CERT-EU
FOR THE EU INSTITUTIONS, BODIES AND AGENCIES

Security Advisory 2019-007

Operation ShadowHammer – Compromised ASUS Computers

March 27, 2019 — v1.1

TLP:WHITE

History:

- *26/03/2019 — v1.0 – Initial publication*
- *27/03/2019 — v1.1 – Version updated with information about ASUS fix*

Summary

In January 2019, Kaspersky [1, 2] has discovered a supply chain attack that affects ASUS computers. Dubbed *Operation ShadowHammer*, the operation took place from June to November 2018. It is similar to other supply chain attacks on Netsarang and CCleaner [3]. Around 500 thousands of computers could have been potentially impacted, although the malware seems to have been only targeting a few hundred (around 660 identified so far) specific MAC addresses [2]. ASUS has now released a fix and a diagnostic tool [6, 7].

Technical Details

ASUS Live Update is a utility that is pre-installed on most ASUS computers and is used to automatically update certain components such as BIOS, UEFI, drivers and applications. According to Gartner, ASUS is the world's 5th-largest PC vendor by 2017 unit sales. This makes it an extremely attractive target for APT groups that might want to take advantage of their user-base.

The researchers estimate that roughly 500,000 Windows computers received the malicious backdoor through the ASUS update server, although the attackers appear to have been targeting only about 600 of those systems. Indeed, the goal of the attack was to surgically target an unknown pool of users, which were identified by their network adapters' MAC addresses. To achieve this, the attackers had hardcoded a list of MAC addresses in the trojanized samples and this list was used to identify the actual intended targets of this massive operation. The attack sequence can hence be summarized as follows:

1) The trojanized ASUS software is delivered from legitimate update servers and signed with legitimate certificates,
2) Once installed, the malicious code checks for the infected computer's MAC address,
3) If the MAC address matches a predetermined list, the malicious code delivers a second-stage payload.

This indicates that the incident was highly tailored to a very small set of preselected targets and that the actor possessed foreknowledge of their desired targets, or rapidly developed their target list as their operation progressed. Researchers were able to extract more than 600 unique MAC addresses from over 200 samples used in this attack. Of course, there might be other samples out there with different MAC addresses in their list.

Researchers assess that this supply chain attack matches or even surpasses the Shadowpad and the CCleaner incidents in complexity and techniques. It stayed undetected for so long partly due to the fact that the trojanized updaters were signed with legitimate certificates (e.g.: `ASUSTeK Computer Inc.`). In this case the attack relied on the trust that users or companies place into software that is automatically updated and the companies/infrastructures behind them.

A limited list of IoCs has been released and a more comprehensive list will be available next April during the SAS 2019 security conference [5].

Products Affected

ASUS products that utilise Live Update.

Recommendations

ASUS has implemented a fix in the latest version (ver. 3.6.8) of the Live Update software, introduced multiple security verification mechanisms to prevent any malicious manipulation in the form of software updates or other means, and implemented an enhanced end-to-end encryption mechanism [6]. All users are encouraged to update as soon as possible.

Kaspersky provided a tool to check if a MAC address is among those that had been targeted [4]. Additionally, ASUS has created an online security diagnostic tool to check for affected systems, and users who are concerned are encouraged to run it as a precaution [7].

References

[1] https://motherboard.vice.com/en_us/article/pan9wn/hackers-hijacked-asus-software-updates-to-install-backdoors-on-thousands-of-computers

[2] https://securelist.com/operation-shadowhammer/89992/

[3] https://www.cnet.com/news/hackers-took-over-asus-updates-to-send-malware-researchers-found/

[4] https://shadowhammer.kaspersky.com/

[5] https://sas.kaspersky.com/

[6] https://www.asus.com/News/hqfgVUyZ6uyAyJe1

[7] https://dlcdnets.asus.com/pub/ASUS/nb/Apps_for_Win10/ASUSDiagnosticTool/ASDT_v1.0.1.0.zip