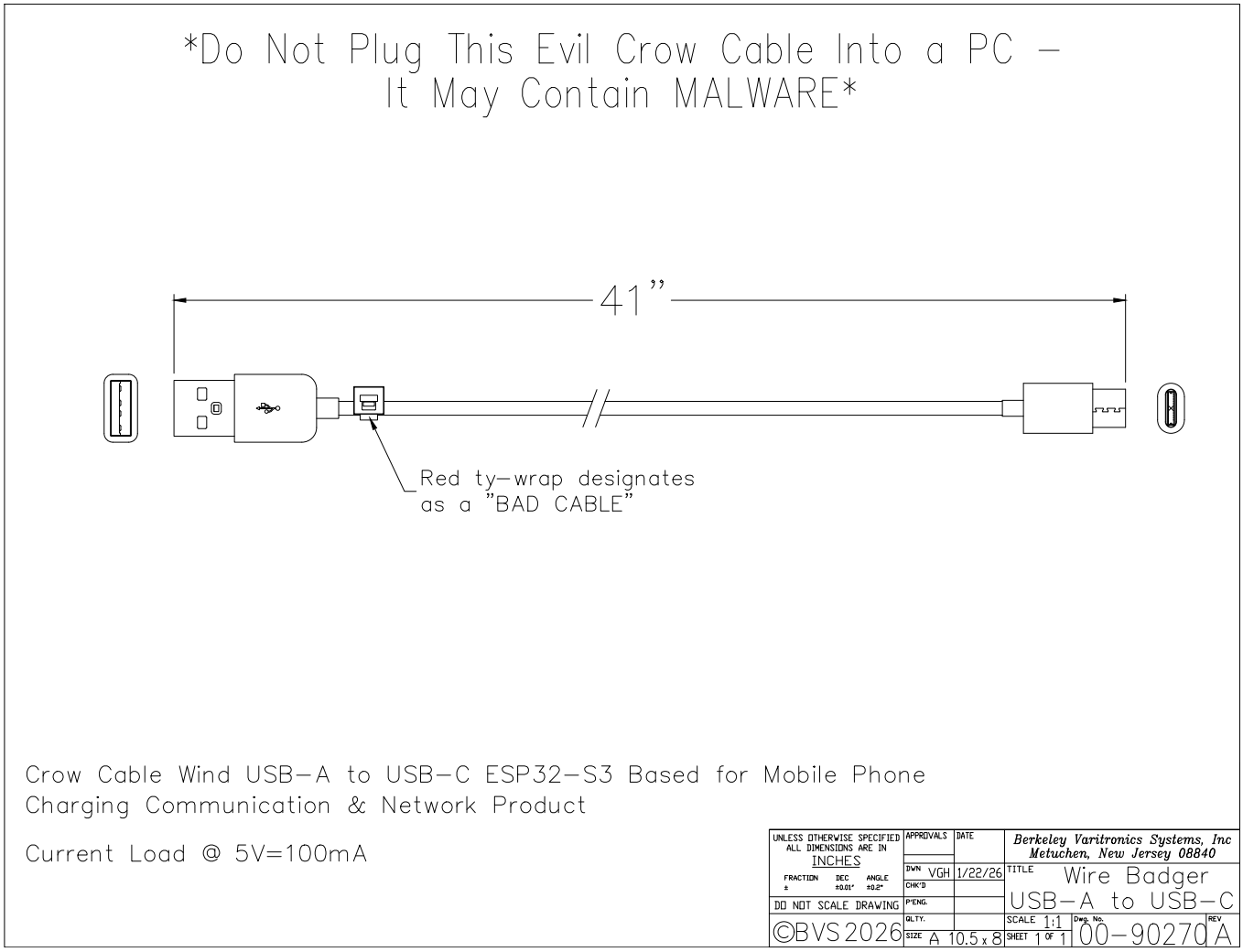

AUTO-SCAN - Choose ON of OFF for analyzing cables. When a cable is plugged into both input and output connectors with this setting tuned ON, WireBadger automatically analyzes the cable. When this setting is OFF, the user must manually choose to analyze cables that are plugged in.


WIRELESS SCANS - Choose ON or OFF to enable wireless scans. Since wireless scans are not always required to determine if cables are malicious and also takes extra time, some users turn this feature OFF.


FIRMWARE & SERIAL – Be sure to reference these numbers when contacting BVS product support or downloading new firmware for your WireBadger.

## Evil Crow Cable Diagram

This is one of (3) malicious cables included in the optional WireBadger cable kit.



Thank you for your purchase, we look forward to supporting you and your team.

**Customer Support**

Berkeley Varitronics Systems, Inc.
Liberty Corporate Park
255 Liberty Street
Metuchen, NJ 08840

8:00 AM to 6:00 PM EST
Toll Free: 888-737-4287
Phone: 732-548-3737
Fax: 732-548-3404

24/7 (expect a reply within one day)
email: support@bvsystems.com
www.bvsystems.com