What is data exfiltration? How to prevent this dangerous behavior?

Data exfiltration also has other ways of calling data theft (data theft), or data exportation (unauthorized data export).

Data security is always one of the core aspects of network security. It goes hand in hand with the general development of the security world as well as the transformation of the network security situation worldwide. Talking about data security, there is an inclusion of many different concepts and certainly cannot be explained in a few pages. In this article, we will explore a small concept in data security, which is data exfiltration, as well as how to prevent and respond to this dangerous security incident.

1. Overview of building enterprise security detection and response system

Learn about data exfiltration

1. Concept of data exfiltration
2. How is data exfiltration done?
3. How to prevent and respond to data exfiltration
4. Endpoint Protection (Endpoint Protection)

Concept of data exfiltration

Basically, data exfiltration also has another method called data theft, or data exportation, so in this case, we can understand data exfiltration as behavior. data theft.

Data exfiltration is data theft

This data theft can be done manually by any individual who has physical access to a computer system or hardware device that stores data, or can be done With the help of the program, malware spreads through network environments, most commonly the internet.

In other words, data exfiltration is a form of serious security breach, in which data can be transmitted or copied without consent from the owner - basically, data has been stolen. literally. In theory, this behavior can be done through a variety of techniques from simple to complex, but in general, it is often done by hackers (cyber criminals) through the internet environment. . Data exfiltration attacks are often planned and targeted specifically, thereby helping hackers locate and steal the data they want with a higher probability of success.

Data exfiltration can be especially difficult to detect in many situations, such as moving data within a company's intranet system, as well as outside this network. And once those data are in the hands of hackers, security disasters are entirely possible, and at the same time, the collapse of a large enterprise system.

1. The 5 most notable cyber security conferences in the world take place throughout the year

How is data exfiltration done?

One of the most common methods used by hackers to deploy data exfiltration campaigns is to target a simple password that is easily 'broken'. According to statistics, the sophistication and complexity of how to use the password of the data storage system will be inversely proportional to the probability of becoming the target of data exfiltration campaigns.

Data exfiltration caused when individuals have access to an intranet system and steal data
After breaking the password "shield", hackers can access the target systems through remote access applications designed or purchased by third parties, or by inserting a mobile multimedia device in case of additional physical access.

There is another form of data exfiltration called Advanced Persistent Threat (APT). This type of attack is often used in situations where specific targets are identified and data theft is highly sensitive information. The main purpose of APT is to try to gain access to the organization's target network system, while minimizing detection while searching for targeted data, such as customer information, intellectual property, or financial information . These are all extremely sensitive data types of any business.

This form of data theft depends heavily on social techniques such as email scams (phishing emails) to try and trick active agents in the target organization, thereby installing a chapter. malicious software into their computers and take that as a 'pedal' to access the organization's general network. After successful penetration, hackers will try to determine the type of data they are targeting and the final step will be to copy or transfer that data outside.

Attackers will now be able to use the data they have stolen for illegal purposes, undermining or damaging the reputation of organizations and businesses.

1. Game industry - an attractive target for cyber criminals

How to prevent and respond to data exfiltration

It's not too much to say that this is a million-dollar question in the field of data security in general. The answer is of course very wide and it depends on the specific situation, but it can be summarized 2 main ideas as follows.

Basically, most data exfiltration campaigns are deployed mainly based on social techniques to install malicious software on personal computers operating in the system (related to human factors). . Therefore, the most effective and urgent precautionary measure for organizations and businesses is nothing more than strengthening their staff training in detecting potential threats through email, as well as encouraging employees to equip them with the latest knowledge in the security field, thereby enabling them to accurately identify fraudulent acts and promptly report problems before a serious incident occurs.

In parallel with human factors, organizations and businesses also need to establish remote security barriers, designed to actively detect potential threats and potential programs, thereby Help the system security team to make timely and accurate response to each specific situation, minimize the problem of leakage and data loss.

1. Find out about Ghidra - NSA's powerful cybersecurity tool

Endpoint Protection (Endpoint Protection)

One of the most important factors in data exfiltration prevention is the absolute security of endpoint devices. Endpoint devices are the source of easy access for hackers. In other words, they are a bridge to make it easier for crooks to enter the system, so it is important to secure these devices.

1. The cybersecurity tools that every business should know

Ensuring safety for end-point devices is important in data exfiltration prevention

If you want to delve deeper into the endpoint security processes, you can consult some of the following articles:

1. Learn about terminal security (endpoint security)
2. Top 5 trends in endpoint security for 2018
3. Endpoint Detection and Response threats, an emerging security technology
4. Insider attacks are becoming more and more popular and difficult to detect

In short, preventing and responding to data exfiltration is not too complicated. However, the difficulty lies in phishing techniques and technologies that are constantly evolving, changing day by day, facilitating the emergence of more sophisticated offensive campaigns, causing more damage. Therefore, organizations, businesses, and especially individuals in the system must always be proactive in all situations, actively update changes in the security world to promptly make changes Combined, along with that is promoting the implementation of strong security policies to prevent data from being stolen from the organization

You finished reading the article "**What is data exfiltration? How to prevent this dangerous behavior?**" 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.