# Some ASUS Updates Drop Backdoors on PCs in 'Operation ShadowHammer'

By Tara Seals

Published: 2019-03-25 · Archived: 2026-04-05 23:16:02 UTC

The attack appears to be associated with a China-backed APT actor.

A supply-chain attack dubbed "Operation ShadowHammer" has been uncovered, targeting users of the ASUS Live Update Utility with a backdoor injection. The China-backed BARIUM APT is suspected to be at the helm of the project.

According to Kaspersky Lab, the campaign ran from June to at least November 2018 and may have impacted more than a million users worldwide – though the adversaries appear to have been after specific victims in Asia.

The threat surface is not small: The ASUS Live Update Utility is a pre-installed utility in most new ASUS computers, for automatic BIOS, UEFI, drivers and applications updates. Popular among gamers, ASUS ranks fifth in the laptop market, with a market share of 7.4 percent as of August 2018, according to TrendForce. With an estimated 41.08 million laptops shipped in that quarter, it means ASUS sold around 3 million of them for that time period. Gartner meanwhile pegged ASUS' overall PC sales, including desktops and notebooks, to be just over 4 million in the third quarter of 2018 (translating into a 6 percent overall PC market share).



To compromise the utility, Kaspersky Lab determined that the cyberattackers used stolen digital certificates used by ASUS to sign legitimate binaries, and altered older versions of ASUS software to inject their own malicious code. Trojanized versions of the utility were then signed with legitimate certificates and were hosted on and distributed from official ASUS update servers – which made them mostly invisible to the vast majority of protection solutions, according to Kaspersky Lab.

While this means that potentially every user of the affected software could have become a victim, researchers said that, true to their APT nature, the attackers were interested in a specific subset of users. About 600 hard-coded MAC addresses were found in the backdoor code (MAC addresses uniquely identify a network adaptor that connects a computer to a network); if the victim's machine didn't match up with one of the specified MAC addresses, the malware went dormant. If it did, the malware downloaded the next payload.

In all, there were about 230 different backdoored samples seen by researchers taking aim at those Mac addresses.

"The modular approach and extra precautions taken when executing code, to prevent accidental code or data leakage, indicates that it was very important for the actors behind this sophisticated attack to remain undetected, while hitting some very specific targets with surgical precision," researchers said in a posting on Monday. "Deep

technical analysis shows that the arsenal of the attackers is very advanced and reflects a very high level of development within the group."

It should be noted that the backdoors dropped on other ASUS users' PCs presumably remain there, even if they weren't "activated" by matching one of the MAC addresses. It's unclear whether there's the potential for further attacks on this group.

"The selected vendors are extremely attractive targets for APT groups that might want to take advantage of their vast customer base," said Vitaly Kamluk, director of Global Research and Analysis Team, APAC, at Kaspersky Lab. "It is not yet very clear what the ultimate goal of the attackers was, and we are still researching who was behind the attack."

That said, the "fingerprints" left on the samples by the attackers – including techniques used to achieve unauthorized code execution – suggest that the BARIUM APT is behind the effort, according to the researchers. BARIUM, a Chinese state player that also goes by APT17, Axiom and Deputy Dog, was previously linked to the ShadowPad and CCleaner incidents, which were also supply-chain attacks. that used software updates to sneak onto machines.

In the 2017 ShadowPad attack, the update mechanism for Korean server management software provider NetSarang was compromised to serve up an eponymous backdoor. NetSarang, which has headquarters in South Korea and the United States, removed the backdoored update, but not before it was activated on at least one victim's machine in Hong Kong.

In the next incident, also in 2017, software updates for the legitimate computer cleanup tool CCleaner was found to have been compromised by hackers to taint them with the same ShadowPad backdoor. The incident exposed millions of computers but, like ShadowHammer, out of 1.65 million malware installs, only a few, about 40, were of interest to the attackers. From there, 11 companies were ultimately infiltrated. Once the backdoor is activated on a targeted machine, various keyloggers and other data-gathering payloads were then fetched from command-and-control.

ASUS is also not alone in being used as a conduit for attacks; Kaspersky Lab researchers said that the search for similar malware has revealed software from three other vendors in Asia have all been backdoored with very similar methods and techniques.

Kaspersky Lab said that it has reported the issue to ASUS and other vendors but has not received a response. Threatpost has also reached out to the PC-maker and will update this post with any comments or responses.

---