
# Industry Report:

## 2016 MouseJack Security Vulnerability Survey

Bastille

# Executive Summary: The 2016 MouseJack Security Vulnerability Survey

In February 2016, Bastille researchers announced a serious security vulnerability in more than one billion wireless computer mice. Dubbed MouseJack, the vulnerability allows hackers to remotely access any computer with an affected mouse. The vulnerability not only affects the individual computer, but allows hackers the means to access any connected networks. Hackers can gain access to a vulnerable computer from up to 500 feet away. To learn more about MouseJack and affected devices, visit www.MouseJack.com.

The 2016 MouseJack Security Vulnerability Survey summarizes results from over 900 responses to our online survey with respect to the emerging security threat associated with over one billion wireless mice.

**In Brief:**

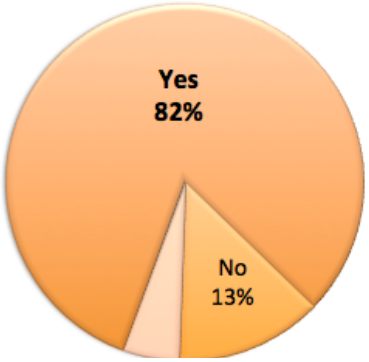
- **More than 80% of organizations are potentially vulnerable to being "MouseJacked"**
- **Within these organizations, 1 in 7 employees plan to do nothing and continue using their vulnerable wireless mouse devices, leaving many Enterprises exposed to attacks.**
- **1/3 said they would replace their wireless mouse with a wired mouse**

**Analysis:**

- **Hackers need just a single weak link. Even if the majority of users patch or replace their wireless mice in a timely fashion, there will still be 160 million weak links.**
- **Organizations need to create and enforce policies to ensure employees patch or replace their affected devices in a timely manner.**

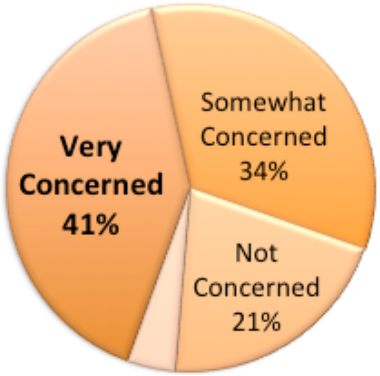
# Key Report Findings

- More than 8 out of 10 employees are allowed to use a wireless mouse at their office. This puts over 80% of businesses potentially at risk to the MouseJack vulnerability.



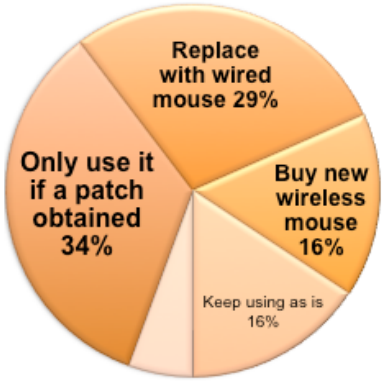

Does your company allow wireless mice to be used?
**82% Yes**

- Concern with the security of wireless mice is a high priority for most with 75% of respondents concerned about whether their wireless mouse can be hacked.




How concerned are you about whether your wireless mouse can be hacked?
**75% Concerned**

- Results suggest that despite increased awareness for the MouseJack vulnerability, some individuals and companies will continue to ignore the risks associated with wireless devices.




What action will be taken?
**80% intend to take action and patch or replace their wireless mouse**

# Table of Contents

# What is the MouseJack Vulnerability?

MouseJack is a class of vulnerabilities that affects the vast majority of wireless, non-Bluetooth keyboards and mice. These peripherals are 'connected' to a host computer using a radio transceiver, commonly a small USB dongle. Since the connection is wireless, and mouse movements and keystrokes are sent over the air, it is possible to compromise a victim's computer by transmitting specially crafted radio signals using a device which costs as little as $15.

Our research shows that an attacker can launch the attack from up to 500 feet away. The attacker is able to take control of the target computer without physically being in front of it. The attacker can then type arbitrary text or send scripted commands at 1000 words per minute, making it possible to rapidly perform malicious activities without being detected.

The MouseJack exploit centers around injecting unencrypted keystrokes into a target computer. Mouse movements are usually sent unencrypted, and keystrokes are often encrypted (to prevent eavesdropping of what is being typed). However, the MouseJack vulnerability takes advantage of affected receiver dongles and their associated software, allowing unencrypted keystrokes transmitted by an attacker to be passed on to the computer's operating system as if the victim had legitimately typed them.

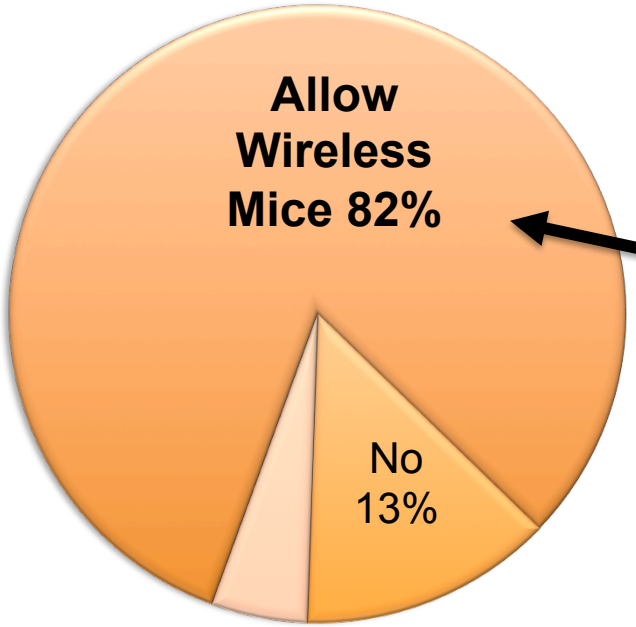
To learn more about MouseJack and affected devices, visit [www.MouseJack.com.](http://www.MouseJack.com)

# Survey Methodology

The Bastille research team began exploring the security of wireless mice as part of the company's mission to secure the Enterprise airspace by identifying airborne threats. Through their research, the MouseJack vulnerability was discovered which leaves more than a billion devices and the networks to which they are attached, vulnerable to remote exploitation via the radio frequency spectrum. Bastille went through ethical disclosure to vendors 90 days in advance of the public announcement of MouseJack to give vendors time to prepare patches or remediation plans. The quantitative portion of the report is based on an online global enterprise concern and readiness survey conducted by Bastille over a 4 week period starting February 23, 2016. Survey respondents included over 900 global professionals.

# Key Findings: (1) Does your company allow wireless mice?

**Does your company allow wireless mice?**



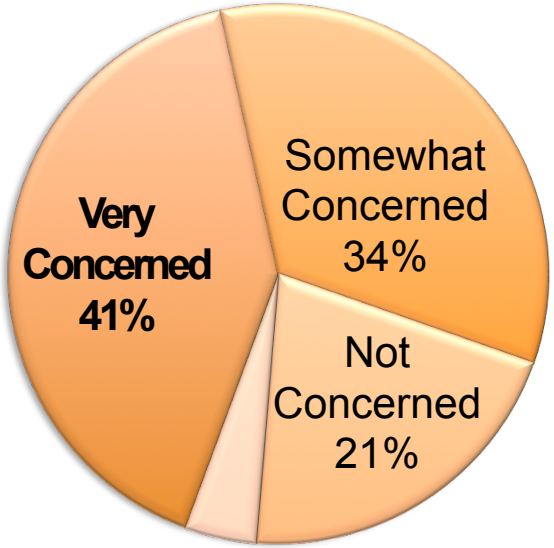

The results indicate that more than 82% of businesses are potentially susceptible to the MouseJack vulnerability.

**Does your company allow wireless mice?**

| | | |
|---|---|---|
| Yes | 749 | 82% |
| No | 122 | 13% |
| (no response) | 46 | 5% |
| | 917 | |

# Key Findings: (2) How concerned are you that your wireless mouse could be hacked?

**How concerned are you about whether your wireless mouse can be hacked?**



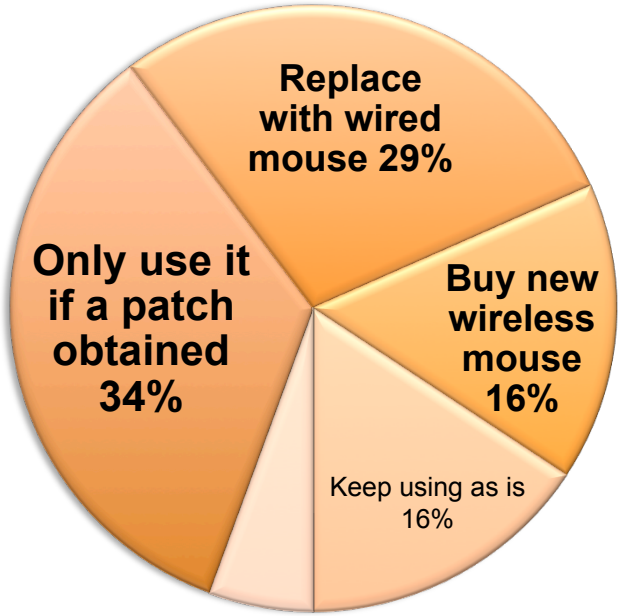

3 in 4 people are concerned that their mouse could be hacked.

**How concerned are you that your wireless mouse can be hacked?**

| | | |
|---|---|---|
| Very Concerned | 376 | 41% |
| Somewhat Concerned | 310 | 34% |
| Not Concerned | 192 | 21% |
| (no response) | 39 | 4% |
| | 917 | |

# Key Findings: (3) What will you do if your mouse has the MouseJack vulnerability?

## What action will be taken as a result of MouseJack?




- **1 in 7 (16%)** of people said they would keep using their mouse even if it was vulnerable, which is of concern as it only takes 1 person to create an entry point for a hacker.
- **Almost 8 in 10 people** said they would like to take action, by patching or replacing their mouse.
- Almost **1/3 are giving up on wireless** mice entirely and replacing with wired mice.

## What action will be taken as a result of MouseJack?

| | | |
|---|---|---|
| Only use it if a patch obtained | 313 | 34% |
| Replace with wired mouse | 263 | 29% |
| Buy a new and safe wireless mouse | 146 | 16% |
| Keep using as is | 144 | 16% |
| (no response) | 51 | 6% |
| | 917 | |

# Industry Response on MouseJack

WIRED

**‘Flaws in Wireless Mice and Keyboards Let Hackers Type on Your PC’**

c|net

**‘Use a wireless mouse? This $15 hack could compromise your laptop’**

InformationWeek DARKReading

**'MouseJack' Attack Bites Non-Bluetooth Wireless Mice”**

NETWORKWORLD

**‘Countless computers vulnerable to MouseJack attack through wireless mice and keyboards’**

# About Bastille

Launched in 2014, Bastille is pioneering Internet of Things (IoT) security with next-generation security sensors and airborne emission detection, allowing corporations to accurately quantify risk and mitigate 21st century airborne threats. Through its patent-pending, proprietary technology, Bastille helps enterprise organizations protect cyber and human assets while providing unprecedented visibility of wireless IoT devices that could pose a threat to network infrastructure. For more information on Bastille, visit www.Bastille.net and follow @bastillenet on Twitter and LinkedIn.

# MouseJack Resource Guide

For more information on the MouseJack vulnerability, visit www.MouseJack.com, where we have a full media kit:

- Press Release
- FAQ
- Video
- Public Advisories
- Technical Details
- Logos

For more information on Bastille, visit www.Bastille.net and follow @bastillenet on Twitter and LinkedIn.


Bastille Contact:
Sophie Koch
504-920-9336
sophie@bastille.io

Media Contact:
Noe Sacoco
408.340.8130
noe@lmgpr.com