Explainer: What is hacking?

The blanket term â€œhackâ€• can encompass a whole range of attacks â€“ but what are they? Credit: Anant N S

Last week, we woke to news that the largest cyber attack ever was underway in Europe, with reports of global internet speeds falling as a result of an assault on the anti-spamming company Spamhaus.

In recent weeks, the Reserve Bank of Australia has been the target of a cyber attack, as have South Korean banks and broadcasters and BBC Twitter accounts.

The above stories were all reported as "hacking" – a blanket term readily used to encompass a whole range of attacks, from crashing a server to more sophisticated infiltration, such as stealing passwords. But, generally, news stories don't discriminate.

So what are hackers and their methods really like? What follows is something of a glossary, to cut out (or at least bookmark) and keep.

Types of hackers

Phreakers: Perhaps the oldest type of computer hackers, Phreakers discover how telephone systems work and use their knowledge to make free phone calls.

In the past, phone phreakers used what we now think of as hacking techniques to access mainframe computers and programmable telephone switches to obtain information, alter records or evade capture.

Famous (and now retired) phreakers include Kevin Mitnick, Kevin Poulsen and Apple founders Steve Jobs and Steve Wozniak.

Crackers: These guys bypass (crack) security controls on proprietary software, DVDs, computer games and Digital Rights Management (DRM)-protected media.

Crackers trade, share and publish game "cracks", patches, serial numbers and keygens (activation key generators). They also embed malware in their cracks and patches forming Trojans to deter outsiders (mostly "script kiddies"; see below) from using their code.

Unsuspecting people who use their cracks more often than not find themselves infected with worms and viruses (explained below). Such infections often bypass anti-virus tools and firewalls, and are probably responsible for most of the malware on teenagers' home computers.

Black Hat Hackers: These are crackers who actively develop malware and intrusion techniques and tools for evil purposes, Black Hats are motivated by profit.

Criminal organisations, foreign governments and spy agencies will pay handsomely for the latest zero-day (not publicly known) exploit.

Journalist Brian Krebs recently reported a bidding war for a Java exploit valued at more than US$5,000.

White Hat Hackers: These are the good guys. White Hats, also known as "ethical hackers" and "pen-testers", are security researchers.

They test systems (often using the same tools as Black Hats, but within the law) by conducting penetration testing and security audits as a service for businesses and organisations that don't want to be hacked.

White Hats report on any vulnerabilities found and what needs to be done to fix them. Both the US and Australian governments have set up competitions to encourage school and university students to take up (White Hat) hacking as a career.

(My Swinburne team competed in the pilot version of Australia's Cyber Challenge in 2012 and scored higher than all other Victorian universities.)

Grey Hat Hackers: Grey Hats generally work within the law but may publish vulnerabilities and exploits or sell exploits to unknown buyers without asking too many questions.

They may also report vulnerabilities to software vendors anonymously to avoid prosecution. Unfortunately some vendors object to having their defective code discovered and discourage security research on their products.

Script kiddies: Also known as "skiddies", these are a growing number of amateur Black Hats who cannot develop their own code but can adapt other people's exploits and use hack tools to attack organisations and each other.

Script kiddies find the term offensive and have been known to launch cyber-attacks against people who have denigrated them or their skills.

It is likely that many of the "hackers" associated with online protest group Anonymous are script kiddies.

Cyber-troops, cyber-soldiers: These are state-sponsored military personnel trained in hacking techniques who use malware and hacking techniques to spy, gather intelligence, steal intellectual property and disrupt enemy systems.

Spammers and Phishers: Spammers use programs – spambots – to automatically send email, SMSs, instant messages and tweets to potential buyers of their products.

Phishers use the same technologies (and fake "pharming" sites) to entice victims to click on links (and type in user-names and passwords) and download and install malware. The book Spam Kings recounts the early history of many spammers.

Types of hacks

Now that we know who the bad guys are, let's consider what they do and how their actions are likely to affect people.

Script injection (SQL, JavaScript) attacks: Most websites are connected to databases. With Structured Query Language (SQL) injection, attackers run their own code on these databases, allowing them to change records, delete data and extract private information such as credit card numbers, passwords or password hashes.

JavaScript injection happens through publicly-writable web sites such as Facebook, Twitter and sites with forums and discussion boards. If not properly filtered, an attacker can upload script that extracts private information from people visiting the site.

Scripts can bypass firewalls to extract user credentials, track user activities, install malware and even turn on the web camera and microphone. The simplest way to prevent such attacks is to turn off scripting (in your browser).

The Firefox NoScript plug-in is an easy way to do this.

Password cracking: Simply put, if an attacker can guess your password, he or she can take over your computer. Most computer users are overwhelmed by the number of account names and passwords they have to remember, so they tend to re-use them.

An attacker can use SQL injection to recover passwords or password hashes from a poorly-secured website, and then try the same user-names and passwords to log into high-value sites such as bank accounts.

Websites and email systems that restrict password length are the easiest to attack.

Brute force attacks: These use automated tools to guess the password or re-create the password hash.

The most effective ways of preventing this is to (a) use long passwords, and (b) use different passwords.

DoS/DDoS: (Distributed) Denial of service attacks are generally launched against organisations, whose servers are flooded with "broken" network communications that cause the servers to slow down or even crash.

Companies that rely on online trading will lose a lot of money (and reputation) if this happens, and will often pay the attackers to call off the attack.

Viruses, worms and trojans: These are infection carriers used to distribute malware. Viruses travel by thumb drives, worms travel through the internet, and Trojans are downloaded by unsuspecting users.

Anti-virus software will stop most of this, but not the latest (or zero-day) malware attacks.

Crimeware, hijackers and ransomware: Black Hat hacking has matured into an industry. Hackers can purchase crimeware packs for a few thousand dollars and start up a business distributing malware, accepting payments and laundering money.

Hijackers take over your web browser and redirect you to advertising sites. Ransomware infects your computer and prompts you to call a toll-free number, where you can pay to have your computer remotely "disinfected".

Man-in-the-browser malware, such as Zeus, can intercept your online banking sessions in your browser and phone, draining your account by sending money to the attackers.

Bots and bot-nets: Bots emulate human users. Once a bot has infected your computer, you are "owned". Your computer (now a zombie) is remotely controlled by a bot herder who can use it and hundreds of thousands of other zombies to launch DDoS attacks, crack passwords, send spam and host illegal content.

Protect yourself

We can only minimise the risks, but the risks are well understood. Turn off scripting, maintain your anti-virus, don't read unsolicited emails, use long passwords, use different passwords, don't download programs you didn't go looking for, be sceptical … and finally: learn about computer security (to find out what else you can do).

There's no need to be paranoid. Just be careful. White Hat hackers are there to help by exposing the risks and testing the systems. Trust them. They're the good guys.

Source: The Conversation

This story is published courtesy of The Conversation (under Creative Commons-Attribution/No derivatives).