Thousands of Linux systems infected by stealthy malware since 2021

This Reddit comment posted to the CentOS subreddit is typical. An admin noticed that two servers were infected with a cryptocurrency hijacker with the names perfcc and perfctl. The admin wanted help investigating the cause.

“I only became aware of the malware because my monitoring setup alerted me to 100% CPU utilization,” the admin wrote in the April 2023 post. “However, the process would stop immediately when I logged in via SSH or console. As soon as I logged out, the malware would resume running within a few seconds or minutes.” The admin continued:

> *I have attempted to remove the malware by following the steps outlined in other forums, but to no avail. The malware always manages to restart once I log out. I have also searched the entire system for the string “perfcc” and found the files listed below. However, removing them did not resolve the issue. as it keep respawn on each time rebooted.*

Other discussions include: Reddit, Stack Overflow (Spanish), forobeta (Spanish), brainycp (Russian), natnetwork (Indonesian), Proxmox (Deutsch), Camel2243 (Chinese), svrforum (Korean), exabytes,>virtualmin,>serverfault and many others.

After exploiting a vulnerability or misconfiguration, the exploit code downloads the main payload from a server, which, in most cases, has been hacked by the attacker and converted into a channel for distributing the malware anonymously. An

attack that targeted the researchers’ honeypot named the payload httpd. Once executed, the file copies itself from memory to a new location in the /temp directory, runs it, and then terminates the original process and deletes the downloaded binary.

Once moved to the /tmp directory, the file executes under a different name, which mimics the name of a known Linux process. The file hosted on the honeypot was named sh. From there, the file establishes a local command-and-control process and attempts to gain root system rights by exploiting CVE-2021-4043, a privilege-escalation vulnerability that was patched in 2021 in Gpac, a widely used open source multimedia framework.

https://arstechnica.com/security/2024/10/persistent-stealthy-linux-malware-has-infected-thousands-since-2021/