SAS 2019

Search blog posts

ShadowHammer: Malicious updates for ASUS laptops

Our technologies detected a threat that seems to be one of the biggest supply-chain attacks ever.

Bender the Robot

March 25, 2019

SAS SAS 2019

supply chain

updates

Thanks to a new technology in our products that is capable of detecting supply-chain attacks, our experts have uncovered what seems to be one of the biggest supply-chain incidents ever (remember CCleaner? This one's bigger). A threat actor modified the ASUS Live Update Utility, which delivers BIOS, UEFI, and software updates to ASUS laptops and desktops, added a back door to the utility, and then distributed it to users through official channels.

The trojanized utility was signed with a legitimate certificate and was hosted on the official ASUS server dedicated to updates, and that allowed it to stay undetected for a long time. The criminals even made sure the file size of the malicious utility

Related

stayed the same as that of the original one.

According to our statistics, more than 57,000 users of Kaspersky Lab's products have installed the backdoored utility, but we estimate it was distributed to about 1 million people total. The cybercriminals behind it were not interested in all of them, however — they targeted only 600 specific MAC addresses, for which the hashes were hardcoded into different versions of the utility. To check if your MAC address is on the target list, use our tool, which you'll find at https://shadowhammer.kaspersky.com/.

While investigating this attack, we found out that the same techniques were used against software from three other vendors. Of course, we have notified ASUS and other companies about the attack. As of now, all Kaspersky Lab solutions detect and block the trojanized utilities, but we still suggest that you update the ASUS Live Update Utility if you use it. Our investigation is still ongoing.

If you want to learn more about one of the biggest supply-chain attacks ever, dive deep into technical details, see the IOCs, understand who the targets were, and get some advice on how to protect yourself from supply-chain attacks such as this one, we suggest visiting the SAS 2019 — the warmest security conference opens its doors on April 8 in Singapore. There we'll have a talk dedicated to the ShadowHammer APT with a lot of

Beekeeper vs. cybercrime

Malicious code discovered in Linux distributions interesting details. The tickets are almost sold out, so you'd better hurry.

Alternatively, you can read our full report, which will also become available during the SAS, on securelist.com. Stay tuned!

Read next

Transatlantic Cable podcast, episode 83

The latest on the Norsk Hydro ransomware plague, the EU preparing for EU-wide cyberattack, a snafu with Sprint, and more.

March 21, 2019

Tips

Tips

Is it the boss — or is it a fraudster? Scams disguised as urgent orders from top brass

Got a message from your boss or coworker asking you to “fix a problem” in an unexpected way? Beware of scammers! How to protect yourself and your company against a potential attack.

March 28, 2024

Tips

How to prepare for Living Off the Land (LotL) attacks

To go undetected, attackers can operate in your network without any malware at all. How to detect them and prevent damage?

March 22, 2024

Tips

Tips

Neither flowers nor gifts: how women get scammed

Another celebration… for scammers. How cybercriminals scam women ahead of March 8.

March 7, 2024

Securing home security

Security companies offer smart technologies — primarily cameras — to protect your home from burglary, fire and other incidents. But what about protecting these security systems themselves from intruders? We fill this gap.

March 5, 2024

Sign up to receive our headlines in your inbox

Email Address

□ I agree to provide my email address to “AO Kaspersky Lab” to receive information about new posts on the site. I understand that I can withdraw this consent at any time via e-mail by clicking the “unsubscribe” link that I find at the bottom of any e-mail sent to me for the purposes mentioned above.

Home Solutions

Kaspersky Standard

Kaspersky Plus

Kaspersky Premium

All Solutions

Small Business Products

Kaspersky Small Office Security

Kaspersky Endpoint Security Cloud

All Products

Medium Business Products

Kaspersky Endpoint Security Cloud

Kaspersky Endpoint Security for Business Select

Kaspersky Endpoint Security for Business Advanced

All Products

Enterprise Solutions

Cybersecurity Services

Threat Management and Defense

Endpoint Security

Hybrid Cloud Security

All Solutions

Privacy Policy Anti-Corruption Policy License Agreement B2C License Agreement B2B

Contact Us About Us Partners Blog Resource Center Press Releases Sitemap

Securelist • Eugene Personal Blog • Encyclopedia