Red Teaming Project
USB Keylogger

Understanding the Invisible Threat

Team - Syprolix

Introduction

What is a USB Keylogger?

A USB keylogger is a **small hardware device** secretly inserted between a keyboard and a computer, designed to record every keystroke made by the user. It operates invisibly, capturing sensitive data like passwords, messages, and confidential information without the user's knowledge.

- A small hardware device placed between keyboard and PC to secretly record keystrokes.
- Operates invisibly, capturing passwords, messages, and sensitive data without user knowledge.
- Used in red teaming to simulate real-world attacks and test security defenses.

How USB Keyloggers Work

USB keyloggers function by intercepting all keyboard inputs. These captured keystrokes are then either **stored locally** on the device's internal memory or **transmitted wirelessly** to an attacker.

- Intercept all keyboard inputs and store data locally or transmit wirelessly.
- Some mimic trusted devices, bypassing security by spoofing hardware IDs.

1

Masquerades as HID

Acts as a Human Interface Device (HID), often appearing as a legitimate keyboard or mouse.

2

Injects / Records Input

Once plugged in, it silently injects keystrokes or records user input without detection.

3

Delivers Payloads

Can deliver malicious payloads such as backdoors, key loggers, or remote access tools.

Advanced keyloggers can even **spoof hardware IDs**, making them appear as legitimate devices to the operating system and bypassing certain security measures.

Team - Syprolix

Hacker Motives Behind USB Keyloggers

Credential Theft

Capturing passwords and usernames to gain unauthorized access to corporate networks, personal accounts, and critical systems.

Espionage

Stealing confidential business data, trade secrets, and intellectual property for competitive advantage or sale on the dark web.

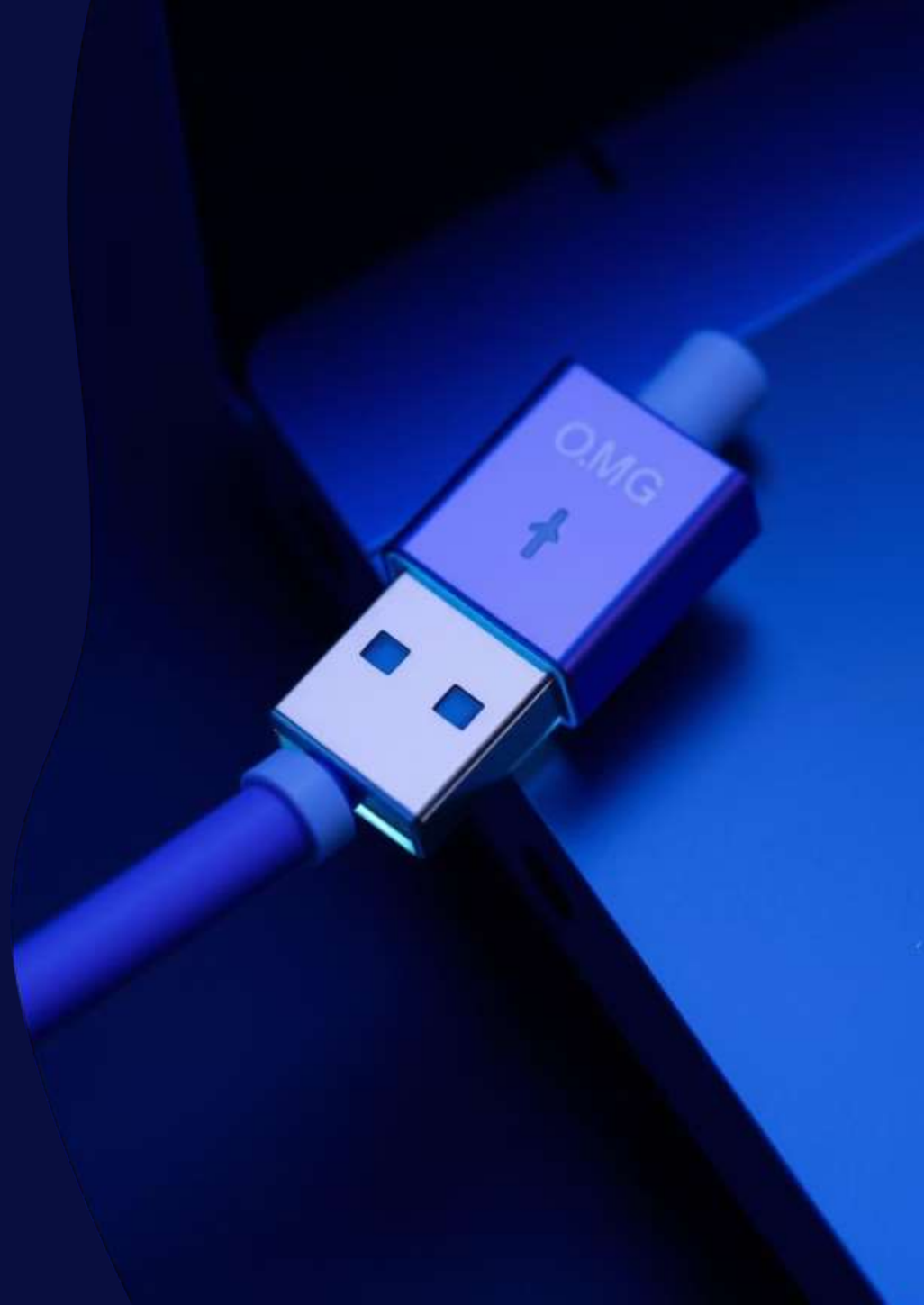
Persistence

Establishing a long-term presence within a target's environment for ongoing surveillance and data exfiltration, often remaining undetected for extended periods.

Dramatic Example: The O.MG Cable

The O.MG Cable is a prime example of advanced keylogger technology. It looks and functions identically to a normal USB charging or data cable, making it incredibly difficult to identify visually. However, once connected, it immediately begins logging keystrokes.

- Looks like a normal USB cable but logs keystrokes immediately on connection.
- Connects to attacker's Wi-Fi for real-time data exfiltration.
- Can be remotely disabled or reprogrammed, making detection very difficult.



Signs of a USB Keylogger Attack

Unexpected USB Devices

Detection of unknown devices in system logs or Device Manager that don't match known hardware.

Unusual Keyboard Behavior

System lag, unresponsive keys, or ghost typing that suggests interference with keyboard input.

Unauthorized Activity

Suspicious logins, data transfers, or access patterns that don't align with legitimate user actions.

Physical Anomalies

Discovery of suspicious USB extensions, adapters, or unknown hardware attached to keyboards or ports.

Precautions to Prevent USB Keylogger Attacks

Protecting against USB keyloggers requires a multi-layered approach, combining physical security with user education and technical controls.

- **Physically secure USB ports** with locks or port blockers to prevent unauthorized device insertion.
- **Train employees** to never plug in unknown USB devices and to report any suspicious hardware.
- **Use endpoint protection tools** that monitor USB activity and block unrecognized or suspicious devices.
- **Conduct regular red team exercises** simulating USB keylogger attacks to test and improve existing defenses.

Team - Syprolix

Advanced Defense Strategies

BIOS USB Disable

Implement BIOS-level USB port disablement for non-essential ports to restrict physical access.

Network Traffic Monitoring

Monitor network for unusual data flows or exfiltration patterns indicative of keystroke data transmission.

Zero-Trust Architecture

Employ zero-trust principles and strict access controls, assuming no user or device is trusted by default.

Asset Inventories & Audits

Maintain up-to-date asset inventories and conduct frequent physical audits of hardware for unauthorized modifications.

Conclusion: Stay Vigilant, Stay Secure

USB keyloggers represent a significant, yet often underestimated, threat in the cybersecurity landscape. Their stealth and effectiveness make them powerful tools for both attackers and red teams.

Understanding their operation and motives is paramount to building resilient defenses. A combination of physical security, robust employee awareness, and advanced technical controls is crucial.

Regular testing and continuous monitoring are your best weapons against these invisible threats, ensuring your organization remains secure in an evolving threat environment.

Team - Syprolix