protiviti®
Global Business Consulting

The Rising Threat of Advanced Bad USB Attacks in Healthcare

By Parth Srivastava, Senior Manager, Protiviti Japan

What is Bad USB?

A Bad USB is a malicious device disguised as a normal USB flash drive, but instead of functioning as a traditional storage device, it behaves as a keyboard or mouse (HID – Human Interface Device). This allows it to bypass USB storage restrictions and execute malicious commands on a connected system without requiring user permission.

Traditional Bad USB attacks have been used for years to inject keystrokes, install malware, steal credentials, and take control of machines within seconds. However, a new, more advanced version of Bad USB has emerged, making it significantly more dangerous—it now includes an inbuilt Wi-Fi module, giving attackers real-time control and persistence over compromised systems.

In a healthcare setting, where medical devices, patient data, and hospital networks are interconnected, an attack leveraging Advanced Bad USB could lead to data breaches, ransomware infections, and even disruptions in critical medical procedures.

Common Scenarios Where USBs Are Used in Healthcare (and How They Can Be Exploited)

Even in today's networked environment, USB devices are still heavily used across healthcare organizations for various legitimate purposes. Unfortunately, this routine creates opportunities for attackers to introduce Bad USBs into critical systems. Here are some common scenarios:

Vendor Technicians Updating Medical Equipment

Imagine a biomedical technician visiting a hospital to perform routine maintenance on an MRI machine or a heart monitor system. As part of the update, the vendor uses a USB device containing new firmware patches.

Exploitation: An attacker compromises the vendor's USB beforehand (or impersonates a vendor), inserting a Bad USB into the machine. Within seconds, malware could be deployed onto the medical device or even the internal hospital network it connects to.

Patient Check-In Kiosks in Hospital Lobbies

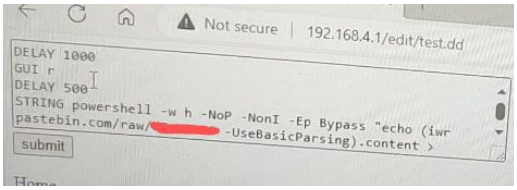
Many modern hospitals have self-service kiosks where patients can check in for appointments or fill out intake forms. These kiosks sometimes have exposed USB ports for maintenance purposes.

Exploitation: An attacker posing as a "concerned patient" or visitor quickly plugs in a Bad USB device into an unattended kiosk. Malware quietly installs itself on the kiosk backend, pivoting into internal networks where sensitive health records are stored.

How the Advanced Bad USB Attack Works

This new version of Bad USB operates differently from its predecessors by incorporating an embedded Wi-Fi chip, which significantly enhances the attacker's capabilities. Here's how it works:

1. **Disguised as a Peripheral Device** – When plugged into a computer or medical device, the Bad USB is detected as a keyboard or mouse instead of a storage device, allowing it to bypass traditional USB restrictions.
2. **Wi-Fi Network Activation** – The embedded chip inside the USB creates a rogue Wi-Fi network, which the attacker can connect to remotely.



3. **Remote Command Execution** – Once connected, the attacker can execute unlimited scripts, unlike earlier Bad USB variants, which could only run a single script upon insertion.
4. **System Compromise** – With real-time control, the attacker can deploy malware, exfiltrate patient data, disable medical systems, or even manipulate connected IoT healthcare devices.
5. **Persistence & Stealth** – Even if the initial payload fails, the attacker can rerun scripts, bypass security measures, and maintain ongoing access to the compromised machine without physical presence.

Why This Attack is Particularly Dangerous for Healthcare

The healthcare industry is a prime target for cybercriminals due to the high value of patient data and the critical nature of medical systems. An advanced Bad USB attack could lead to:

1. **Unauthorized Access to Patient Data**
   - Electronic Health Records (EHRs) contain sensitive personal and medical information that can be sold on the dark web or used for identity theft.
   - Attackers can exfiltrate patient data within seconds of plugging in the malicious USB.

2. **Ransomware Deployment on Hospital Networks**
    - With real-time remote access, attackers can inject ransomware into hospital systems, encrypting patient records and demanding ransom payments to restore access.
    - This can lead to delayed treatments, misdiagnosed conditions, and even loss of life.
3. **Compromise of Medical Devices**
    - Many medical devices, such as infusion pumps, ventilators, and imaging systems, are connected to hospital networks.
    - An attacker could remotely manipulate device settings, causing equipment failure or incorrect dosages.
4. **Disruption of Critical Healthcare Operations**
    - Attackers can deploy malware to crash hospital management systems, disrupt communication channels, and halt emergency services.
    - A widespread attack could shut down entire departments, leading to postponed surgeries and medical crises.

How Healthcare Organizations Can Defend Against Advanced Bad USB Attacks

To mitigate the risk of such sophisticated attacks, hospitals and healthcare organizations must adopt a multi-layered cybersecurity approach.

1. **Restrict USB and Peripheral Device Access**
    - Block unauthorized HID devices (keyboards, mice, or other input devices) using endpoint security solutions.
    - Implement strict USB policies, allowing only approved medical devices and encrypted storage devices.
    - Use USB port security solutions that detect and block rogue HID-based USB attacks.
2. **Monitor Wireless Activity & Rogue Wi-Fi Networks**
    - Deploy Wi-Fi scanning solutions to detect unauthorized access points.
    - Configure network monitoring tools to alert security teams when an unknown Wi-Fi network appears in hospital premises.
    - Disable automatic connection to unknown Wi-Fi networks on hospital machines.
3. **Train Healthcare Staff on USB-Based Threats**
    - Educate employees about the dangers of plugging unknown USB devices into medical computers or hospital networks.
    - Implement strict policies against using personal USB drives on work machines.
    - Conduct simulated phishing and USB attack drills to improve staff awareness.
4. **Deploy Endpoint Detection and Response (EDR) Solutions**
    - Use behavior-based security solutions that monitor keystroke injection attacks from fake HID devices.

- Ensure real-time monitoring of connected devices to flag suspicious behavior.
- Implement automated responses to isolate infected systems and prevent lateral movement.

5. **Implement Zero Trust Security Architecture**
   - Adopt a zero-trust approach by verifying all devices and users before granting access to hospital networks.
   - Require multi-factor authentication (MFA) for all privileged accounts.
   - Limit privilege escalation to prevent unauthorized script execution.
6. **Regular Security Audits and Testing**
   - Conduct penetration testing to assess vulnerabilities in hospital systems.
   - Run red team exercises to simulate Bad USB attacks and train incident response teams.
   - Ensure compliance with cybersecurity regulations (e.g., HIPAA, GDPR) to strengthen data protection strategies.

Conclusion

As healthcare institutions continue to digitize operations, cybercriminals are evolving their tactics to exploit vulnerabilities in medical systems. The new generation of Bad USB devices with inbuilt Wi-Fi capabilities represents a serious threat, giving attackers remote access, unlimited script execution, and the ability to compromise hospital networks within seconds.

Since these devices masquerade as keyboards or mouse, even traditional USB restrictions cannot fully prevent their execution. Healthcare organizations must go beyond basic USB blocking and enforce stricter security measures to defend against these stealthy threats.

By implementing USB and HID device restrictions, monitoring wireless activity, and training staff on cybersecurity best practices, healthcare organizations can reduce the risk of these advanced attacks and ensure patient safety remains uncompromised.