Asus just patched the ShadowHammer malware that was masquerading as a security update

That “critical” software update for your Asus computer may have actually been malware, planted by hackers in a targeted attack now known as “ShadowHammer,” we learned yesterday. Now, Asus says it has a fix in the form of an actual security update — one that you can download using its Live Update software tool.

In addition, the company says it has a second “security diagnostic” tool you can use to scan to see if your computer has been affected. “[W]e encourage users who are still concerned to run it as a precaution,” reads part of the company’s press release, which includes a link to the software.

The company’s press release notably does *not* include an apology, and it downplays the hack, stating that “Only a very small number of specific user group were found to have been targeted.” Cybersecurity firm Kaspersky Lab had previously estimated that the malware could have been distributed to as many as 1 million computers, and installed on hundreds of thousands of those machines, which doesn’t sound like a small number to me. Both Kaspersky and Symantec say they’d identified the malware in at least tens of thousands of cases.

However, Asus does say it’s taken steps to ensure such a trojan horse won’t make it through again, including “multiple security verification mechanisms to prevent any malicious

manipulation” and “an enhanced end-to-end encryption mechanism.”

“At the same time, we have also updated and strengthened our server-to-end-user software architecture to prevent similar attacks from happening in the future,” Asus says.

https://www.theverge.com/2019/3/26/18283039/asus-just-patched-the-shadowhammer-malware-that-was-masquerading-as-a-security-update