Rare BadUSB attack detected in the wild against US hospitality provider

By Written by Catalin Cimpanu, ContributorContributor March 26, 2020 at 6:00 a.m. PT

Archived: 2026-04-05 14:36:52 UTC

A US hospitality provider has recently been the target of an incredibly rare BadUSB attack, ZDNet has learned from cyber-security firm Trustwave.

The attack happened after the company received an envelope containing a fake BestBuy gift card, along with a USB thumb drive.

The receiving company was told to plug the USB thumb drive into a computer to access a list of items the gift card could be used for.

Image: Trustwave

But in reality, the USB thumb drive was what security experts call a "BadUSB" -- a USB thumb drive that actually functions as a keyboard when connected to a computer, where it emulates keypresses to launch various automated attacks.

Trustwave, who couldn't reveal the target company's name for confidentiality reasons, said the victim recognized the attempted hack and called it in to investigate the incident.

In a report published today and shared with *ZDNet*, Trustwave said that once they plugged the BadUSB into a test workstation, the BadUSB triggered a series of automated keypresses that launched a PowerShell command.

This Powershell command downloaded a bulkier PowerShell script from an internet site and then installed malware on the test machine -- a JScript-based bot.


badusb-attack.png
Image: Trustwave

"At the time of the analysis, we did not found a similar strain of malware," Phil Hay, Senior Research Manager at Trustwave, told *ZDNet* in an email yesterday.

"The malware is unknown to us. It is also hard to say if it is custom-built, but it probably is, because it is not wide spread and seems to be targeted," Hay added.

However, the Trustwave researcher also told us that since their initial analysis, a file similar to the malware they analyzed was later uploaded on VirusTotal, a web-based file scanning engine. Per subsequent analysis from Facebook and Kaspersky researchers, the file is believed to be the work of a hacking group known as FIN7.

It is unclear who uploaded this file, or if it comes from another cyber-security vendor also investigating a BadUSB attack at another victim.

But the lesson here is that someone actually detected a BadUSB attack in the real world. BadUSB attacks were first detailed at the start of the 2010s, and for many years they represented a theoretical attack scenario, something that employees are often warned about, but which has rarely been seen in the wild.

"These sorts of [BadUSB] attacks are often simulated in penetration testing and used during red teaming exercises," Hay told *ZDNet*. "Seeing these types of attacks in the real world is much more rare."

An FBI spokesperson told *ZDNet* that any users or companies who receive malware-laced USBs should report the incident to their local FBI office for further investigations.

Last known attack happened two years ago in Eastern Europe

The last known case of a BadUSB attack -- also known as a Bash Bunny attack -- was detailed in December 2018 by Russian cyber-security firm Kaspersky.

At the time, the company said it found BadUSB devices, along with cheap laptops and Raspberry Pi boards, on location at eight banks in Eastern Europe. The banks called Kaspersky to investigate a series of mysterious cyber-heists during which hackers stole tens of millions of dollars.

Security
