Cyberwatch Finland

WEEKLY REVIEW
WEEK 7/2024

”CYBERSECURITY IS BUILT BY SMALL ACTIONS AND MANAGEMENT OF LARGE CONCEPTS”

Cyberwatch Finland

KEY TAKEAWAYS

1. An international will has emerged to establish the rules of the game for the use of commercial spyware

2. Unupdated or poorly protected devices can end up as part of a botnet. As a result, devices can end up as part of criminal activities such as denial-of-service attacks.

3. If a device ends up in the wrong hands, by default all data in it is lost despite protection software. For example, BitLocker used on Windows computers has been cracked in less than a minute.

Cyberwatch Finland

1. URGE FOR REGULATION OF COMMERCIAL SPYWARE

Last week, several countries and companies, including Microsoft, Google and Meta, as well as numerous organisations, signed a joint agreement led by France and Britain to address the threat posed by commercial spyware. The most well-known spyware includes Predator, developed by Cytrox, and Pegasus, developed by NSO Group. Both have been used, for example, to track opposition politicians, human rights activists and journalists in several countries. Their feature is that delivering malware doesn´t require an error from the target, but they can be installed discreetly on the device as a so-called zero-click. This has guaranteed access to all the functions of the phone, including files, camera and microphone. Spyware has been seen as a threat not only to the privacy of the people it targets, but also to human rights and democracy more broadly.

Instead of a total ban on spyware, the agreement now signed aims to tackle its unethical use and distribution. The agreement states that the uncontrolled distribution of spyware contributes to unintended escalation in cyberspace. At the same time, they pose risks to cyber stability, human rights, national security and digital security. Four key terms are used to change this situation: accountability, precision, oversight and transparency. This means, among other things, that operations should be carried out responsibly on the basis of existing international and national legislation, and that operations should be restricted and supervised. At the same time, business operations should be responsible, interactive and comply with good business practices for both service providers and users.

Although the agreement and its objectives are appropriate in themselves and lay the foundation for international rules in the cyber world, the discussion and thus regulation seem to be overdue, as in the cyber dimension in general. Spyware has been talked about for years, and the first version of Pegasus, for example, was released back in 2011. Over time, commercial spyware has become an ecosystem of its own, with several companies offering the service. Attempts have been made to restrict their operations before, and NSO Group, which developed the Pegasus spyware, has been placed on the US sanctions list.

Attempts to curb spyware developed by commercial operators and to demand morality in its use also seem hypocritical. It is abundantly clear that countries are developing their own capacities and are interested in these capabilities. In addition, the effectiveness of the agreement is undermined by the absence of Israel and Israeli companies from the table, because the country has been a forerunner in development and use of spyware. Cyber espionage can also be carried out through other means than those mentioned. For example, Chinese Huawei has been suspected of possible backdoors to its network infrastructure.

The process of creating rules for commercial spyware will continue in 2025, when the signatories will meet again to discuss the topic at a follow-up conference. Nevertheless, it is certain that the threat posed by commercial spyware will not diminish in the future. More players can be predicted to enter the market, because authoritarian states in particular will continue to be interested in these services. Neither will the cybercriminals follow these kind of agreements, and many state actors will use also their services.

2. BOTNETS ARE A TOOL FOR CYBERCRIMINALS

At the turn of January and February, the Federal Bureau of Investigation (FBI) announced that it had succeeded in disrupting the Chinese threat actor Volt Typhoon and the botnet it controls. This was made possible after the FBI gained access to the botnet's servers and managed to send orders to infected devices, mainly routers, to uninstall the malware and leave the botnet. Volt Typhoon is a Chinese state actor known especially for cyber espionage targeting critical U.S. infrastructure. Its trademark has been exploiting security vulnerabilities in routers, VPNs and, more generally, outdated and unupdated devices. According to a January report by security firm Security Scorecard, Volt Typhoon managed to infect up to 30% of certain types of Cisco routers in about a month after discovering a suitable vulnerability. Routers and other internet-connected devices being a part of a botnet is a common nuisance. What are these botnets and what kind of threat can having your own hardware as part of it cause?

Botnets are networks of hundreds of thousands or millions of devices that can be managed simultaneously. Virtually any device with processing capability and network connectivity can become part of a botnet, nowadays for example almost any smart device from household appliances to remote-controlled industrial equipment. Although the computing power of a single botnet device, and thus the benefit to the network operator, is often negligible, networks containing millions of devices are quite powerful and valuable tools for cybercriminals. Criminal gangs, or even individual hackers, may control their own networks of millions of devices, but they are also some of the best-selling or rented products on the black market. At present, botnets mostly contain various IoT (Internet of Things) devices, as it is often harder to notice that they end up as part of the network. The security of such devices is also often weaker, making it easier to assemble the network. On the other hand, the higher computing power of computers or smartphones makes them valuable parts of a botnet, and therefore ending up as part of botnets is not very rare. In recent years, the size of botnets has continuously increased and their use in various crimes has increased at the same rate. The most typical use of a botnet is to exploit it in a denial-of-service attack, but they are also used, for example, for mass entry of usernames and passwords (Credential Stuffing Attack), bulk sending spam or cryptocurrency mining.

A device can end up as part of a botnet in many different ways. The basic rule is that the worse the protection of the device is implemented, the easier it is to capture it on the network. In practice, hijacking is done by infecting the device with malware and connecting it to the server controlling the network. Belonging to a botnet may not be noticeable from the outside when viewing the device and may not cause any actual harm to the operation of the device itself. Often, malicious network traffic is disguised as part of the normal operation of the device. Thus, the threat posed by botnets does not target the devices themselves, but they serve as tools for other cyberattacks. However, in some cases, it is possible that devices that are part of the network may experience a decrease in computational capacity, overheat for no reasonable reason, or become impossible to install new updates.

The best way to protect your devices from ending up in a botnet is to have up-to-date updates. Along with these, the device's own security is also updated. A failed update process can tell about malware that has already been infected. Maintaining the update rhythm is important, especially for devices that do not necessarily do this automatically: this applies, for example, to many modems and smart devices or some parts of industrial automation. It is also possible for organizations to detect device hijacking by monitoring network traffic. Of course, maintaining protection is important for more than just preventing botnets from becoming part of them. On the other hand, if an organization's devices are so poorly protected that they may end up online, it is likely that they are also vulnerable to other kinds of influence. Thus, if devices end up as part of a botnet, other serious flaws in cybersecurity practices can be exposed.

3. BITLOCKER BYPASSED IN 43 SECONDS

Last week, a video uploaded to YouTube attracted attention in security circles, in which a video uploader demonstrates a way he found to bypass BitLocker protection on a laptop. The bypass took about 43 seconds and the target was a Lenovo computer that was a couple of years old but still widely used. BitLocker is a hard disk protection program developed by Microsoft and found in almost all Windows devices. In practice, it is intended to encrypt all data stored on the device's hard drive, and also prevent the data from being read if, for example, the disk to be protected is transferred to another computer. BitLocker's protection is generally considered good, and it is widely used on both business and consumer devices, although often the user may not even be aware of how the program works. The fact that it is possible to bypass protection with unlimited time and resources has already been known for a long time. What has attracted attention now is that the bypass was done so quickly and with tools that cost less than ten dollars in total.

In practice, bypassing was based on unencrypted communication between the machine's processor and the TPM chip found in almost every modern computer. A Trusted Platform Module (TPM) is often a physical component of a computer that stores most of the device's most sensitive information, such as passwords and BitLocker keys. In principle, the data passing between the processor and the TPM chip should not be readable at all, but the video showed that on most motherboards there is a point where an attacker can attach a microprocessor specifically designed for this purpose and use it to capture BitLocker keys. According to Microsoft itself, such a bypass would require not only a high level of expertise, but also long-term physical access to the device and soldering own components to the motherboard. In the attack method demonstrated in the video, instructions and resources can be found on the Internet, the bypass takes less than a minute, and instead of soldering, simply unscrewing the back cover of the computer and inserting the USB stick-sized microcomputer into the correct position is enough.

However, it is a bit confusing to describe that the entire attack took place in said 43 seconds, as this was probably preceded by much longer preparatory work in which the bypass was planned. In addition manufacturing and obtaining the necessary microcomputer also took time. Only when both understanding and tools were available could the attack be carried out within that time. However, according to the perpetrator of the attack, a similar attack is possible on the majority of modern laptops, either using the same tool or modifying it to suit the targeted device. If the attacker knows what kind of computer the target is using and can prepare themselves in advance, it is indeed possible that using the same method it is possible to bypass the protection of the hard disk and access the data stored on the device in at least minutes.

While in itself hacking into a physically hijacked device is nothing new, it's still good to understand that this can happen within minutes of the device falling into the wrong hands. There are also very few possibilities to prevent a device from being hacked once it has fallen into the hands of an attacker. Although the bypass method shown in the video does not work for all laptop models, and it is possible to further improve the security of both the TPM chip and BitLocker with configurations and additional levels of encryption, weaknesses have been found in virtually all of these solutions that allow bypassing protection. No security solution is unbreakable, and especially with unlimited physical access, any encryption program can be cracked or bypassed. Therefore, organizations need to consider when it makes sense to store in the physical storage spaces of computers. Especially for machines that travel with employees, storing data in a cloud environment, for example, from which a lost device can be quickly isolated, may be a better solution. This isolation must be done quickly, and the personnel must have clear instructions on who to contact if they notice that their device has been lost. On the other hand, if the machines never leave the organization's premises and access to them is effectively controlled, storing data physically on these devices is not necessarily a bad option. As with cyber security in general, there is no single clear solution for storing data securely, and organizations must conduct their own assessment of how and where data is best secure. Also, not all data is equally valuable, so classifying, storing and limiting data processing goes a long way. These are also things that need to be noticed in the cyber riskanalysis and mirror into one´s own business.

REFERENCES

1. Urge for regulation of commercial spyware

https://thehackernews.com/2024/02/global-coalition-and-tech-giants-unite.html

https://www.diplomatie.gouv.fr/en/french-foreign-policy/digital-diplomacy/news/article/the-pall-mall-process-tackling-the-proliferation-and-irresponsible-use-of

https://www.reuters.com/technology/cybersecurity/britain-france-lead-35-nation-agreement-controlling-spyware-mercenary-hackers-2024-02-06/

https://www.reuters.com/world/us/us-announces-visa-restriction-policy-those-misusing-commercial-spyware-2024-02-05/

2. Botnets are a tool for cybercriminals

https://www.paloaltonetworks.com/cyberpedia/what-is-botnet

https://www.einfochips.com/blog/botnet-attacks-how-iot-devices-become-part-victim-of-such-attacks/

https://www.bleepingcomputer.com/news/security/fbi-disrupts-chinese-botnet-by-wiping-malware-from-infected-routers/

https://securityscorecard.com/blog/threat-intelligence-research-volt-typhoon/

3. Bitlocker bypassed in 43 seconds

https://www.tomshardware.com/pc-components/cpus/youtuber-breaks-bitlocker-encryption-in-less-than-43-seconds-with-sub-dollar10-raspberry-pi-pico

https://learn.microsoft.com/en-us/windows/security/operating-system-security/data-protection/bitlocker/countermeasures

https://www.youtube.com/watch?v=wTl4vEednkQ

Pictures: Pixabay

Cyberwatch Finland