Deep Learning - new cybersecurity tool?

Artificial intelligence (AI) is increasingly contributing to every area of ??human life. Among the sub-domains of artificial intelligence in general and machine learning in particular, it can be said that deep learning is a truly outstanding technological breakthrough.

Artificial intelligence (AI) is increasingly contributing to every area of ??human life. Among the sub-domains of artificial intelligence in general and machine learning in particular, it can be affirmed that deep learning is a truly outstanding technological breakthrough. It is possible to gain immeasurable benefits when successfully applied in many different areas. The development of deep learning technology has also opened a new direction in the field of network security as well as information security. As many of us know, the advantages of artificial intelligence are fully capable of applying effectively to enhance the power of anti-virus technology, malicious code . contributing to the tools signature-based malware and heuristic algorithms are gradually becoming obsolete. One of the main reasons lies in the reality of today's cyber security situation, when cyber attacks are constantly becoming more sophisticated, simply by the cyber criminals in nature. is the 'master' in the field of security, and these subjects, of course, also know how to practice research and develop new, more effective forms of attack on their own.

1. Young people are too confident when talking about online security!

For example, the majority of current network attacks use even more malware at a rate of up to 90% or more and even security experts say that some attacks are critical. vi is being launched with malware at about every 5 seconds. In the case of such an attack method that allows cybercrime to enter the system, the consequences that they leave will be huge even if it only happens in very short time. For this situation, once again the phrase "prevention is better than cure" is more correct than ever. However, with the traditional security methods currently being applied universally, namely conventional malware detection technology (listing and discovering data on the characteristics of malware based On special characters called signature, it will be greatly limited. In addition, there is a "deadly" weakness of this security method, in case the new malware appears, it will not work unless provided with the corresponding signature.

In other words, non-signature malware cannot be detected and they will be able to 'hide' permanently until the new signature is created and the malware features are captured. can. But whether this security method can grow quickly and catch up with the constant evolution of customized malware for each individual goal, while the attacker is always the one holding the initiative. ? I'm afraid it will be very difficult.

1. More than 4,000 Office 365 accounts are affected by account hijacking attacks

In addition, this fact has shown that there is always a large amount of malware that cybercriminals have created to try to overcome the protection barrier from antivirus software. It is an attempt to 'hide' from the ability to detect signature-based malware by changing the content of the malware a bit and at the same time creating a large amount of malware Different origins to avoid detection.

From the above reasons, it can be clearly seen that the ability to detect malware based on conventional antivirus functions contains quite a few limitations. Therefore, the application of new technology to develop more effective measures is essential, especially in the context that the world is facing the ability to access, share huge information, and all come with existing risks. Some of the typical reasons are as follows:

Information leakage due to internal fraud

1. DNA information leaks are worse than leaking many credit card information

It is a fact that no matter how many measures and security tools your business owns, the 'disasters' stem from human factors (internal The system) is still very difficult to prevent and can have more serious consequences than any external attack. Today, perhaps we are no stranger to the following cases: 'Employees handle unauthorized use of customers' personal information for personal purposes, or misuse of data. Credit card and customer security code within the system itself . '. In particular, if it is the behavior originating from employees in a company that is still famous for safety and reliability, it can be said that customers will have absolutely no way to prevent and at the same time Such cases also greatly affect community trust.

Attack targeting smartphones and apps for smartphones

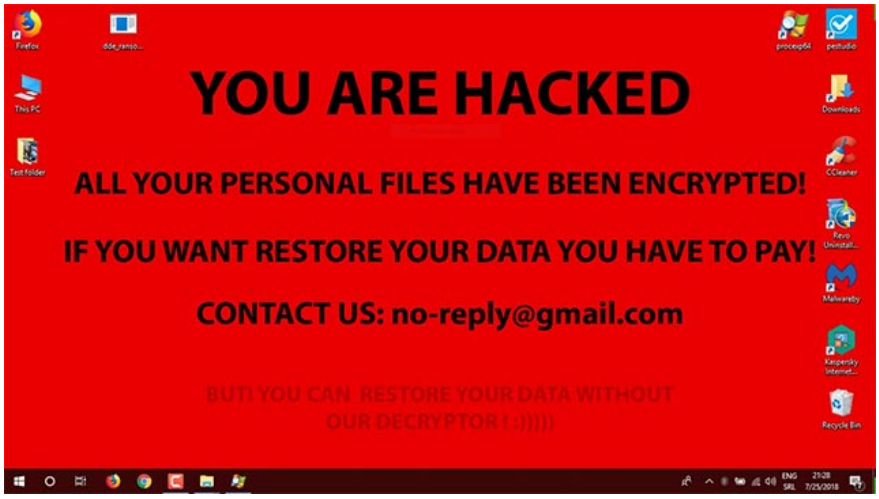
1. [Infographic] How to recognize and prevent Phishing attacks

More and more cyberattacks are targeted at smartphones and smartphone applications, in parallel with the development of this type of device. There is also the emergence of separate viruses for smartphones as well as malicious codes hiding the ball in the form of a free mobile application to steal personal information of users. In particular, if the smartphone is used exclusively for business purposes to be attacked, the damage caused to the business may be huge.

Unauthorized use of credit card and internet banking information

One of the most common types of personal damage on cyberspace today is violations of credit card information and online banking. Typically, bank account information is often leaked through infected PC and smartphone applications. Based on stolen information, crooks can easily access internet banking accounts as well as victims' credit card data.

Damage due to ransom attacks (ransomware)



1. [Infographic] 7 effective ways to protect businesses from Ransomware

Among the types of cyber crime, ransomware damage, kind of ransom data encryption for recovering information and systems, is a sore topic for cyber security on worldwide in recent years. Ransomware becomes even more frightening for businesses. When a company's important data is encrypted and falls into the hands of an attacker, the damage will be huge, possibly even bankruptcy.

Damage due to targeted attacks

1. India's largest IT services company is hit by a hacker '

Targeted attack refers to launching a cyberattack targeting a specific company. A typical targeted attack will often operate under the 'script' of sending emails attached to viruses, malware to employees and certain parts of the targeted company. Malicious emails of this type are dangerous in that it is difficult to distinguish between them and other normal emails. When exposed to the above emails, the employee's computer or further is the network of the entire business will be infected with malicious code.

With the above reasons, along with some of the disadvantages of the usual signature-based security method, deep learning - with the advantages of artificial intelligence that it owns - will play a role. The most important in the task of creating security walls is tighter, easier to operate, more proactive, and important is more effective!