Meet PoisonTap, the $5 tool that ransacks password-protected computers

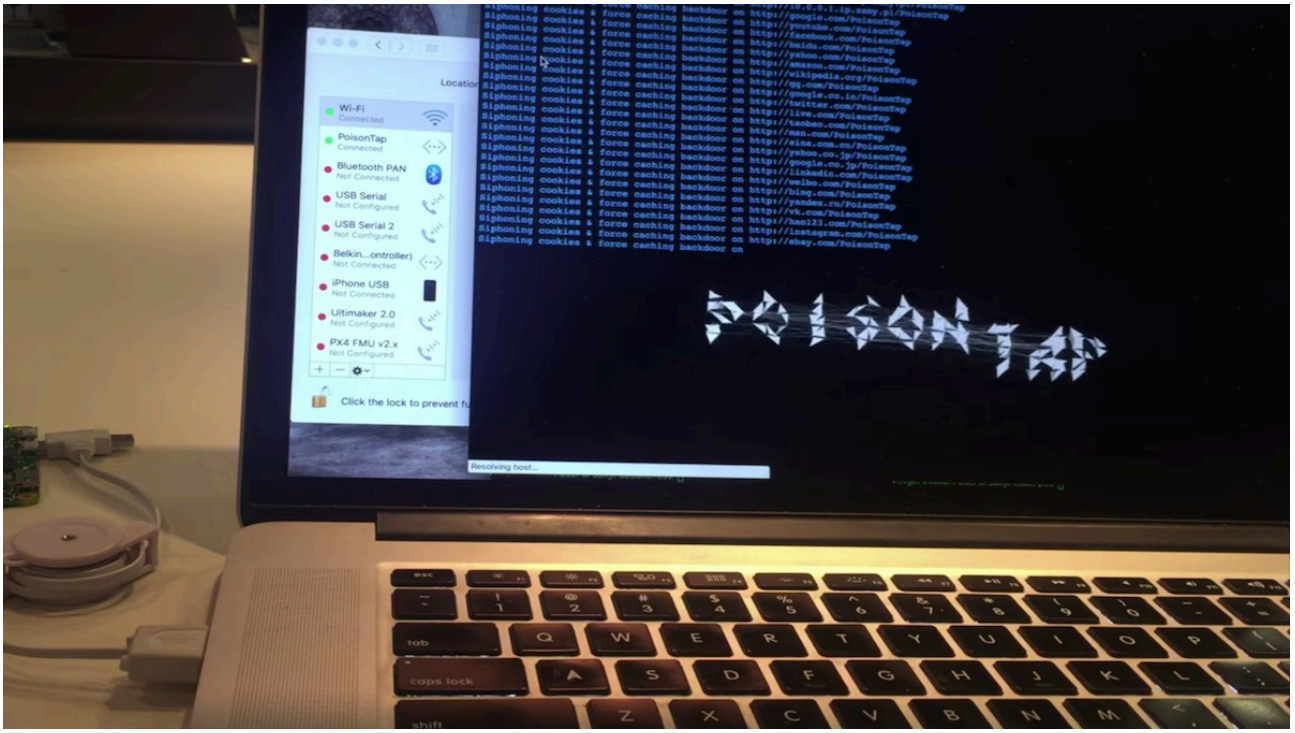
By Dan Goodin

Published: 2016-11-16 · Archived: 2026-04-06 03:31:05 UTC

Skip to content

Biz & IT

The perils of leaving computers unattended is about to get worse.

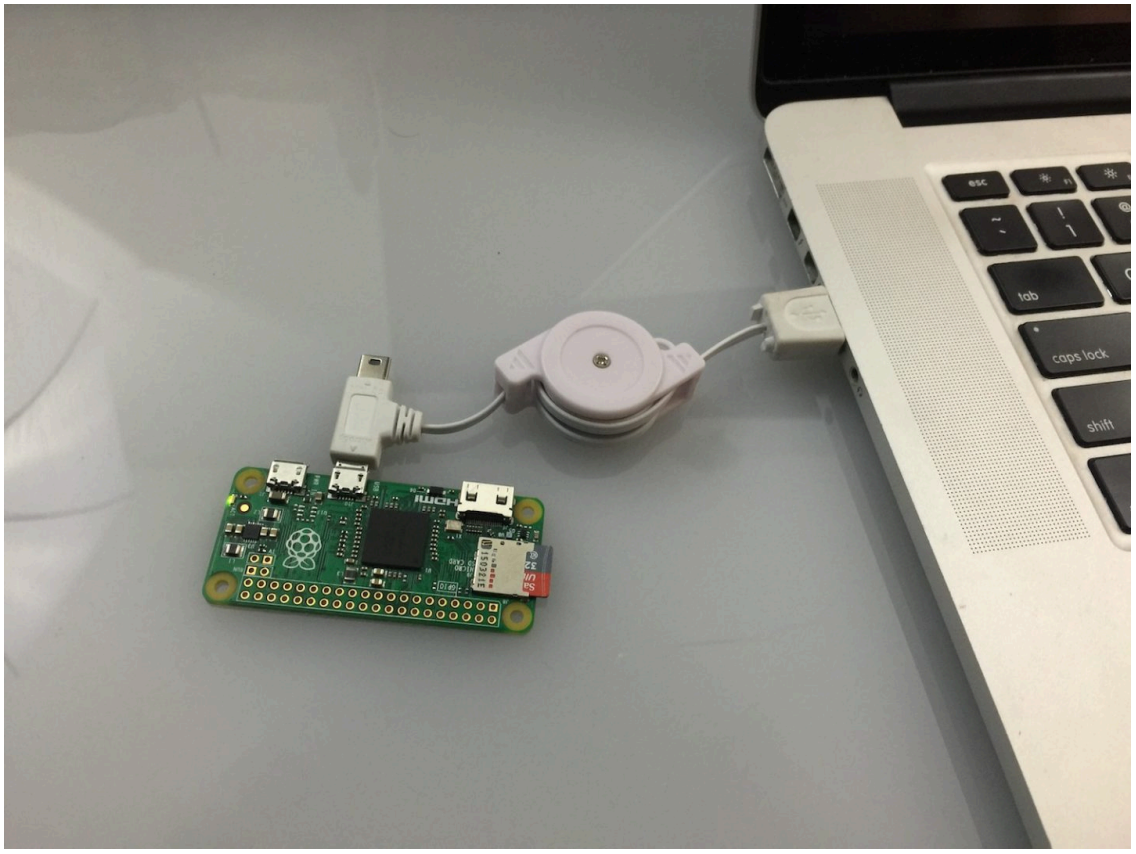


Credit: Samy Kamkar

Credit: Samy Kamkar

The perils of leaving computers unattended just got worse, thanks to a newly released exploit tool that takes only 30 seconds to install a privacy-invading backdoor, even when the machine is locked with a strong password.

PoisonTap, as the tool has been dubbed, runs freely available software on a $5/£4 Raspberry Pi Zero device. Once the payment card-sized computer is plugged into a computer's USB slot, it intercepts all unencrypted Web traffic, including any authentication cookies used to log in to private accounts. PoisonTap then sends that data to a server under the attacker's control. The hack also installs a backdoor that makes the owner's Web browser and local network remotely controllable by the attacker.



Credit: Samy Kamkar

Credit: Samy Kamkar

PoisonTap is the latest creation of Samy Kamkar, the engineer behind a long line of low-cost hacks, including a password-pilfering keylogger disguised as a USB charger, a key-sized dongle that jimmies open electronically locked cars and garages, and a DIY stalker app that mined Google Streetview. While inspiring for their creativity and elegance, Kamkar's inventions also underscore the security and privacy tradeoffs that arise from an increasingly computerized world. PoisonTap continues this cautionary theme by challenging the practice of password-protecting an unattended computer rather than shutting it off or, a safer bet still, toting it to the restroom or lunch room.

Kamkar told Ars:

> The primary motivation is to demonstrate that even on a password-protected computer running off of a WPA2 Wi-Fi, your system and network can still be attacked quickly and easily. Existing non-HTTPS website credentials can be stolen, and, in fact, cookies from HTTPS sites that did not properly set the 'secure' flag on the cookie can also be siphoned.

Unsecured home or office routers are similarly at risk. Kamkar has published the PoisonTap source code and additional technical details here and has also released the following video demonstration:

PoisonTap – exploiting locked machines w/ Raspberry Pi Zero.

Once the device is inserted in a locked Mac or PC (Kamkar said he hasn't tested PoisonTap on a Linux machine), it surreptitiously poisons the browser cache with malicious code that lives on well after the tool is removed. That makes the hack ideal for infecting computers while they are only briefly unattended. Here's how it works.

Once the PoisonTap software is installed, the Raspberry Pi device becomes a miniature Linux computer that presents itself as an Ethernet network. Like a router, it's responsible for allocating IP addresses for the local network through the dynamic host configuration protocol. In the process, the device becomes the gateway for sending and receiving traffic flowing over the local network. In this sense, PoisonTap is similar to a USB exploit tool demonstrated in September that stole login credentials from locked PCs and Macs.

Through a clever hack, however, PoisonTap is able to become the gateway for all Internet traffic as well. It does this by defining the local network to include the entire IPv4 address space. With that, the device has the ability to monitor and control all unencrypted traffic the locked computer sends or receives over its network connection.

PoisonTap then searches the locked computer for a Web browser running in the background with an open page. When it finds one, the device injects HTML iframe tags into the page that connect to the top 1 million sites ranked by Alexa. Because PoisonTap masquerades as the HTTP server for each site, the hack is able to receive, store, and upload any non-encrypted authentication cookies the computer uses to log in to any of those sites.

Given its highly privileged man-in-the-middle position, PoisonTap can also install backdoors that make both the Web browser and connected router remotely accessible to the attacker. To expose the browser, the hack leaves a combination of HTML and JavaScript in the browser cache that produces a persistent WebSocket. PoisonTap uses what's known as a DNS rebinding attack to give remote access to a router.

That means attackers can use PoisonTap to remotely access a browser as it connects to a website or to gain administrative control over the connected router. Attackers still must overcome any password protections safeguarding an exposed router. But given the large number of unpatched authentication bypass vulnerabilities or default credentials that are never changed, such protections often don't pose much of an obstacle.

PoisonTap challenges a tradition that can be found in almost any home or office—the age-old practice of briefly leaving a locked computer unattended. And for that reason, the ease and thoroughness of the hack may be understandably unsettling for some people. Still, several safeguards can significantly lower the threat posed by the hack. The first is to, whenever possible, use sites that are protected by HTTPS encryption and the transmission of secure cookies to prevent log-in credentials from being intercepted. A measure known as HTTP Strict Transport

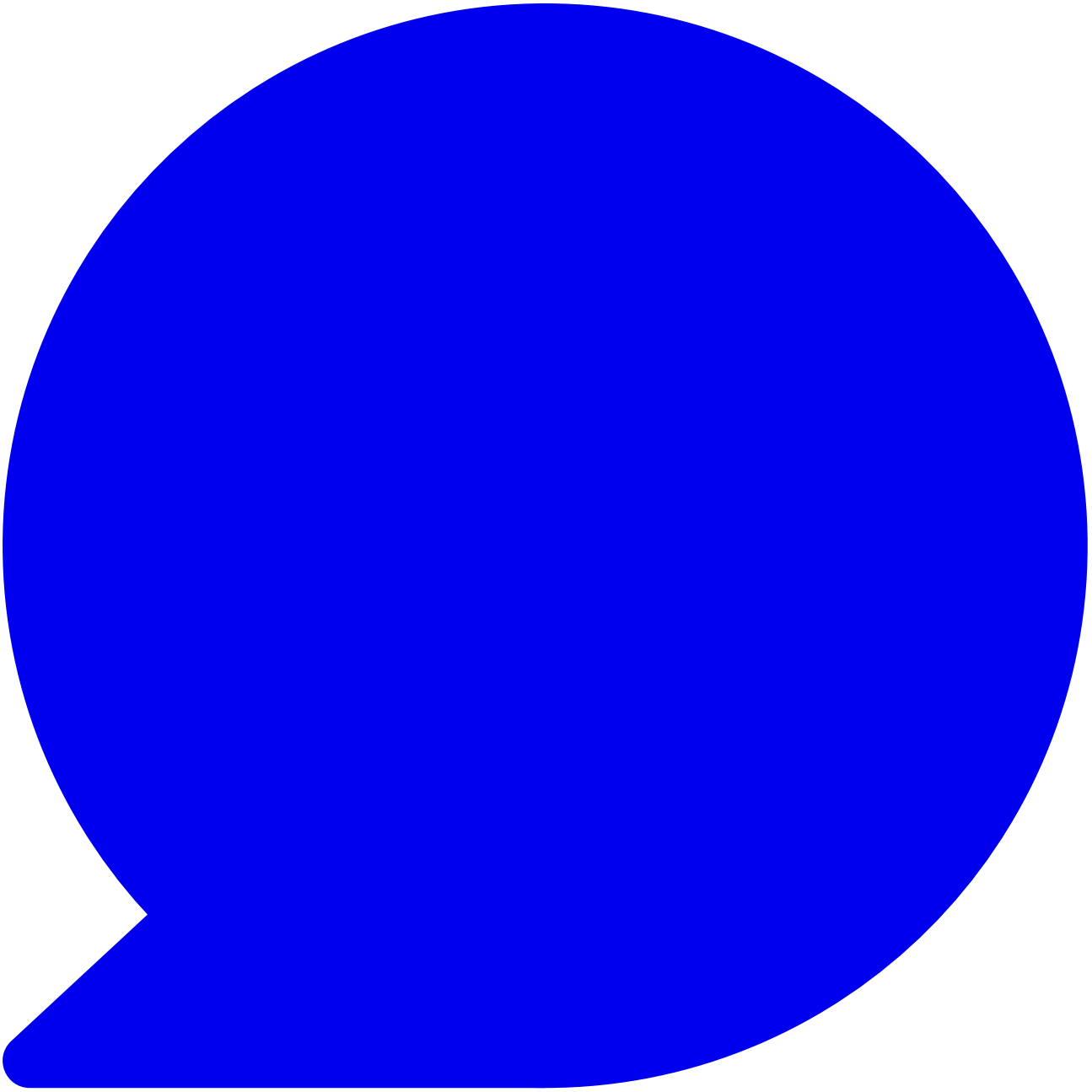
Security is better still, because it prevents attack techniques that attempt to downgrade HTTPS connections to unsecured HTTP.

As a result, neither Google nor Facebook pages can be triggered by computers infected by PoisonTap. Sadly, multi-factor authentication isn't likely to provide much protection because it generally isn't triggered by credentials provided in authentication cookies.

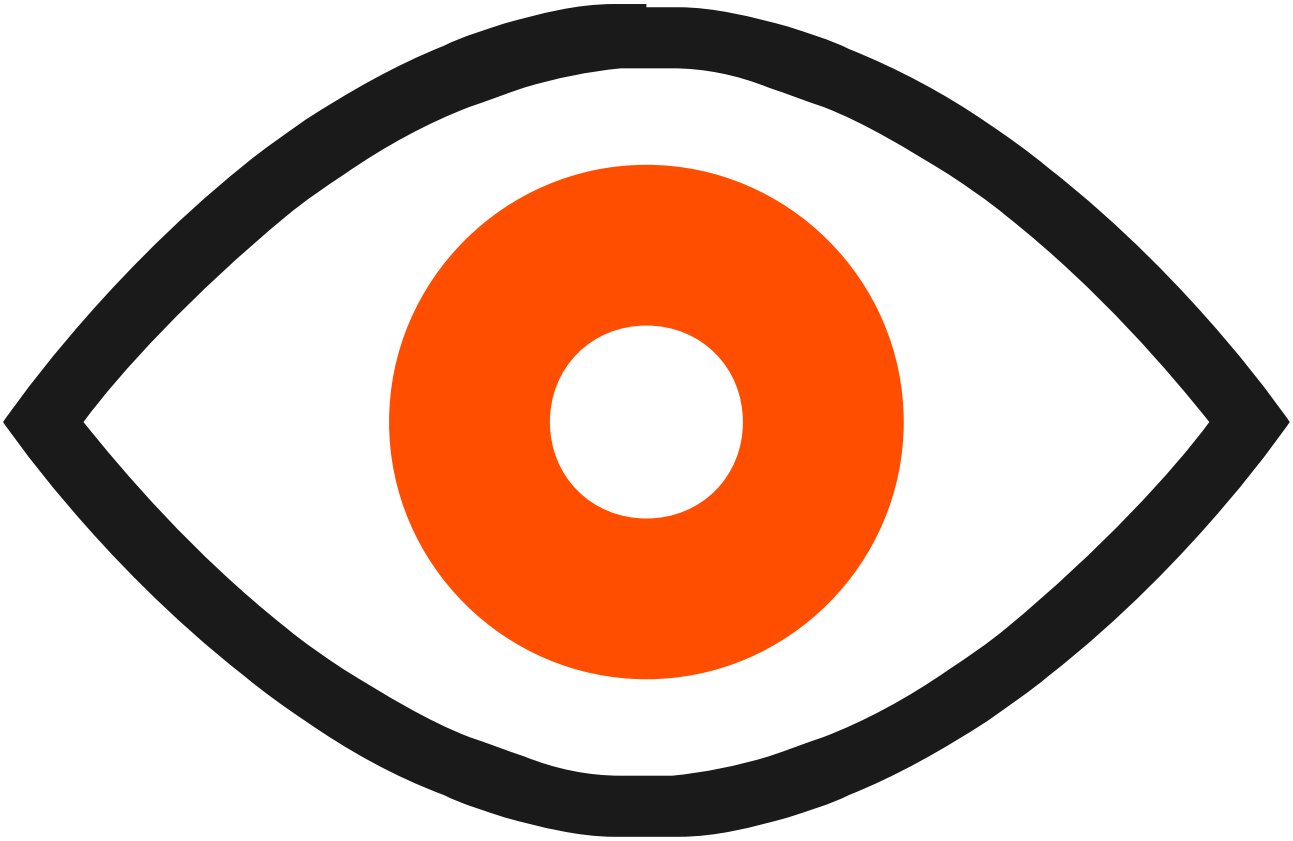
End users, meanwhile, should at a minimum close their browsers before locking their computer or, if they're on a Mac, be sure to enable FileVault2 and put their machine to sleep before walking away, since browsers are unable to make requests in such cases. Regularly flushing browser caches is also a sound, albeit imperfect, measure. For the truly paranoid, it may make more sense to simply bring laptops along or to turn off machines altogether.

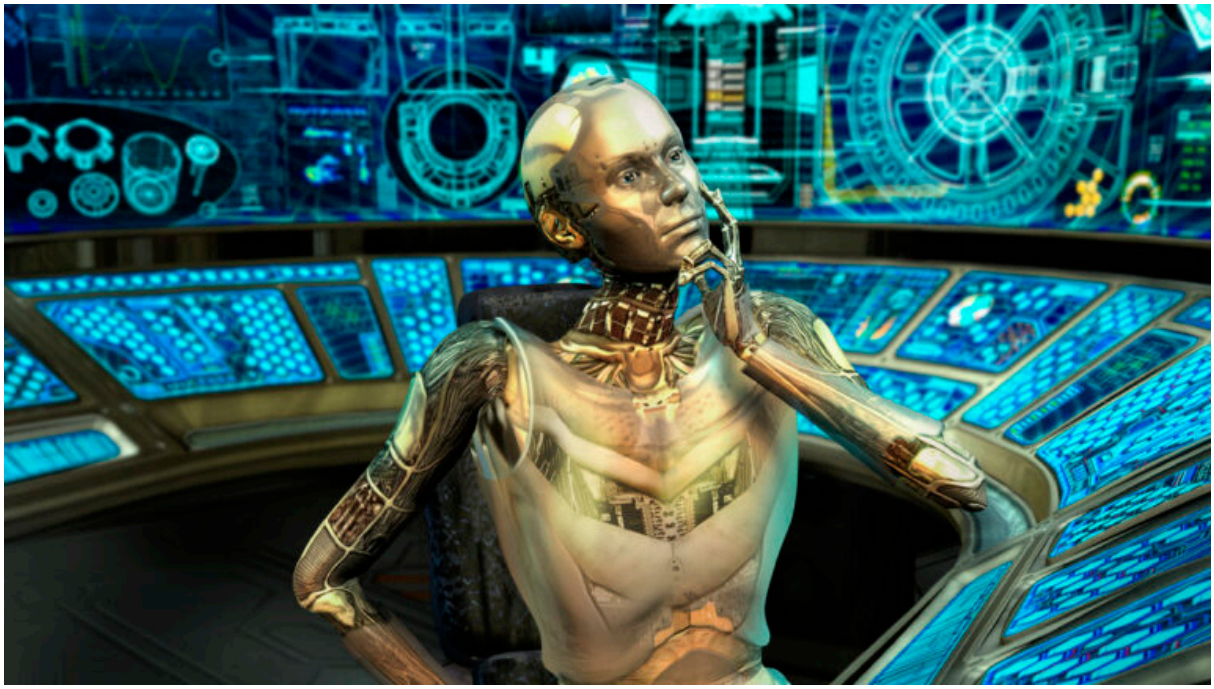
Listing image: Samy Kamkar

Dan Goodin is Senior Security Editor at Ars Technica, where he oversees coverage of malware, computer espionage, botnets, hardware hacking, encryption, and passwords. In his spare time, he enjoys gardening, cooking, and following the independent music scene. Dan is based in San Francisco. Follow him at here on Mastodon and here on Bluesky. Contact him on Signal at DanArs.82.



102 Comments



1. 
2.
3.
4.
5.

Source: http://arstechnica.com/security/2016/11/meet-poisontap-the-5-tool-that-ransacks-password-protected-computers/