Hackers and Crackers

What you should know

Who are hackers?

A common opinion is that hackers are malicious individuals who launch attacks against computers, break networks and write viruses. However, the original definition of a "hackers" is someone who tweaks, disassembles and builds software for fun and to improve knowledge. In the IT community, the correct name for malicious computer attackers is "crackers", while a "hacker" is a more general term that can also include harmless programming and networking enthusiasts. When it comes to computer security and threats, more accurate hacker definitions are Black, Grey and White Hat:

- Black Hat is someone bent on attacking others systems. S/he would do it without any ethical or legal considerations.
- White Hat or "ethical hacker" is an IT security enthusiast who does not attacks systems illicitly. A White Hat would find flaws in software and networking protocols and report them to the public. A typical White Hat is an IT security professional or will eventually end up as one.
- Grey Hat is someone with IT security interest and knowledge who follows situational ethic and may break the law if pushed.

The major danger for your network comes from Black Hats, while the White Hats are actually allies. Another common term you can encounter on the Internet is "script kiddie". Script kiddies are the lowest form of Black Hats who attack systems using tools they download from hacker websites without understanding the inner workings of these tools and mechanisms behind the attacks launched. Script kiddies are the most numerous group of attackers on the Internet and they tend to overwhelm networks by sheer mass and effort spent rather than skill and knowledge. Often, but not always, script kiddies are teenagers or undergraduates.

Why do hack attacks happen?

There is a great variety of reasons why crackers attack. They include:

- Ego satisfaction, financial gain and theft, vandalism, curiosity and new attack tools testing, boredom, playing pranks on unsuspecting users, gaining "fame" in the underground and media, personal grudges and revenge, political, religious, environmental etc.
- Fraud, giving bad reputation to a company / bringing down competition, industrial espionage, exposing private data of individuals and on-line stalking, gaining machines to spread porn and pirated movies, music or software,
- Turf wars between script kiddie groups, gaining machines to use them as host for anonymous attacks on other, often or important famous sites (BBC, CNN, e-bay, banks, military, government)

Why should you be concerned?

It is a common misconception to think that you won't get attacked because your company is low profile, you do not keep any confidential information and do not perform on-line transactions. As you can see, industrial espionage, theft and corporate defamation are only a few reasons on the long list of real world cracker motivations. Your systems can get attacked simply because they happened to be in his/her close proximity, or simply to hide tracks behind your network credentials and hack into others system from your address. Often, the first sign of such attack is police knocking at your door and accusing you in serious hacking.

Many Black Hats use automated tools capable of scanning vast ranges of network addresses in search for vulnerable systems. Such tools with an in-built automatic "attack-and-break-in" feature save crackers a lot of time, but they do not distinguish between a sole trader or home user and the vast Pentagon's network.

What to do if you suspect that you were hacked?

- If your company has IT personnel, inform your system administrator or IT technician about the incident or your suspicion.
- If the suspicion appears to be well-founded, disconnect your network from the Internet.
- Do not reboot or shut down the affected machine/s. In fact, do not touch them at all to avoid destroying the evidence.
- Contact the authorities.

Larger companies must have a security policy that defines an Incident Response Team which handles hacking incident cases and communicates with the authorities. Such team has to include someone from the top company management as well as technical IT personnel. If network security / maintenance is outsourced, a technical representative of the service company should be included in the team as well.

How to avoid being hacked?

Recognise the risk and understand which systems are likely to be attacked, for example, these could be the systems that hold credit card data and customer databases.

Decide what level of risk your company systems can be exposed to, how much you plan to spend and take appropriate actions.

Make sure that your network is separated from the Internet by a decent dedicated firewall. Never use the default vendor configuration! Update the firewall software on a regular basis.

Keep on top of firewall logs, do not ignore messages about the attacks! You may want to report the network addresses of persistent attackers to their providers. In a larger company, make sure that an Intrusion Detection system is installed to warn the technical team about hacking attempts.

Ensure that your antivirus software is updated on a daily basis; automated updates are preferable. Use centralised gateway / firewall virus filtering where possible. Filter out undesirable SPAM mail and suspicious e-mail attachments.

Update your software on a regular basis and apply all security patches released by your software in time. In particular, this applies to the server and firewall software.

If you have a wireless network, treat it as an insecure link to the Internet and ensure that appropriate wireless defences are in place. See our "Wireless for Security for Wireless LAN's" awareness sheet.

Check that the passwords used on your systems are hard to guess. A good password should not be included in any dictionary and consists of combinations of letters, numbers and special characters. "Bob" is a very bad password, *1^4M_B0b#* is a good one.

If you have a system administrator, check that s/he is aware of / follows the current IT security trends. If you are going to hire IT personnel, remember that security-related IT certifications such as CISSP/SSCP, SANS GIAC or TIA Security+ are beneficial. It is unlikely that an SME can afford having a specialised security system administrator or IT security officer. To bypass this limitation, outsource your IT security to specialised information security firms. By doing so, you can receive benefits similar to employing a highly professional security expert for a fraction of such professional's salary.

The only way to find out if your network has security problems is a professional independent security audit. The auditing team of White Hats would try to break into your network using the same tools crackers use and will work with you on fixing the holes discovered. You don't have to pay a fortune for such audit – we in Arhont offer this service for a fraction of charge applied by major consultancies such as KPMG or Ernst &Young while providing similar or better assessment quality.

Finally, have a company security policy outlining the countermeasures we have described above, defining personnel responsibilities and acceptable employees behaviour and providing guidelines on IT backup & resilience solutions as well as handling cracker break-in incidents.

Dr. Andrew Vladimirov
Arhont Information Security