ALL HANDS ON DUCK

The USB Rubber Ducky has been a potent threat for over 15 years—innocent on the surface but paddling fast underwater

Tired of performing repetitive tasks in his IT job in 2010, Hak5 Founder Darren Kitchen took a creative route to efficiency.

Using USB hardware modified to pose as a standard keyboard, Kitchen used scripting and keystroke injection to automatically send commands to the servers and printers he was administering. The idea quickly morphed into the USB Rubber Ducky, the first commercially available keystroke injector.

Despite looking like an innocent USB flash drive, the Ducky could inject 1,000 words per minute, automatically firing when plugged in.

"You plug it in, and it acts like a keyboard," explained Kieran Human, ThreatLocker® Special Projects Engineer and head of Rubber Ducky labs at Zero Trust World. "Anything you can do with a keyboard, this can do. It can open PowerShell, delete files, exfiltrate data, or encrypt it. You don't even need elevated privileges to fire any of this stuff off, because you're technically not executing scripts. You (or, more correctly, the Ducky) are just typing."

Because the device identifies itself as a standard human interface device (HID), the operating system grants it the same level of trust and access as a user's actual keyboard. No admin rights required, no suspicious binaries dropped, no obvious malware signatures created.

Limitless automation

There is almost no limit to what a USB Rubber Ducky can do, as Human explained. "You just create the PowerShell script and then run it. It could be literally anything. You can use it for any repetitive task; we had 500 computers that had to get connected to the internet, and instead of having to go to each one manually, I made a script that opened PowerShell and connected them automatically and did a few other fixes."

Of course, not every use is quite as benign. “In my lab sessions, I’ve put together a script that will take screenshots of your computer every 10 seconds, or one that copies your clipboard every minute and uploads it. There is another one that will detect if you copy a Bitcoin address and then switch it with a fake one. I’ve even managed to put ransomware on a Ducky. One major endpoint detection and response (EDR) vendor initially detected it, but after I split it up and made a couple of changes, they couldn’t see it. I ran it across multiple EDRs—the big EDRs you hear about—and none of them detect it. It’s straight ransomware.”

> **“Anything you can do with a keyboard, Rubber Ducky can do. It can open PowerShell, delete files, exfiltrate data or encrypt it**

Why traditional security tools fail

This is the uncomfortable truth: Behavioral security tools are trained to detect malware, not a user typing at lightning speed. And since blocking keyboards is not generally an option, the Rubber Ducky cannot be stopped conventionally.

In the years since the product first reached the market, it has evolved significantly, making detection even more difficult. That is true post-attachment, with modern iterations of the Ducky platform able to slow typing to human speed and cadence, avoiding behavioral detection. And it is true of the physical form of the Rubber Ducky, too. Though many versions remain packaged in the familiar USB flash drive shell, some now hide in the limited space usually afforded to e-marker chips in USB cables.

The only practical defensive strategies for stopping Rubber Ducky attacks involve removing the ability of the scripts to do any damage, reducing the attack surface, and containing the blast radius through microsegmentation. “Even if you need access to PowerShell,” explained Human, “using Ringfencing™ properly means it can’t access all your files, and it can’t access the internet. If you don’t need PowerShell, block it with Application Allowlisting. The whole point is that even if the Ducky gets a command through, the application it launches shouldn’t be allowed to do anything it isn’t allowed to do.”

HOW THREATLOCKER NEUTRALIZES RUBBER DUCKY ATTACKS

Even though a Rubber Ducky masquerades as a genuine keyboard, ThreatLocker can neutralize what it attempts to do after the keystrokes land.

Application Allowlisting
Ducky payloads rely heavily on PowerShell, the command prompt, and other script interpreters. Allowlisting ensures that only approved applications can run. If an endpoint does not need PowerShell, block it entirely; if it does, restrict its use.

Ringfencing
Ringfencing isolates applications from one another and from sensitive data. A Rubber Ducky script may successfully launch PowerShell, but ThreatLocker prevents it from reading user documents, connecting to remote repositories, executing unapproved binaries, or exfiltrating content that is outside its permission boundary. The payload may “run,” but it becomes functionally toothless.

Many Ducky scripts rely on outside sources. Even if a Ducky attempts to download a full malicious script from an attacker’s server, which is a common tactic to evade detection, ThreatLocker can block outbound traffic from tools that should not have internet access.

Storage Control
While Rubber Duckies tend to use only minimal storage, many attackers pair HID devices with the capacity of traditional USB drives. ThreatLocker can enforce device-level restrictions to prevent data exfiltration or the execution of unwanted files.

Beyond signatures
Most Rubber Ducky payloads never drop files and are therefore invisible to traditional EDR signature-based detection. Policy-based enforcement stops the behavior, not the specific file.