Speãr-Phišhiñg

What is a spear-phishing attack?

Attackers want to breach your defenses and gain access to your network.

Spear-phishing attacks circumvent strong organizational defenses and gain network access by targeting the weakest link in a security policy: the people.

Before beginning, attackers collect sensitive intelligence on an organization, its people, and operations. This information is then used to trick the company's employees into naively performing a malicious act.

Spear-phishing attempts can take whatever form the attackers desire (emails, websites, phone calls…) to allow them to successfully penetrate the organization's security measures.

"84% of organizations said a spear - phishing attack successfully penetrated their organization in 2015"

* source: Symantec Intelligence Report 2016

What is the risk?

Once attackers have a foothold in the network, they can move laterally, escalating the attack to a full APT.

How does the attack operate?

1. Target identification - based on the attack's objective (financial gain, trade secrets, confidential information …) select a target organization

2. Intelligence gathering - learn everything possible about the organization and its employees

3. Cover story - construct a reliable story to appear authentic

4. Engagement - using the cover story, engage people in the organization until one of them is fooled

5. Lateral movement - with a foothold in the organization, access the network

What are the challenges to detection?

Attackers invest heavily in a cover story that prevents suspicion. Documents, and websites look legitimate and malicious actions are sophisticatedly concealed.

Traditional email and web-filtering solutions are unfortunately not built to detect spear-phishing attacks, and awareness-training is costly.

What would minimize the risk?

A breach is inevitable. Persistent attackers targeting your organization will eventually get in. However, breaches cannot become APTs if attackers cannot perform lateral movements.

With illusive installed, the attacker discovers an alternate reality, made of smoke and mirrors, that makes it impossible to discover real employee information or perform lateral movements without getting caught.