**Investigation about security issues associated with Smart Cities**

In a smart city, any network-related equipment may become the target of attacks, such as smartphones, computers, bank ATMs, doors with fingerprint locks, cameras, and even cars and aeroplanes. Most attackers use profit as their purpose of the attack. Nowadays, the importance of computers is undoubtedly very important. From being a company's user data management tool to a personal learning tool, it has an indelible position. According to a survey about operating systems market share of desktop PCs 2013-2020, by month, windows OS worldwide survey of July Recording 2020 with a share of 77.74 per cent. It has remained the first. Most companies choose Microsoft windows system because the Microsoft company brings together the world's top computer technology experts and sufficient maintenance of the system, which can provide users with technical support so that their personal information can be secured on the Internet. Because of this, the windows system has always been the most used system in the world. This further illustrates how much people pay attention to their personal privacy. In the 21st century, a world connected by the Internet, people most urgently need privacy. The emergence of smart cities and the flourishing development of the Internet have led to the birth of an illegal industry, that is, cybercrime. There are many types of cyber threats, such as Phishing, Trojans and Botnets (Secureworks, 2020). This article will mainly explain Botnets. Botnets are hackers who use some hacking methods to achieve the purpose of invading and controlling the victim’s network. During the invasion, the hackers can do whatever they want. Control all computers covered by the victim's network. In order to execute large-scale crimes, the most common threat is to blackmail the victim with sensitive personal privacy such as ID cards, private photos, secret company documents, etc. Control all computers covered by the victim's network. In order to execute large-scale crimes, the most common threat is to blackmail the victim with sensitive personal privacy such as ID cards, private photos, secret company documents, etc. botnet attack will pose a serious threat to the confidentiality and integrity of the victim's data.

According to an article by the BBC, in 2019, a ransomware called Sextortion botnet was distributed. (Lee, 2019) Hackers usually escape the scan of spam mailboxes through distinctive mailbox headers and induce them to click to download. One of the ways to induce it is to claim to have a nude photo of the victim or his friend as a threat. Usually the first time the victim will not immediately hand in the blackmail request from the attacker, but after receiving the processed photo, the curious victim will click on the picture. When the picture is clicked, the ransomware code will spread into the computer, and the victim will be ransomed on the grounds of unlocking the computer's permission. The virus is difficult to track the spreader of the virus, because the ransom money submitted by the victim is a decentralized virtual currency, and the transaction process is the person to person instead of a third-party transaction. It cannot be investigated through the bank's transaction records. In addition, the article Point out "They can carry out attacks spread across a wide number of machines, making it harder to disrupt and the attacker's origins harder to trace." After that, Clare, one of the victims, spoke out the threatened process and told us how much damage the victim's psychology is caused by blackmailing with nude photos in the video (BBC, 2020). Although smart cities have brought convenience to people, they also provide criminals with a hotbed for crime, allowing the hidden network to be used as a tool for crime.

For the countermeasures against the threat, First, avoid clicking link that is doubtful. Sextortion botnet is the same as most virus intrusions. The victim must download or click on the malicious software or link prepared by the hacker to be poisoned. Therefore, suspicious software, email attachments or hyperlinks should not be clicked. Hackers will use it. The victim takes advantage of the psychology and uses "free", "low price" and so on to commit fraud. Second, install an authoritative firewall. As an article from Indiana University: "A firewall is a system designed to prevent unauthorized access to or from a private network. You can implement a firewall in either hardware or software form, or a combination of both." (Indiana University, 2020) Firewall can block malicious traffic such as viruses in your computer network. The firewall is like a door that keeps the hacker out. If he wants to come in, he must spend a lot of time unlocking it. After that, install the latest security patches, as we all know, there is no absolutely a secure system. Unknown vulnerabilities will be discovered constantly. Only by constantly updating the latest security patches can the computer be maintained in the most secure state. Last but not least, to develop a habit of regularly backing up data to external devices. Important data is invaluable for both individuals and businesses. It carries precious time, such as the accumulation of countless customers and the memories of photos. Such important data deserves to be backed up regularly. If the company is very large and the backup takes a long time, then reduce the frequency of backup. When all the computers of the company are unfortunately infected with ransomware, it is for every computer It is impractical to pay expensive fees. At this time, the value of regular backups is revealed. You only need to reinstall the system and restore the data to solve the problem. Compared to the company’s loss, it’s good to spend some time backing up data.

To sum up, although the smart city makes our lives fast and convenient, it is also a place where hackers show their talents. Windows is the most popular platform for computers, and there are many active hackers who use the security leak of the Internet to make illegal profits. The most thread of cybersecurity requires the victim to personally click on the software, hyperlink or attachment provided by the hacker so that the malicious code can be authorized and executed. The things that can usually be prevented is not to be greedy for cheapness, to be suspicious of documents from unknown sources, to install firewalls and update security patches. It is best to back up important data regularly. Hackers’ scams are all similar, as long as the above principles are done well, it will be very difficult for them to invade, so that computers can maintain a clean network environment in the smart city.

1237 words

**References**

Rouse, M., 2020. *What Is A Smart City? Definition From Whatis.Com.*. [online] IoT Agenda. Available at: <https://internetofthingsagenda.techtarget.com/definition/smart-city> [Accessed 1 December 2020]. (Rouse, 2020)

Lee, D., 2019. *'Sextortion Botnet Spreads 30,000 Emails An Hour’*. [online] BBC News. Available at: <https://www.bbc.com/news/technology-50065713> [Accessed 1 December 2020].

Liu, S., 2020. *Desktop OS Market Share 2020 | Statista*. [online] Statista. Available at: <https://www.statista.com/statistics/218089/global-market-share-of-windows-7/> [Accessed 1 December 2020].

BBC, B., 2020. *Sextortion Hackers Use 'Friend's Naked Girlfriend' Lure*. [online] BBC News. Available at: <https://www.bbc.com/news/technology-51817468> [Accessed 1 December 2020].

Kb.iu.edu. 2020. *About Firewalls*. [online] Available at: <https://kb.iu.edu/d/aoru#:~:text=A%20firewall%20is%20a%20system,to%20the%20internet%2C%20especially%20intranets.> [Accessed 1 December 2020].

Moore, M., 2020. *Top Cybersecurity Threats In 2020*. [online] University of San Diego. Available at: <https://onlinedegrees.sandiego.edu/top-cyber-security-threats/> [Accessed 1 December 2020].

Secureworks.com. 2020. *Cyber Threat Basics, Types Of Threats, Intelligence & Best Practices*. [online] Available at: <https://www.secureworks.com/blog/cyber-threat-basics> [Accessed 1 December 2020].