HACKERS PROFILING: WHO ARE THE ATTACKERS?

Who is attacking you? “We don’t know...”

When talking about attackers and hacking it often happens that I ask people working at customer’s sites “who is scaring you?” Most of the time the answer I hear is not “Well, you know... I’m scared by script kids, playing with those couple of unpatched machines I have,” nor is it “I’m really scared about industrial spies.” Rather, 98% of the time the answer is “I don’t know.”

These answers possibly mean that the company, feeling as a potential target, has not developed a proper IT Security Risk Analysis, while trying to figure out who may want to attack its IT infrastructure and gain access to its information.

This mistake probably happens because every time people hear “hackers profiling,” the word “profiling” automatically makes them think about something that has already happened, rather than something that may happen.

The hacking world has changed dramatically in the last thirty years, and the somehow “romantic” figure of the hacker of the ‘80s is far from today’s.

At the very beginning, “hackers” were computer researchers in places like MIT and Berkley; they wore long, white lab coats and gloves while working in big aseptic data rooms. Hacking used to mean “building something” while thinking outside the box, in a different manner, applying new views and problem-solving approaches.

The reason why the hacking phenomenon spread at the beginning of the ‘80s is simple: because of the business. Companies went on the market with the very first home computers, models like Commodore VIC-20 and C-64 or Sinclair ZX-Spectrum, and with the grandparents of today’s Internet routers, the “modems,” running as slow as 300 baud-bits per second!

It was the beginning of the second hacker’s generation, and the most known to the public too. It is not by chance that the general cliché image of a hacker that most people have in mind is that of a teenager, sitting at his desk in his room, typing at the keyboard of his PC, sending commands to the other side of the world... In reality, those kids who were hacking in the ‘80s are probably your IT Security Managers today, and the world of hacking has been replenished with different players. Most of these new players may attack the same targets, but their motivations and goals will probably differ from each others, and substantially so.

Applying the same approach used above, when analyzing the digital evidences left from the attacker on a computer system (meaning, while running a Digital Forensics analysis) we may ask ourselves what the overall goals of the attacker were and why he/she would run that kind of attack on our machine.

The Hackers Profiling Project (HPP) started in 2004 at UNICRI to answer these and many other questions.

And, even if we do not have all the answers yet (since the project is still on-going), we can nonetheless surely address the question raised above: who are the attackers?

As a matter of fact, the HPP research team has been able to identify nine different main categories of attackers. We use the word “attacker” and not “hacker” simply because the evolution of the hacking world and of cybercrime itself has merged together different actors, who do not always belong to the category of “hackers” in a strict sense, at least as we were used to know.

The 9 main attacker categories

Wannabe (Lamer)

The "wannabe," often labelled a "lamer," is the "I would love to be a hacker" kind. They use hacker techniques without neither knowing nor having the curiosity to learn how they actually function. They use "hacker toolkits," which can be downloaded for free from Internet; these toolkits automate processes otherwise made manually and in a "creative" way by more experienced hackers (and that often include mistakes and backdoors). They post a huge amount of messages on forums and BBSs (Bulletin Board Systems), asking other hackers to teach them how to become a real hacker. They want to learn to be hacker without really being one, and often their actions result in huge damages to some computer system or network.

Script kiddie

The "script kid" term stands for "the boy from the scripts," meaning those hackers relaying on UNIX/Linux shell scripts written by others. They lack technical skills and sophistication, and the ones least capable are called "point-and-clickers," since their attacks are called "point-and-click attacks." They are interested only in the result and not in learning how computer and hacking techniques work. They simply download from Internet (or from the "crews" they belong to) software and hacker tools, and follow the related instructions. A very good example of this profile was "Mafia Boy", a 14 years-old kid arrested on Montreal, Canada, after running DDoS (Distributed Denial-of-Service) attacks to e-Bay, Amazon, Yahoo! back in 2000.

Cracker

The term "cracker" was created around the beginning of the '90s, when the hacker community wanted to somehow differentiate the malicious (or lame) actions highlighted by the media, from the serious hacker research done by many underground groups such as CCC, L0pht, THC and so on.

Generally speaking, crackers have good technical skills, which allow them to pursue their purposes; in the last years, nevertheless, due to the different players in the cybercrime arena (particularly when referring to skimming and phishing activities), we have also found crackers with poor or average technical background and field skills. Note also that they are different from the so called "software crackers" who crack software protection to reproduce it illegally (a.k.a. software cracking): this was something very in vogue back in the '90s, and it is still employed in many Asian and African countries.

Ethical Hacker

"Ethical hacker" is not just a term, but it designates an entire debate both in the underground community and in the information security market. An ethical hacker is somebody with excellent hacking skills, whose "past life" may have been with the bad or with the good guys, who decides to help the community, digging with software and discovering bugs and mistakes in widely (or poorly) used IT infrastructures (i.e. social networks), protocols or applications.

They are creative hackers, since they try not to use software created by others and they prefer creating it by themselves (scripts, exploits and/or 0-days) or improving it when there are no useful programmes for their attacks. They would prefer a manual attack rather than an automated one, and this is something to carefully note and a rule to apply to your IDS (Intrusion Detection System)! Ethical hackers are also highly sophisticated and specialised in different operating systems, networks and attack techniques: this means they can range from Sun Solaris, HP/UX or OpenVMS to Microsoft Windows.

QPS (Quiet, Paranoid, Skilled Hacker)

If this type of attacker are on a system, and if they have just a remote feeling that they may be caught, they will disappear. This kind of hackers attack IT systems not because they are looking for information, but perhaps because they just love that particular release of HP/UX that one is running, or loves a SS7 backbone.

The QPS are creative hackers, using as little as possible software made by others, since they prefer creating them by themselves. They are similar to Ethical hackers on a lot of issues.

Cyber-warrior/Mercenary

This is one of those categories that appeared in the last few years because of Internet's globalization and of the "hacktivism" phenomenon. Cyber-warriors feel like heroes from their own environment (i.e. an extremist group with political or religious background). Their skills may vary substantially, from basic ones of a script kid to good or excellent ones, especially when specialized on focused areas (i.e. DDoS, or Web Defacing, or Wi-Fi).

Not being "exposed" in the business environment like the Industrial Spy profile, the Mercenary hacker works on commission, getting money to attack specific targets. A lot of the well-known Russian mobs (such as the RBN, the Russian Business Network) use this kind of elements to support their illegal activities

Industrial Spy Hacker

The practice of industrial espionage had existed as long as business itself, infiltrating spies in companies throughout the years, and walking out of them with information stored on paper files, microfilms, floppy disks, cd-roms and, today, USB keys or emails.

Nevertheless, the recent scandals of industrial espionage that have emerged in the last years surely involve Industrial Spy Hackers, which modernized this practice taking advantage of the new opportunities brought in by Information technology.

Government Agent Hacker

Nowadays the existing information technology and the granularity itself of information allow external attackers from governments to run highly-sophisticated attacks, specifically focused towards nations' know-how in different business markets.

Military Hacker

When the HPP research team introduced this kind of profile back in 2004, the reactions we received were doubtful: it appeared we had gone "too far." Unfortunately, history seems to confirm our assumptions, given the latest waves of "information warfare" highlighted in the newspapers from all over the world.

This profile is also often associated with the term "state-sponsored attack," which effectively represents the logic and the approach behind those attacks run by Military hackers.

Conclusions

While this list of profiles is not to be considered a complete one or a golden rule to follow blindly, it is nevertheless a very good first step. In order to apply it to your own company or institution's environment, keep these profiles in mind when trying to figure out the W4s: Who, Where, Why, When. As for the "How," refer to the Honeynet Project, an excellent program created by Lance Spitzner (www.honeynet.org) to figure out how malicious hackers act. But that's another story.

* Raoul Chiesa, UNICRI Senior Advisor, Strategic Alliances & Cybercrime Issues.