



Hacker Speak

A Guide to Understanding the Acronyms, Slang & Jargon Used in Describing Computer Security Breaches, and How to Protect Against those Risks

By Marv Chen and Kevin Tsuei, AuditOne LLC

In light of recent computer security breaches, you may have heard some colorful terms used to describe hacker attacks such as spear phishing, Trojan, zombies, DDOS, poisoning, and spoofing. We will approach an understanding of these terms by contextualizing them in plausible scenarios. In addition, we'll provide some ways to protect against the related risks, though it is extremely difficult to defend against these types of social engineering attacks (the failure rate is surprising high on the social engineering simulation tests that AuditOne has conducted in the past several years).

In the past several years, we have seen spear phishing become a common occurrence the banking industry. In this scenario, an attacker sends a counterfeit e-mail to employees of a specifically targeted bank; this e-mail is disguised to appear as if it came from a trusted source, such as a technology service provider, a member of senior management, or a board director (an attacker can find important relationships between the employees of the Bank and other entities with a little detective work by searching social media sites [LinkedIn, Facebook], Google, or even a bank's own informational website).

This email would contain a Trojan, or a link to download one. The Trojan is designed to imitate a legitimate PDF document, application update, news release document, etc. but is actually a disguised malicious computer program. Because the Trojan has now been allowed through the firewall into the corporate network, it's pretty much "game over" once an employee opens the package (it should be obvious now why these programs are called Trojans – after the Trojan Horse of Greek mythology). These Trojans can be sophisticated programs that record users' keystrokes, eavesdrop on data network traffic, leak confidential information, crash computing systems, or stay hidden as zombie programs.

Zombies are used by hackers to launch DDOS attacks. DDOS stands for Distributed Denial of Service. An attacker wanting to bring down a website will issue commands to hundreds, even thousands, of zombie-infected computers. These zombies will then send a large amount of informational requests to the targeted website. The enormous amount of data from the combined effort of these zombies overwhelms the processing capabilities of the targeted website's servers and routers. This effectively "denies service" to the website because it is now only able to respond very slowly, or not at all, to requests from real users.

Poisoning is a more difficult concept to understand. This term is most often heard in the context of DNS poisoning. All websites have what is called an IP address. What DNS does is convert the domain name that you type into your browser (for example: www.yourbankswebsite.com) to the IP address of the desired server. Therefore, without DNS, you cannot surf the web (at least not without entering a direct IP address).

DNS poisoning is an attack that exploits flaws in DNS software. An attacker spoofs (forges or masquerades) the IP address of a domain name entry on a DNS server. This method is used to redirect users of a website to a counterfeit website of the attacker's choosing. The counterfeit website can be used to collect users' logins and passwords; these websites can even be sophisticated enough to transparently redirect the user back

to the legitimate website so as not rouse any suspicion on the user's part.

So how do we protect ourselves against the types of attacks described above? The truth is that it's not easy. All of the scenarios described above involve a user being an active participant, albeit unwilling a one.

The best answer is training and education: making sure that new employees are trained as soon as possible upon hire, that current employees receive ongoing training, and that customers receive appropriate training, notices, and warnings. Users should be taught how to distinguish legitimate e-mails and websites from phishing attempts, as well as to seriously heed the warnings issued by operating system and e-mail applications when they attempt to run unknown programs. Customers should be instructed on the importance of the browser's "lock" icon, indicating a secure connection to an authenticated website, when using transactional internal banking websites.

In closing, while technological tools such as firewalls, intrusion detection systems, and anti-virus software contribute to a stronger computer security stance, when it comes to combating social engineering attempts, it is still people who matter the most.

[<back to June 2011 Technology & Security Digest>](#)

Marv Chen is Technology Practice Director for AuditOne (www.audit-one.com). He can be reached at Marv.Chen@audit-one.com. Kevin Tsuei is an IT Auditor at AuditOne. He can be reached at Kevin.Tsuei@audit-one.com.