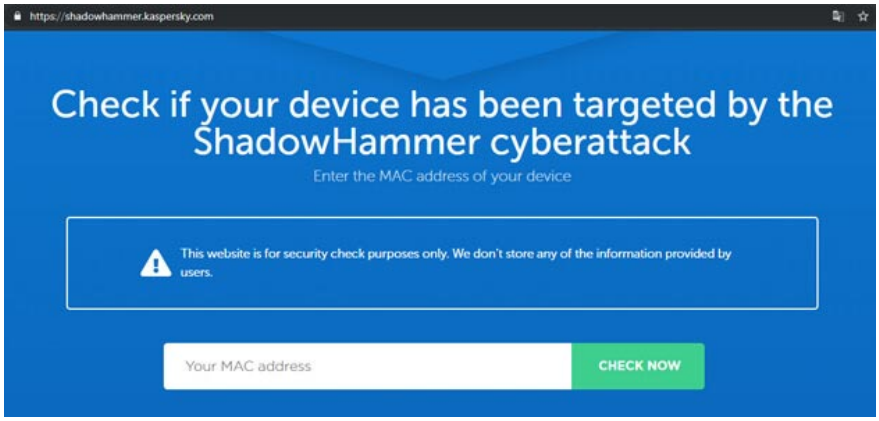
The list of nearly 600 MAC addresses was targeted in the recent hacking of millions of ASUS computer users

According to a recent announcement by researchers at Kaspersky Lab, tens of thousands of ASUS computers have been infected with malware by an attack that took place last January.

While revealing details about the widespread cyberattack targeting large supply chains for ASUS customers (ASUS Supply Chain Attack), Russian security company Kaspersky last week did not publish the full list of All MAC addresses that hackers have encrypted into their malware to target specific user groups.

Instead, Kaspersky has released a dedicated offline tool, and also launched an online website where users of ASUS computers can search the device's MAC address for testing. Check if you are on the affected list at the address:

`https://shadowhammer.kaspersky.com/`



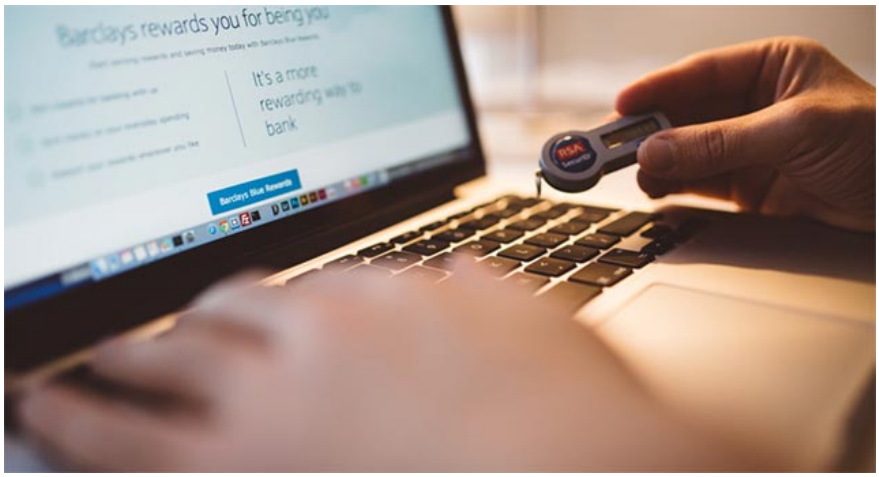
1. Hackers take control of the update tool, attacking tens of thousands of ASUS computers

However, many people believe that this is not really a convenient option for large enterprises with hundreds of thousands of devices in the system, if conducting manual search as with individual users, it is too lost. time. Hopefully Kaspersky will offer a method to find more effective MAC addresses for businesses in the future.

List of targeted MAC addresses in ASUS Supply Chain Attack

To help address the raid issues, and at the same time to help other cyber security experts continue to hunt for relevant hacking campaigns, Australian security company Skylight has decided to provide a full list Enough of

nearly 583 MAC addresses were targeted in the ASUS server attack to send malicious code, according to the statistics performed.



1. The alarming increase in the number of attacks targeted at IoT devices

'I think that if the information related to the hacked targets has been compiled, it should be provided publicly to the security community to help us better protect ourselves. So Skylight thinks that extracting the list of MAC addresses is targeted in the ASUS Supply Chain Attack, and publicizing it so everyone can conduct the necessary comparisons on their own ASUS device. Knowing in your domain will be a great idea at this time, 'said Shahar Zini, CTO of security company Skylight.

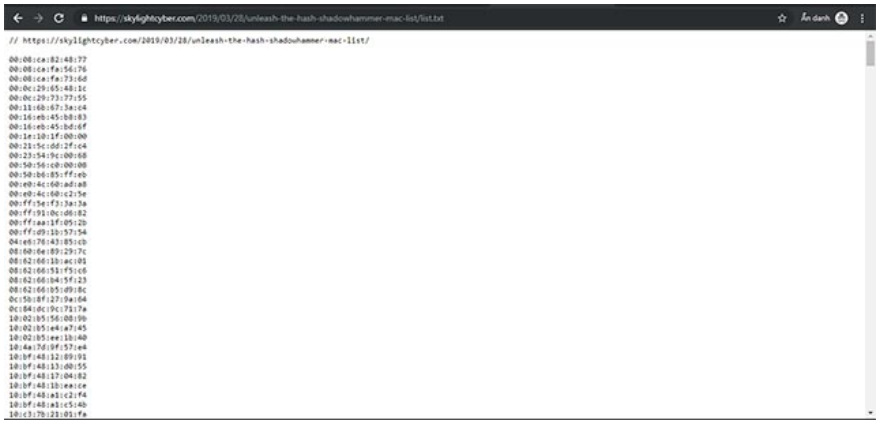
Accordingly, Skylight's security researchers successfully extracted the list of targeted MAC addresses with the help of the offline search engine released by Kaspersky, which contains the complete list of 619. The MAC address is in the executable file, but is protected by salted hash algorithm.

Specifically, Skylight experts used a powerful Amazon server combination and a modified version of the HashCat password cracking tool to successfully extract 583 MAC addresses in less than an hour.

'We took advantage of Amazon's AWS p3.16xlarge server. This 'monster' carries within itself 8 NVIDIA V100 Tesla 16GB GPUs. All 1300 prefixes have been brute force in less than an hour, "the Skylight team said.

You can access the target MAC address list extracted by Skylight at the following address:

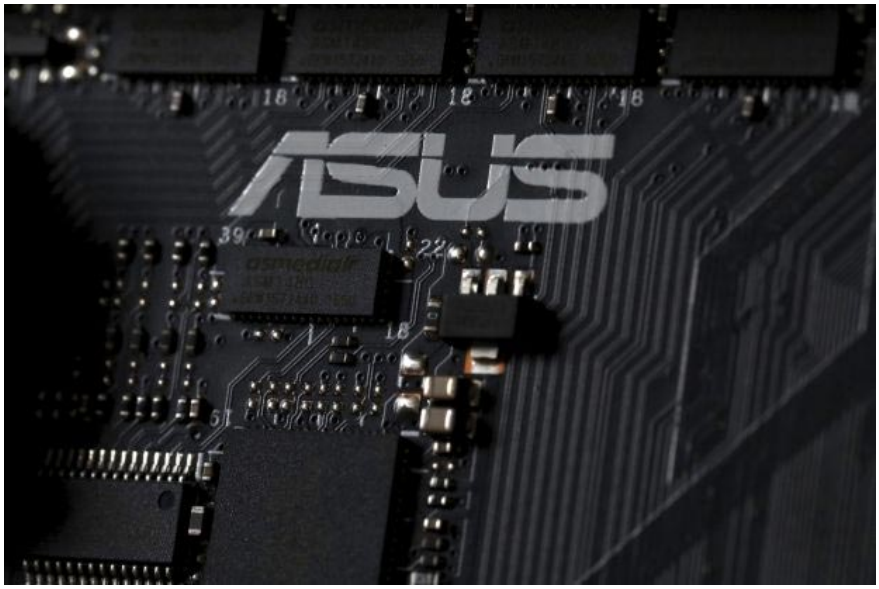
`https://skylightcyber.com/2019/03/28/unleash-the-hash-shadowhammer-mac-list/list.txt`



1. Endpoint Detection and Response threats, an emerging security technology

The hack on ASUS: Operation Shadow Hammer

Last week, a sponsored group of hackers tried to hijack the ASUS Live automatic update software server (launched last year) and pushed malicious updates to more than a million Windows computers. worldwide to infect them into backdoor systems. Kaspersky Lab calls this attack "Operation ShadowHammer" and it takes place from mid-June to November 2018, possibly affecting more than 1 million ASUS users worldwide, including more than 57,000 users. install Kaspersky computer saver.



The Russian security company later informed ASUS of this ongoing supply chain attack campaign on January 31, 2019.

After analyzing more than 200 malicious updates, Kaspersky researchers have identified attackers (not yet attributed to any APT group) that really want to target only a specific list of users. These are identified by their unique MAC addresses, and these addresses are hard-coded into malware.

Although in phase 2, malware is only pushed to nearly 600 targeted users, but that doesn't mean that millions of ASUS computers have received updates to be "immune" to the category. malicious code used in this attack campaign.

1. Fileless malware - Achilles heel of traditional antivirus software

How to check if your ASUS laptop has been hacked?

After admitting that his server was successfully hacked by an unidentified hackers between June and November 2018, ASUS released a completely clean new version earlier this week. of LIVE Update application (version 3.6.8) and also promises to add "multiple security verification mechanisms" to limit hackers' attack capabilities.

1. What is cybercrime? How to prevent cybercrime?

However, you should also know that installing only the updated version will not help remove malicious code from thoroughly infected systems. Therefore, to help their customers determine if they are a victim of this attack, ASUS has also released a diagnostic tool that you can use to check if the system Is my ASUS affected by a malicious update that hackers spread earlier. You can download this tool at the following address:

```
https://dlcdnets.asus.com/pub/ASUS/nb/Apps_for_Win10/ASUSDiagnosticTool/ASDT_v1.
```

If you find your computer's MAC address in the list, that means the device has been backed up by a malicious update and ASUS recommends that you restore the original settings to wipe the entire code. exclusive on the system.

You finished reading the article "**The list of nearly 600 MAC addresses was targeted in the recent hacking of millions of ASUS computer users**" edited by the **TipsMake** team. We hope this article has provided you with many useful tech tips and tricks. You can search for similar articles on tips and guides. Thank you for reading and for following us regularly.