Advisory from Maharashtra Cyber Office in response to **Operation ShadowHammer**

Issued by:
Maharashtra Cyber Office
Home Department
Govt of Maharashtra
Mantralaya
Mumbai

Kaspersky Labs has discovered a sophisticated supply chain attack involving the **ASUS Live Update** Utility affecting more than a million computer users worldwide through a campaign called **ShadowHammer**.

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.

The attack is estimated to have taken place between June and November 2018 and according to Kaspersky, has affected a large number of users.

Modus Operandi

- **Operation ShadowHammer** was a new advanced persistent threat (APT) campaign which targeted users of the ASUS Live Update Utility, injecting a backdoor.

- 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.

➔ 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.

➔ In total, security experts were able to identify more than 600 MAC addresses hard coded into the malware.

How to detect whether your ASUS device has been affected

To check whether your Asus device has been affected, Kaspersky Labs has developed an **online tool** which can determine if your computer has been one of the surgically selected targets of this attack. It compares MAC addresses of all adapters to a list of predefined values hardcoded in the malware and alerts if a match was found.

Please note that **only ASUS Windows users are affected**. If you own a device running MacOS or any of its distributions, you are not affected and need not check.

1. Visit https://shadowhammer.kaspersky.com/

2. Find out your device's MAC address using the steps below:

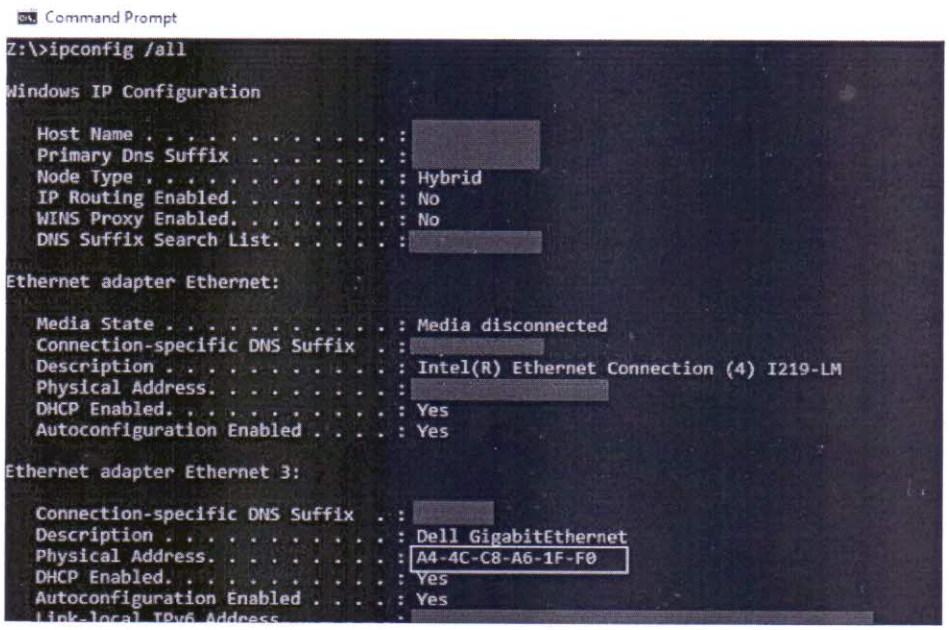
Run the command line terminal. To do this:

- On **Windows 10** – click on the magnifying glass pictogram near the "Start" button, enter "cmd" in the search dialog and press Enter, or click on the "Start" button, then select "Windows System" > "Command Prompt".

- On **Windows 8/8.1** – move your mouse into upper left corner to open the "Search" dialog and type "cmd", then hit Enter.

- On **Windows 7** – click "Start" button then type "cmd" in the search dialog, press Enter.

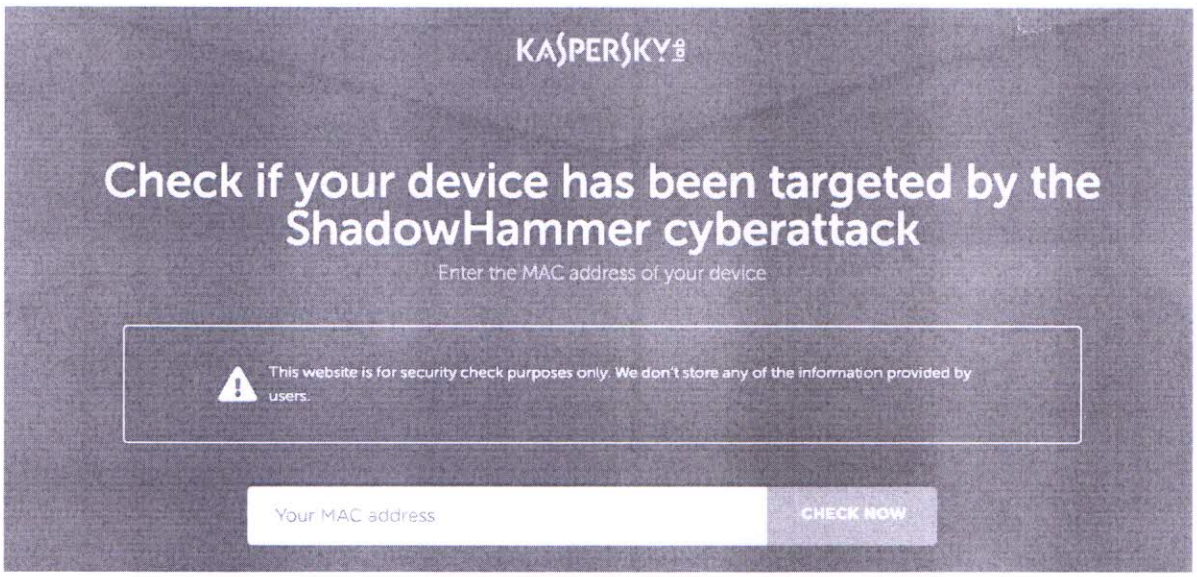
Once it opens, type "ipconfig /all". You'll see a lot of information on the screen:



Disregard those items which are marked with "Media disconnected" and search for lines with "Physical address:" – they will be showing **strings of six hexadecimal numbers**, like in the screenshot above.

These strings are your MAC addresses for each of your network adapters – both wireless and wired. You can copy one MAC address at a time to the clipboard from the command line prompt and paste into the box on our site.

3. Type your MAC address on the textbox and press '**Check Now**'



4. The tool will inform you whether your MAC address has been affected or not.

5. If you discover that you have been targeted by this operation, please take necessary actions urgently.

6. For an online demo of the above process, watch this video.

(OR)

Alternatively, Kaspersky has also provided a downloaded a tool which can be run to determine if your computer has been one of the surgically selected targets of this attack.

It can be downloaded through this link, or visit https://kas.pr/shadowhammer

Potential Implications

If the infected machine has a MAC address on the malware's target list, then the malware activates a "backdoor" through which other malware can be downloaded and installed.

Through this, it reaches out to a command-and-control server to grab more software, and thus, such a device can be used to carry out malicious activities of any scale.

References

1. https://securelist.com/operation-shadowhammer/89992/
2. https://shadowhammer.kaspersky.com/
3. https://www.tomsguide.com/us/chinese-hackers-asus-kaspersky,news-29722.html