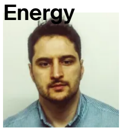
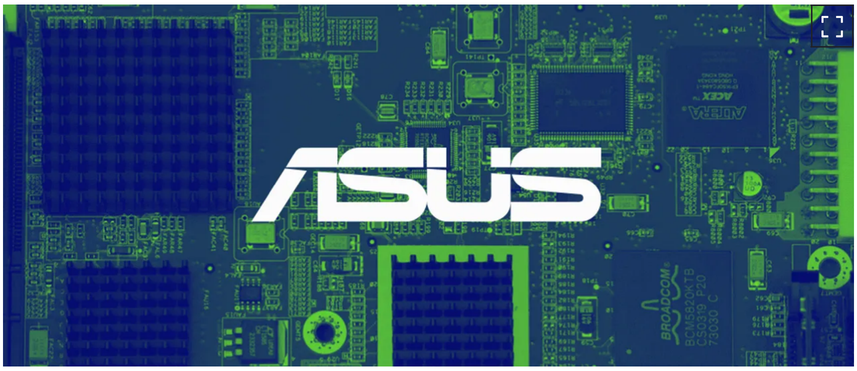
Researchers publish list of MAC add targeted in ASUS hack

Most of the targeted MAC addresses are used by ASUStek, Intel, and AzureWave devices.



Written by **Catalin Cimpanu,** Contributor
March 29, 2019 at 8:50 a.m. PT



Logo: ASUS // Composition: ZDNet

Security researchers from Skylight Cyber have published today a list containing the 583 MAC addresses that hackers had targeted using the recent ASUS hack.

The Skylight team obtained this list by reverse engineering a Windows app created by Kaspersky Lab to let ASUS users test if their computers were of interest to hackers.

The ASUS hack happened last year when suspected Chinese hackers breached the ASUS IT

/ security

Do you need antivirus on Linux?

6 ways to protect yourself from getting scammed online, by phone, or IRL

The best VPN free trials for 2024

8 habits of highly secure remote workers

ZD NET INNOVATION INDEX

rank		trend	
1	new	Google now shows AI	→
2	new	Google Maps introduces	→
3	new	Microsoft integrates	→
4	new	Claude 3 LLM surpasses	→

read full trend report →

/ related

Th
an

M
Ap
th

Ap
M
$2
Bi

infrastructure and backdoored the company's Live Update tool that's installed on all ASUS notebooks to help with automatic firmware updates.

How to find and remove spyware from your phone

Not all ASUS users were targeted during this hack. The backdoored Live Update tool would only install additional malware on certain computers that had a specific MAC address for their network interfaces.

When the ASUS hack become public earlier this week, Kaspersky published an app that would check users' computers and report if they were on the hackers' very small list of potential targets.

"Kaspersky was probably distributing those [MAC] lists through their paid service," a Skylight Cyber spokesperson told *ZDNet* earlier today. "Now, the unhashed list is free for everyone to use, researchers and organizations alike."

What's on the list?

Although the MAC list was made public today for the first time in a cleartext version, its content was never a secret.

Lists containing the MAC addresses in a hashed version have been going around the web all week --for example, this version uploaded on GitHub.

Other security firms, like Qihoo 360, were already analyzing it even before today. *ZDNet* also received a cleartext copy earlier this week and had been looking into the vendors' whose MAC addresses were included on the list.

Image: Qihoo 360

The vast majority of these MAC addresses belong to large corporations ASUStek, Intel, and AzureWave. Almost all vendors included on the list, even the ones who had just a handful of MAC addresses targeted, are makers of WiFi-capable devices.

An industry insider told *ZDNet* that while this might suggest that the purpose of Operation ShadowHammer (the codename given to the ASUS hack) might be to target certain types of WiFi capable systems, the small number of MAC addresses that hackers selected actually proves the opposite point --that they were after selected targets, rather than mass-targeting generic WiFi-capable devices as a whole.

Attackers knew exactly who they wanted to hack

Costin Raiu, one of the Kaspersky Lab researchers involved in the ShadowHammer investigation, also told *ZDNet* that no conclusions could be drawn from this MAC list.

Attackers can determine the MAC address of a device without compromising it, through a technique called network scanning.

Raiu said the target list was most likely put together after reconnaissance operations in previous attacks, and it will be almost impossible to tell who hackers targeted. Only the device vendors would be able to answer these questions, and especially ASUS.

Furthermore, there have been different backdoored versions of the Live Update software, each targeting different MAC addresses. Sometimes these lists were small, and sometimes they contained hundreds of entries, as was highlighted by both Kaspersky and an F-Secure analysis published today.

This shows that the hackers' targeting changed as time went by, and as they either compromised desired victims, or realized some targets would be unreachable. This also suggests that hackers had full control over ASUS' infrastructure for months,and deployed different Live Update payloads to use in multiple operations, and not just one.

In other cases, the hackers wanted to infect devices that had two MAC addresses at the same time, confirming the theory that hackers knew in advance what they wanted to target, and were merely using the ASUS Live Update tool as a jumping point into desired systems.

> In some cases, the #shadowhammer backdoor checks both the NIC and WiFi adapter MACs to identify the victim for further exploitation. Second stage is deployed only if both addresses match. It was really that targeted.
>
> — Costin Raiu (@craiu) March 26, 2019

From the F-Secure report:

> **1) 0c:5b:8f:27:9a:64, which was found in 8 samples, appears to be a Huawei wireless chip address. It is not assigned to Huawei, but looks like it's being used in Huawei E3372 devices, which is a 4G USB stick. This particular MAC address is always checked along with a specific Asustek Computer Inc. MAC address.**
>
> **2) 00ff5eXXXXXX is always checked along with a VMWare MAC address, which suggests that this MAC address is used in virtualized environments.**

But in other cases, the targeting was way off. This wasn't because of the hackers' mistake, but because several hardware vendors reused the same MAC address for thousands of devices.

> I also wonder how many Huawei customers were inadvertently affected by the ASUS-delivered malware because Huawei apparently decided that using unique MAC addresses for each device was too much work. pic.twitter.com/h3jQicfglb
>
> — Will Dormann (@wdormann) March 29, 2019

> Apparently, one of the MACs targeted by #ShadowHammer is used on thousands of hosts: it is VMware VMNet8 adapter with default MAC 00:50:56:C0:00:08. If you got one of those - don't freak out. You were probably just a collateral target. Check if you ran ASUS Live Updater in 2018.
>
> — Vitaly Kamluk (@vkamluk) March 26, 2019

> Another case is 0C:5B:8F:27:9A:64. This one is used by Huawei E3772 USB 4G dongle and seems to be the same for all owners of such devices. Looks like #ShadowHammer targeting wasn't accurate in some cases and could cause unplanned infections.
>
> — Vitaly Kamluk (@vkamluk) March 26, 2019

What all this tells external observers is that the Operation ShadowHammer seems to the last stage of a larger hacking operation that most likely began with reconnaissance operations months before the actual ASUS hack.

Kaspersky said that hackers stopped delivering a backdoored version of the Live Update tool last November, suggesting that hackers might have hacked the targets they were after and moved to other operations since then.

ASUS released a clean version of the Live Update tool earlier this week.

These are the worst hacks, cyberattacks, and data breaches of 2018

→

More cybersecurity coverage:

- French gas stations robbed after forgetting to change gas pump PINs
- Microsoft takes control of 99 domains operated by Iranian state hackers
- North Korean hackers continue attacks on cryptocurrency businesses
- Top dark web marketplace will shut down next month
- Report deems Russia a pioneer in GPS spoofing attacks
- Toyota announces second security breach in the last five weeks
- We invited professional hackers to attack us CNET
- The 3 least secure programming languages TechRepublic

Editorial standards

show comments ↓

we equip you to harness the power of disruptive innovation, at work and at home.

topics

galleries

videos

do not sell or share my personal information

about ZDNET

meet the team

sitemap

reprint policy