Operation ShadowHammer

By GReAT

Published: 2019-03-25 · Archived: 2026-04-02 10:47:26 UTC

Earlier today, Motherboard published a story by Kim Zetter on Operation ShadowHammer, a newly discovered supply chain attack that leveraged ASUS Live Update software.

While the investigation is still in progress and full results and technical paper will be published during SAS 2019 conference in Singapore, we would like to share some important details about the attack.

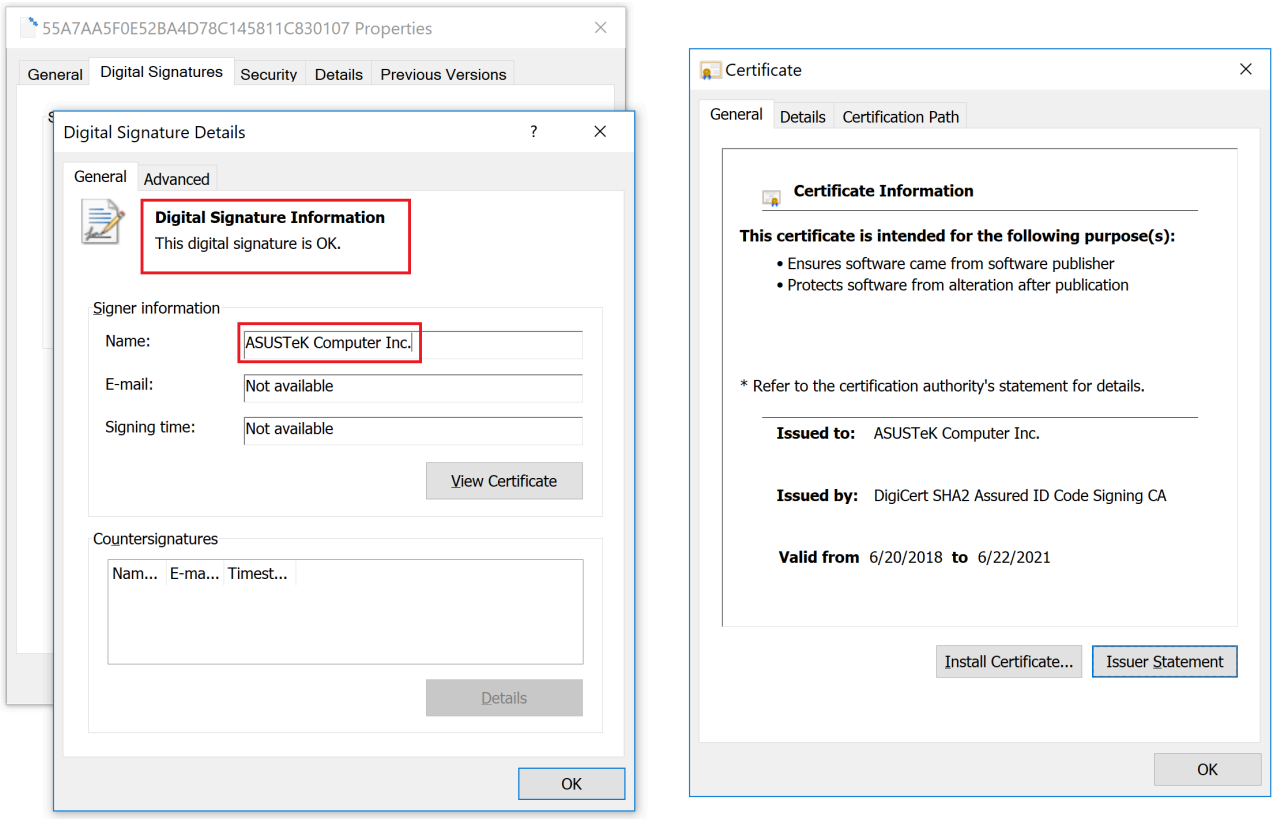
In January 2019, we discovered **a sophisticated supply chain attack involving the ASUS Live Update Utility**. The attack took place between June and November 2018 and according to our telemetry, it affected a large number of users.

ASUS Live Update is an 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 userbase.

Based on our statistics, **over 57,000 Kaspersky users have downloaded and installed the backdoored version of ASUS Live Update** at some point in time. We are not able to calculate the total count of affected users based only on our data; however, we estimate that the real scale of the problem is much bigger and is possibly affecting over a million users worldwide.

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. We 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.

We believe this to be a very sophisticated supply chain attack, which matches or even surpasses the Shadowpad and the CCleaner incidents in complexity and techniques. The reason that it stayed undetected for so long is partly due to the fact that the trojanized updaters were signed with legitimate certificates (eg: "ASUSTeK Computer Inc."). The malicious updaters were hosted on the official liveupdate01s.asus[.]com and liveupdate01.asus[.]com ASUS update servers.

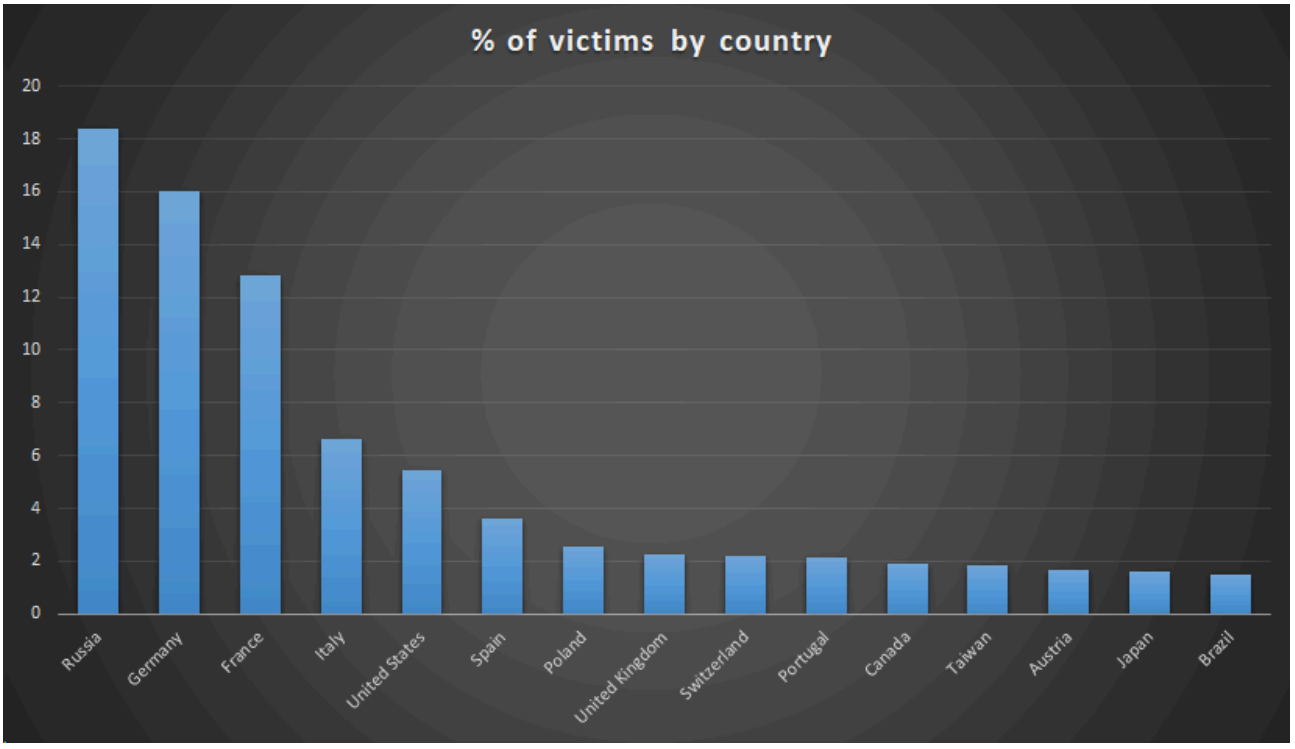


Digital signature on a trojanized ASUS Live Update setup installer
Certificate serial number: 05e6a0be5ac359c7ff11f4b467ab20fc

We have contacted ASUS and informed them about the attack on Jan 31, 2019, supporting their investigation with IOCs and descriptions of the malware.

Although precise attribution is not available at the moment, certain evidence we have collected allows us to link this attack to the ShadowPad incident from 2017. The actor behind the ShadowPad incident has been publicly identified by Microsoft in court documents as BARIUM. BARIUM is an APT actor known to be using the Winnti backdoor. Recently, our colleagues from ESET wrote about another supply chain attack in which BARIUM was also involved, that we believe is connected to this case as well.

A victim distribution by country for the compromised ASUS Live Updater looks as follows:



It should be noted that the numbers are also highly influenced by the distribution of Kaspersky users around the world. In principle, the distribution of victims should match the distribution of ASUS users around the world.

We've also created a tool which can be run to determine if your computer has been one of the surgically selected targets of this attack. To check this, it compares MAC addresses of all adapters to a list of predefined values hardcoded in the malware and alerts if a match was found.

Download an archive with the tool (.exe)

Also, you may check MAC addresses online. If you discover that you have been targeted by this operation, please e-mail us at: shadowhammer@kaspersky.com

IOCs

Kaspersky Lab verdicts for the malware used in this and related attacks:

- HEUR:Trojan.Win32.ShadowHammer.gen

Domains and IPs:

- asushotfix[.]com
- 141.105.71[.]116

Some of the URLs used to distribute the compromised packages:

- hxxp://liveupdate01.asus[.]com/pub/ASUS/nb/Apps_for_Win8/LiveUpdate/Liveupdate_Test_VER365.zip
- hxxps://liveupdate01s.asus[.]com/pub/ASUS/nb/Apps_for_Win8/LiveUpdate/Liveupdate_Test_VER362.zip
- hxxps://liveupdate01s.asus[.]com/pub/ASUS/nb/Apps_for_Win8/LiveUpdate/Liveupdate_Test_VER360.zip

- hxxps://liveupdate01s.asus[.]com/pub/ASUS/nb/Apps_for_Win8/LiveUpdate/Liveupdate_Test_VER359.zip

Hashes (Liveupdate_Test_VER365.zip):

- aa15eb28292321b586c27d8401703494
- bebb16193e4b80f4bc053e4fa818aa4e2832885392469cd5b8ace5cec7e4ca19

A full set of IOCs and Yara rules is available to customers of Kaspersky Intelligence Reporting service – contact intelreports@kaspersky.com

---