Learn about the Whaling network attack technique

You may have heard about the Phishing network attack technique, but do you know about its more advanced 'brother'? That's the Whaling technique.

You may have heard about the Phishing network attack technique, but do you know about its more advanced 'brother'? That's the Whaling technique. Let's learn about this network attack technique

1. Summary of popular network attacks today
2. Analyze hacker attacks on Microsoft-UK website
3. Some basic website security rules

What is the network attack technique Whaling?

The difference between Whaling and Phishing

Whaling itself is not an advanced technique. At a basic level, it is a more complex scam. Whaling learns from Phishing's flaws and changes to trick people into doing what hackers want. The main problem with Phishing is that they are often inefficient. Everyone was more aware of the detection of a Phishing attack, so it was no longer as effective as before.

Therefore, hackers must make more efforts to trick others. People often recommend not believing in things sent from friends, family and colleagues, so hackers have used this trust to create Whaling technology.

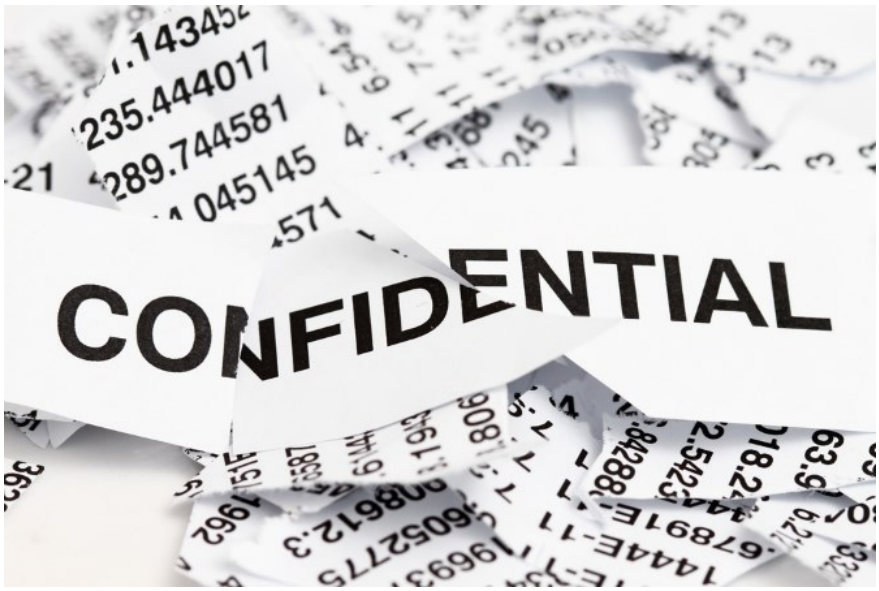
Whaling is a technique that attacks hackers to use to target someone in a high position in the company. Usually, they will collect information about that person to learn more about them. Hackers also try to access the corporate network and do some investigations on how the company works.

How is the information collected used?

When hackers have all the information they need about the senior manager of the company, they will infiltrate their account and use email services, send messages to subordinates to deceive them.

If hackers cannot access the company's network or account, they will impersonate them by creating an email address similar to those who want to impersonate, then email their employees. While this method is susceptible to blocking spam filters or if the whitelist does not reach anyone who wants to scam, sometimes there is a chance of success.

How do hackers benefit from Whaling?



Of course, hackers do not do these things in vain without getting anything. Their main goal is to get money from these employees by asking them to transfer money to management.

Hackers also impersonate the manager's voice and tone to make the attack more reliable. They will require employees to transfer money to their accounts for business reasons. In addition, hackers require sensitive data to earn more money.

Damage from the Whaling attack

We now know how Whaling used to cheat people, but how many companies fall into their trap? Can these companies quickly discover attacks or hackers who have earned a decent amount before being exposed?

Forbes reports that, since 2013, an estimated $ 12 billion has disappeared from 80,000 businesses due to the Whaling attack. Not only that, Varonis also statistics on the Whaling attack that has increased by 200% only in 2017, showing how hackers are heating up a big scam idea.

How to protect against Whaling attacks

Privacy policy of the company

Good corporate security policies are an effective way to stop hackers. As a company employee, you should secure user accounts to prevent hacking. You should set strong passwords, implement additional countermeasures against intruders (such as two-factor authentication).

1. Summary of how to create strong passwords and manage the most secure passwords

Companies should also set up internal email systems so that when receiving mail from outside addresses will be more alert. Even impersonal emails will be blocked if blacklisted.

Data protection and money transfer

Ideally, you should ensure the safety of sending data and transferring money to prevent leaks outside the company. Always handle data and money in the safest way possible. That way, when someone is tricked, the transaction will be flagged by the system before the hacker can handle it for money.

Raise vigilance

When these measures fail, hackers aim at you, you can only trust yourself and be more alert. A hacker uses attack techniques aimed at your motivation by impersonating your superior to contact you. That way, when they ask you for sensitive information or ask you to transfer money, you'll send them without thinking.

If the manager suddenly asks you for cash or personal information, you should check the name and email address carefully. If something is not right, try contacting the boss to see if this is a legal transaction.

Use secure email service

The Whaling attack can only take place if there is enough information to carry out the attack. If you prevent this information from leaking, they will have no tools to infiltrate the company. Therefore you should set up your email security carefully.

You can choose some secure and encrypted email services, prioritizing your privacy first. If an email service provider doesn't care if your connections are at risk of leaking sensitive data, don't use that service, because hackers can use it to do a Whaling attack. . You can refer to some of the services in lesson 8 of the best secure email service to ensure your privacy.