Telefónica

From hacking to modern-day computer crime

Marta Villén Sotomayor
Director of Logical Security and Online Fraud Prevention

1. The evolution of hacking

The days are gone when teenagers attacked the computer systems and data assets of large government organisations and companies merely to challenge their intellect.

The key difference between present-day computer crime and the traditional attacks performed by the first hackers is the intention behind the attacks. The aim today is to obtain valuable data on a government organisation, citizens, the company and its customers, in order to use them as a source of financial profit.

In the past, attackers sought the popularity that is gained by becoming the first person to achieve a successful attack. The attacks of modern-day computer crime, however, are specifically designed to prevent their detection. Stealth is fundamental to their execution and the perpetrators seek financial gain rather than fame.

This shift in motivations that has resulted from criminal groups taking over traditional hackers requires the agents responsible for countering these criminal activities to adapt to the new scenario.

Rapid growth in the amount of valuable information that is transmitted, stored or processed online, together with the increased number of financial transactions necessary for electronic trade, have awakened the interest of criminal groups who are intent on seizing the opportunity to make money.

The threat of cybercrime is particularly concerning in the present day, as criminal groups are becoming increasingly organised and adept.

Over the last decade, organised crime has come to comprehend the opportunities offered by the information society, new technologies and the web; access to an online market through electronic trade, the possibility to operate globally, without any borders. They have also understood that the capacity to tackle this kind of criminality is limited on account of the appearance of anonymity, which generates a feeling of impunity.

Cybercrime is the fastest growing category of crime. In 2006 the US Treasury already considered that the profits it generates had surpassed those of illegal drug sale. In 2009 the number of links to malicious content websites rose by 345% according to the latest IBM X-Force Trend and Risk Report, a document released annually by IBM Internet Security Systems' R&D department (NYSE:IBM).

Computer crime is regarded as one of the most concerning emerging risks among the business community, where it is believed to have greater impact than conventional crime. Lost profits, lost hours of work that need to be devoted to managing security attacks, and damage to corporate image and reputation, are considered to outweigh the problems derived from conventional criminal activity.

Impacts on business include, in addition to direct financial injury, lost earnings as a result of temporary closures of operations to curb the effects of an attack and intangible damage to corporate image and reputation caused by increased negative coverage in the media.

Turning to society at large, attacks against critical infrastructures in energy, healthcare, transport, telecommunications, etc., are strategic targets that could potentially affect a very large part of the population and block the supply of essential services.

Furthermore, computer crime is proving extremely profitable for those involved. And the impact on business for the organisations targeted will very likely be stronger in the future as criminal groups become more ambitious and adept.

2. Modern-day computer crime

Computer attacks are becoming increasingly sophisticated, as they are managed and orchestrated quite aptly by different criminal groups through a network of agents operating in different regions across the world, who are very loosely connected to one another.

The other major shift is the fact that crimes are now committed in separate parts. The activities involved are divided up and executed by specialists in a process comprising a sequence of phases, and it is through the combination of all the phases that the complete crime materialises. The agents of each individual part do not know one another. All they have in common is the distribution of the proceeds, which takes place in advance.

Rather than being executed by one individual, by an association or organised group, attacks are broken up and dealt out to a number of specialised agents, often having no links between them, who are only rewarded for their participation in each of the phases into which the attack was divided.

Current-day criminal attacks are broken up and delegated to different "agents" (individuals who specialise in executing a specific set of actions). These are often located in different

parts of the world and they are rewarded according to the extent of their participation only. This results in a decentralised, very loosely connected process.

The five key phases into which computer crime attacks are divided are:

1. *Reconnaissance* – Investigating potential targets of the attack.
2. *Development* – Building the attack(s) with the greatest chances of success.
3. *Extraction* – Executing the attack against the target and extracting the data.
4. *Exploitation* – Using the products or services obtained through cybercrime to commit criminal activities.
5. *Laundering* – Concealing the origin of the proceeds by moving it through a complex network of bank accounts.

A part of the proceeds of each phase of a profitable attack may be used to develop more sophisticated methods for attack (e.g. viruses and polymorphic and concealed trojans, or automated attack kits), to infiltrate more "sleepers" into organisations who will purport to be honest workers, or to engage with hacker communities in order to have them identify high value targets for subsequent attacks.

2.1. Reconnaissance

The purpose of the *initial Reconnaissance phase* consists in carrying out investigations to help the criminals identify potential targets for their attacks.

Any computer crime starts with a preliminary investigation to identify the government or business organisations and/or individuals offering the best chances for attack and extraction of valuable data.

Using a trawl-and-discard approach, the "explorers" and/or "sleepers" commence by identifying the potential targets that hold valuable data. Next, they determine the probability of success of the attack by studying the security vulnerabilities or weaknesses of the target.

The targets preferred by cyber criminals are institutions that publish details on their operating systems, have equipment with open ports and services, and present known vulnerabilities that can be taken advantage of. Other favourite targets are organisations with a low level of security awareness among their personnel, which also publicise the names of their employees.

The techniques used in this phase are: IP scanning, intercepting unencrypted traffic, detecting security vulnerabilities that can be attacked using exploits, and impersonating an employee to gain access to a building or system.

2.2. Development

The purpose of the *Development phase* is to build attack kits with a high probability of success.

The information on the target obtained in the Reconnaissance phase enables malware developers to design their attack in such a way as to heighten its probability of success.

This phase is usually carried out by internet hacker communities and malware creators.

The most adept malware developers usually test the attack in a "sterile" environment to check its effectiveness. If it passes the tests and is therefore deemed ready for distribution, the developer sells the attack kit over the internet. Quite often the buyer is allowed to try the product and is provided with a "warranty of no detection", which guarantees proper operation and concealability.

Some methods used to carry out cyber attacks do not rely on attack kits that need to be developed. Such is the case of social engineering attacks, information disclosure by accomplices planted to act as moles, and rubbish searching. The Development phase of these techniques is not very important, as it only involves planning the Extraction phase that follows.

The more sophisticated attack kits can be bought online with no need to know or be introduced to hacker communities, and hardly any technical expertise is required to operate them.

2.3. Extraction

The purpose of the *Extraction phase* is to execute the attack against the target and extract the relevant data.

Extraction implies executing the attack to obtain the valuable data held by the target organisation (e.g. personal details from a passport agency, credit card details from a bank, details on new drugs from a pharmaceutical company).

The targets preferred by cyber criminals are official identifiers such as social security and national identity numbers, credit card details and PINs, customer data, email addresses, passwords, patent information, bank account information, names of employees and the degree of security awareness among the staff.

The attack is launched by an agent commonly known as a "miner", often from a part of the world where anti-cybercrime legislation is lax. Once the data have been "harvested", they are advertised and sold online.
When a denial-of-service attack is used, i.e. blocking business services and demanding ransom to unblock them, instead of extracting the data, the agents involved in this phase benefit from providing the means necessary to execute the attack. For instance, they rent out "botnets", consisting in groups of zombie computers ready to implement attack orders.

The agents in this phase typically limit themselves to advertising and selling the stolen data (on the black market).

The range of prices charged for extraction services or "deliverables" varies according to supply and demand in the black market. The chart opposite shows examples of prices asked online for different types of data available from hacker communities.

Overall Rank 2009	Overall Rank 2008	Item	Percentage 2009	Percentage 2008	Range of Prices
1	1	Credit card information	19%	32%	$0.85–$30
2	2	Bank account credentials	19%	19%	$15–$850
3	3	Email accounts	7%	5%	$1–$20
4	4	Email addresses	7%	5%	$1.70/MB–$15/MB
5	9	Shell scripts	6%	3%	$2–$5
6	6	Full identities	5%	4%	$0.70–$20
7	13	Credit card dumps	5%	2%	$4–$150
8	7	Mailers	4%	3%	$4–$10
9	8	Cash-out services	4%	3%	$0–$600 plus 50%–60%
10	12	Website administration credentials	4%	3%	$2–$30

Fuente: SYMANTEC

2.4. Exploitation

The purpose of the *Exploitation phase* is to use the data purchased in the extraction phase to commit other financial crime.

The participants in the Exploitation phase use the product of the work carried out in the Extraction phase. Depending on the nature of the data extracted, they are used to perpetrate financial crimes, such as credit-card fraud, mortgage application fraud, point-of-sale terminal (POS) payment fraud, forgery of negotiable instruments; or else in other types of crime, such as identity theft, extortion and industrial espionage.

But the identities of the agents who take part in this phase are veiled by the agents of the next phase, who are in charge of carrying out the financial transactions on their behalf.

2.5. Laundering

The purpose of the *Laundering phase* is to conceal the identity, source and/or destination of the money, typically by moving it through a complex network of bank accounts.

In the final phase of a profitable attack, the criminal group transfers the proceeds of selling the data and/or the attack kits through a complex network of bank accounts, thereby avoiding detection of the origin, destination and holders of the accounts.

The agents involved in this phase, known as "mules" or "launderers", are paid to make their bank accounts available to receive and subsequently transfer the money to the criminal group's address.

Mules or launderers are enrolled using employment offers posted on the internet, and they are typically unaware as to the identity of who they are serving.