# Operation ShadowHammer: new supply chain attack threatens hundreds of thousands of users worldwide

By Kaspersky

Published: 2019-03-25 · Archived: 2026-04-02 12:15:21 UTC

**Kaspersky Lab has uncovered a new advanced persistent threat (APT) campaign that has affected a large number of users through what is known as a supply chain attack. Our research found that threat actors behind Operation ShadowHammer have targeted users of the ASUS Live Update Utility, by injecting a backdoor into it at least between June and November 2018. Kaspersky Lab experts estimate that the attack may have affected more than a million users worldwide.**

A supply chain attack is one of the most dangerous and effective infection vectors, increasingly exploited in advanced operations over the last few years – as we have seen with ShadowPad or CCleaner. It targets specific weaknesses in the interconnected systems of human, organizational, material, and intellectual resources involved in the product life cycle: from initial development stage through to the end user. While a vendor's infrastructure can be secure, there could be vulnerabilities in its providers' facilities that would sabotage the supply chain, leading to a devastating and unexpected data breach.

The actors behind ShadowHammer targeted the ASUS Live Update Utility as the initial source of infection. This is a pre-installed utility in most new ASUS computers, for automatic BIOS, UEFI, drivers and applications updates. Using stolen digital certificates used by ASUS to sign legitimate binaries, the attackers have tampered older versions of ASUS software, injecting their own malicious code. Trojanized versions of the utility were 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.

While this means that potentially every user of the affected software could have become a victim, actors behind ShadowHammer were focused on gaining access to several hundreds of users, which they had prior knowledge about. As Kaspersky Lab's researchers discovered, each backdoor code contained a table of hardcoded MAC addresses – the unique identifier of network adapters used to connect a computer to a network. Once running on a victim's device, the backdoor verified its MAC address against this table. If the MAC address matched one of the entries, the malware downloaded the next stage of malicious code. Otherwise, the infiltrated updater did not show any network activity, which is why it remained undiscovered for such a long time. In total, security experts were able to identify more than 600 MAC addresses. These were targeted by over 230 unique backdoored samples with different shellcodes.

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

The search for similar malware has revealed software from three other vendors in Asia, all backdoored with very similar methods and techniques. Kaspersky Lab has reported the issue to Asus and other vendors.

"*The selected vendors are extremely attractive targets for APT groups that might want to take advantage of their vast customer base. It is not yet very clear what the ultimate goal of the attackers was and we are still researching who was behind the attack. However, techniques used to achieve unauthorized code execution, as well as other discovered artefacts suggest that ShadowHammer is probably related to the BARIUM APT, which was previously linked to the ShadowPad and CCleaner incidents, among others. This new campaign is yet another example of how sophisticated and dangerous a smart supply chain attack can be nowadays,*" said Vitaly Kamluk, Director of Global Research and Analysis Team, APAC, at Kaspersky Lab.

All Kaspersky Lab products successfully detect and block the malware used in Operation ShadowHammer.

In order to avoid falling victim to a targeted attack by a known or unknown threat actor, Kaspersky Lab researchers recommend implementing the following measures:

- In addition to adopting must-have endpoint protection, implement a corporate grade security solution which detects advanced threats on the network level at an early stage, such as Kaspersky Anti Targeted Attack Platform;
- For endpoint level detection, investigation and timely remediation of incidents, we recommend implementing EDR solutions such as Kaspersky Endpoint Detection and Response or contacting a professional incident response team;
- Integrate Threat Intelligence feeds into your SIEM and other security controls in order to get access to the most relevant and up-to-date threat data and prepare for future attacks.

Kaspersky Lab will present full findings on Operation ShadowHammer at Security Analyst Summit 2019, in Singapore, 9-11 April.

A full report on the ShadowHammer campaign is already available to customers of Kaspersky Intelligence Reporting Service.

A blog summarizing the attack as well as a special tool designed to validate whether users' devices were a target can also be found on Securelist. The validation is also available on a separate website.

**About Kaspersky Lab**

*Kaspersky Lab is a global cybersecurity company, which has been operating in the market for over 21 years. Kaspersky Lab's deep threat intelligence and security expertise is constantly transforming into next generation security solutions and services to protect businesses, critical infrastructure, governments and consumers around the globe. The company's comprehensive security portfolio includes leading endpoint protection and a number of specialized security solutions and services to fight sophisticated and evolving digital threats. Over 400 million users are protected by Kaspersky Lab technologies and we help 270,000 corporate clients protect what matters most to them.*

Source: https://www.kaspersky.com/about/press-releases/2019_operation-shadowhammer-new-supply-chain-attack