What are hackers looking for?

Julie Gommes,
Cognizant

Abstract:
Regardless of their technical capacities or age, hackers mainly undertake actions as a function not of their profiles but of their objectives, which vary depending on the group. Let us not forget, however, that these groups, despite sometimes quite different motivations, can come together at random for an operation, a pattern we ever more often come across.

The Internet is a new international battlefield distributed over millions of servers. Firms and businesses have posted their signboards, at street level on what Quemener and Ferry (2009) have called "cyberparadises". We are far from the Internet imagined by Perry Barlow (1996), who hoped it would be disconnected from any physical activity and obey its own rules, which would be drafted and modified depending on decisions made by users. In this misshapen mirror reflection of the physical world, people, whatever their motives might be, are roaming who know its codes (in all senses of the word) and are capable of drawing profit from this virtual reality.[1]

The historical boundary between black and white hats (bad and good hackers, respectively) has never been so porous. It is hard to draw a map with this boundary or to identify what these actors are after. In each of these two groups are persons with various skills, ideals and technical qualifications. This boundary does not separate black and white, with pirates on one side. The line of cleavage runs through motivations instead of skills.

Distinct motives…

Getting rich

Criminals are the pirates who have received the most attention in recent years, in particular from the media. They mostly turn to piracy to make money.

Piles of money

Phishing has been one of the most common forms of cybercriminality in the past few years. Hackers often play on what has been called social engineering so as to adapt their hacking techniques to the physical world. This social engineering involves practices that exploit the psychological, social and organizational vulnerabilities of persons or organizations in order to fraudulently obtain goods, services, bank transfers, (physical or virtual) access permissions, confidential information, and so forth. The attacker, often after several months of searches for

[1] This article, including quotations from French sources, has been translated from French by Noal Mellott (Omaha Beach, France). The translation into English has, with the editor's approval, completed a few bibliographical references. All websites were consulted in February 2020.

information on a firm and of contacts with its employees, calls the bookkeeping department, claims to be a senior white collar and asks to have funds transferred in an emergency to an account abroad or to modify a supplier's banking references. Under pressure due to the emergency and under stress owing to the fake white collar's alarming comportment, the department transfers the funds… which will not remain for long on the account and will be laundered thanks to the cooperation of certain online banks (GUEYE 2018).

Between 2010 and 2016 in France, 2300 complaints about scams of this sort were filed; and the Ministry of the Interior estimated damages at €485 million. The accounts of big French firms — Michelin for €1.6 million and Pathé for €19 million — have thus been hacked. These criminals have also targeted small organizations.

Bunches of small sums

Another sort of extortion typical of our times involves "cryptolockers", which block computers while waiting for a ransom to be paid. Hackers use ransomware to collect very small sums (ranging from five to fifty euros in bitcoins) in exchange for their promise to decrypt the servers or computers of the targeted firm or person.

This malware — software designed for malevolent purposes — circulates through e-mail attachments or fake online advertisements, which have links where we heedlessly click. It spreads fast and easily. Some CEOs, their computers blocked, think there is no other solution than to pay. In most cases, the attacker recuperates funds that are made untraceable but never sends the decryption key that would enable victims to unlock their data.

In the summer of 2017, a wave of ransomware attacks blocked production in several big firms, when WannaCry infected Vodafone, FedEx, Renault, Telefonica and Deutsche Bahn.

Masses of data

The current "black gold" is data, ranging from social security numbers in the United States (which can be used to open an account in the person's name and retrieve, in his stead, income tax overpayments) and visa numbers to the ground plans of airports or the instructions for machines that operate oil wells. No major technical skills are needed to find an airport's ground plan or a listed corporation's latest business. Even if a firm manages its security efficiently, third parties (communications firms, plumbers, service-providers) might leave data stored on their own server or a hard drive that is connected to the Internet without basic protection (such as a robust password) — sometimes without knowing about the connection. It is easy to find on line freeware that scans the Internet looking for connected devices, USB sticks, unprotected servers and network attached storage devices (NAS: an autonomous server with files that, connected to a network, mainly serves to store data in a centralized unit for customers). Hackers need but install the software and let it run to retrieve and download data, which they then resell to competitors or, in the case of industrial espionage, to whoever pays the most on a darknet. Darknets are distinct from other peer-to-peer networks in that the "sharing" is anonymous (*i.e.*, IP addresses are not publicly disclosed). Users can communicate while remaining anonymous. In general, "darknet" refers to any form of information and communication technology on the underground web, the usual place for illegal activities or acts of dissidence. On darknets, forums open access to other forums, and so on, till reaching the platforms where major transactions take place — where pirated data are resold.

It is less and less obvious how to legally qualify offenses and rank them by seriousness (GUEYE 2018). Committing them involves many actions: infringement on a website, theft of its database, the recuperation of information from e-mail boxes, hacking a server once its password has been cracked, etc.

Geopolitical destabilization

The diversification of cyberthreats makes it even harder to forestall attacks that seek to destabilize a government or state. Attacking forces might look like nationalistic hackers, or they might not disclose their actual motivation, as in the case of Stuxnet, the virus for slowing down Iran's nuclear program (BONNEMAISON & DOSSE 2014). Recall that Stuxnet, a "worm" discovered in June 2010 and allegedly designed by the US National Security Agency along with Israeli intelligence, targeted Iranian centrifuges for enriching uranium.

It is also hard to clearly tie groups of hackers to a government sponsor, even though, according to Bannelier and Christakis (2017), certain states (not named by the authors) entertain relations with nongovernmental groups whom they use as intermediaries for carrying out malevolent actions against other states.

Gueye (2018) has described the effects (economic, social, environmental or "vital") of such attacks, while emphasizing the "*devastating effect for an unprepared country*" if its system for distributing cash (automatic teller machines), gasoline or fresh produce is locked down. Making a country teeter without firing a single missile or shot is now possible. Developments in civilian ICT and the Internet have made asymmetric combat symmetric on the cyberbattlefield.[2]

Russian interference

In this wargame, eastern Europe has become the Petri dish of Russia, or at least of nationalistic hackers who claim to be close to the Kremlin. Attacks have been on the increase for several years now (HUVERT & RAZON 2019):

- In April 2007, when the Estonian government planned to move the statue of a soldier, a symbol of the Soviet era, a denial of service attack (DoS) targeted the websites of the country's government, political parties, media and banks. Emergency telephone numbers (police, fire brigades) were inoperative for a while. A DoS attack brings down services by blocking, for example, access to a web server or the distribution of e-mail in a firm.
- In July 2008, an attack hit Georgia's President's Office and parliament along with 54 Internet sites of political parties and in finance.
- In 2015, the Russians made maps of Ukrainian power stations; and the following year, these maps were used to launch the BlackEnergy attack. Hackers used backdoors left open on the system and cut off electricity for an hour in Kiev. A backdoor is a feature that, though unknown to legitimate users, opens stealthy access to software or an information system.
- In March 2018, Russian hackers, who claimed to be close to power-holders and the ATP28 group (also known as FancyBear), were identified on the network of Germany's federal administration. According to secret services, these pirates had apparently infiltrated the network a year earlier and gathered information without being detected.

Pirates from the former Soviet Union often have the same profile: engineers (many of them highly trained) who, not wanting to work for a pay far below their level of qualifications, turn toward less orthodox ways of earning a living from their skills. In Europe, many of them are young people from Rumania, Russia or Ukraine who came in first in the hacking matches ("war games" and "capture the flag") organized on the sidelines of cybersecurity conferences. This is where agents from intelligence services take notice of them.

[2] Asymmetric warfare pitches a country's army against an opposing force made up of less well-equipped fighters. Examples are wars of independence, terrorism and guerilla warfare, in contrast to wars between nation-states.

The Indo-Pakistani conflict

Patriotic Russian hackers are not alone in taking position on the line of combat when tensions mount with a rival. Indians and Pakistanis have engaged in ceaseless cyberwarfare related to their dispute about Kashmir. As recently proven, some of these hackers have honed their skills, for instance, Godzilla, an Indian hacker.

- In 2012, Godzilla started by rather coarsely defacing easily targeted websites. This is often a good exercise for beginners, a way to build up a résumé and show what one is capable of doing. Website defacement refers to an alteration of the presentation of a pirated website by, for example, displaying one country's flag on the homepage of another country's government.
- In 2013, Godzilla brought down the websites of several Pakistani ministries: Railroads, the Economy, the Interior, Religious Affairs, the Environment… while posting the loophole used for the attack. The three administrators who managed all key government websites accessed a joint database with the password *11111*.
- In 2014, Godzilla knocked down several official Pakistani websites (the government, the Ministry of Defense and the President's Office) not by attacking the sites directly but by targeting their infrastructure. Godzilla also attacked Bangladesh several times; and with little doubt, these hackers will be at the origin of attacks against countries that position themselves as enemies of India.

Activism

"Hacktivists" have been active in politics since the 1960s. Gicquel (2014) has mentioned the German Chaos Computer Club (CCC, one of the most influential hacker organizations in Europe), L0pht Heavy Industries (pronounced "loft", a renowned group of Boston-based hackers active from 1992 to 2000) and the writings of Perry Barlow (1947-2018, an essayist, libertarian and founding member of the foundations Electronic Frontier and Freedom of the Press). Even today, various activist groups are using hacking techniques to advance their causes. Hacking is not the goal (as for nationalists) but a means for communicating or collecting information.

Let us take a brief look at two groups of hacktivists: Anonymous and Telecomix.

The Anonymous movement emerged in 2006 on the website 4Chan, a mixture of a forum, chat group and platform for sharing images. Strictly speaking, Anonymous is not a group with codes and rules (a group of the sort that nationalists or criminals might form) but a movement and beacon for many a hacker (COLEMAN 2014). Though initially lacking cohesion, it has gained visibility through its small attacks:

- In 2006 and 2007, it attacked the American Nazi Party.
- In 2011, hacktivists claiming to belong to Anonymous published the names of pedophiles and invited other hackers to do as much. This call was heard: the e-mail and IP addresses of 1589 pedophiles were posted on line.

Gabriela Coleman has defined this movement as "*a myriad of relations, structures and moral positions*" with the objective of systematically attacking whoever causes harm to human beings: intelligence services, Church of Scientology, etc.

Over time, the movement has repositioned itself around communications, its major goal being to communicate well and fast: "*Anonymous produces as many contents as its members have creative skills*" (GICQUEL 2014). It undertook actions in 2008 against the Church of Scientology. In 2010 when Wikileaks was blocked, Anonymous set up mirror websites to diffuse translated diplomatic cables and gain visibility; and it launched DoS attacks against Visa and Mastercard. Several groups were working together around ideological poles within the movement.

Anonymous broke up in the summer of 2011. The result is an archipelago of independent hackers, ideological hotbeds of resistance with actions ranging from opposition to censorship in Tunisia to the fight against the "rape culture" in the United States. The infiltration of corporate information systems is no longer an inevitable *modus operandi* as it used to be.

Telecomix, formed around the fight against the Telecoms Package in the European Union in 2009, has always been strongly involved in politics. In 2011, these hacktivists helped people from North Africa and the Mideast maintain communications when Internet connections were down:

- In Egypt, where landlines were not down, since the army used landline telephones to communicate, Telecomix proposed analog technology via FDN, a French operator, and sent the numbers and codes of access to hundreds of fax machines in Egypt, along with directions about how to connect old analog modems (56k).
- In Syria, the initial idea was to offer Syrian revolutionaries an electronic toolkit for their online security and anonymity. Telecomix informed Syrians by mail (six thousand addresses) of links toward various tools, such as the proxy Tor. It also shared a link toward a chat board for discussing these tools. This has helped Syrians communicate outside the country and improve the safety of their communications.
- In parallel, Telecomix has posted technical information about mass surveillance in Syria and Libya, and organized campaigns for sending 56k modems in case Internet connections are cut in Syria (GUITON 2013).

…but now and then common interests

We might assume that high walls separate from each other these hacktivists, libertarians, criminals (who want to make money, if possible right away) and nationalists (who want to bolster their country's influence). However these players might work together during an attack.

In August 2008, several Georgian websites were blocked; and others, pirated. The site of the Ministry of Foreign Affairs caricatured President Mikheïl Saakachvili as Adolf Hitler. Given the geopolitical context, this attack was blamed on Russia. Its characteristics were:

- a military sense of discipline in its organization (attributed to nationalists);
- the know-how of criminals (who were paid to execute attacks fast);
- the experience of groups of activists involved in operations of communication.

Even if Russian nationalists oversaw the operation, it is hard to know how the attack started. It followed a pattern that we observe more often. The most probable explanation is that nationalists hired criminals to conduct the attack.

An online battle between hackers from countries in the Mideast and the West broke out shortly after the terrorist attack in 2015 on the satirical newspaper *Charlie Hebdo* in Paris. There were several phases of attacks and counterattacks:

- A first wave of actions by Western hackers targeted randomly chosen websites in Arabic, in particular through distributed denial of service attacks (DDoS, a DoS attack using several sources called "zombies") or website defacements under the guise of Anonymous. These attacks for "fighting back" did not require highly technical skills. Well-documented online tools could be used to carry them out.
- During a second phase, attackers from the Mideast targeted vulnerable websites in French (camping grounds, village town halls, small shops), often designed by public relations agencies or independent developers who did not pay enough attention to security. On the surface, this was a rather symmetric combat between Western and Mideastern forces on the cyberbattlefield. This was but the first offensive however.

● Once Internet sites had been infected and servers made accessible, another group of highly experienced pirates (not from the Mideast) upped the ante and stole data (server data, banking card information, etc.) to offer them for sale on the darknet's black market.

We were thus confronted with more seasoned hackers, but it was impossible to know whether the occasion enabled them to commit their misdeeds or whether, in preparation of this series of attacks, they had already "recruited" less experienced hackers in order to provide cover for their crimes. After all, engineers would be busy trying to get sites up and running or to remove defacements instead of watching out for suspicious activities on their servers.

What will tomorrow's hackers be after?

Warfare tomorrow

The growing tendency is for hackers pursuing different objectives to work on joint projects. This complicates the task of our armed forces. Since mid-June 2019, NATO has switched paradigms, recognizing cyberspace as a new front, like war on land, on the sea or in the air — a zone where states launch attacks against other states or mount a defense of themselves or their allies. This decision has been carefully thought out. In 2014, leaders of NATO countries had already pointed out that an online attack could destabilize the real world. During an attack, hackers might play different roles:

● a destabilizing role, as during the attacks against Georgia or Ukraine.

● a role of recruitment to muster, now and then, "script kiddies" (a derogatory word referring to beginners who spend most of their time trying to infiltrate information systems by using scripts or programs not of their own making) to make a smokescreen for criminals (who will be paid for hiring out their technical skills).

● A role of diversion so that attacks will be blamed on others (the insertion of natural language comments in code so as to mislead investigators, software proxies, etc.) and so that the targeted country's attention will be diverted toward another country.

Information tomorrow

Hackers' technical skills will soon enable them to easily mount campaigns of information or disinformation (in particular, website defacements) while other hackers will contact journalists and transmit to them information about practices at the limits of legality (like Edward Snowden's revelations). Pirates might also share the information they have hacked with an international consortium of journalists, as in the case of the Panama Papers, when more than 11.5 million confidential documents from Mossack Fonseca, a Panamanian law firm, were leaked with detailed information about more than 214 thousand offshore entities and their owners, including politicians, billionaires, sports champions and celebrities).

References

BANNELIER K. & CHRISTAKIS T. (2017) “Construire la paix et la sécurité internationales de la société numérique. Acteurs publics, acteurs privés: rôle et responsabilités”, *Les Cahiers de la Revue Défense nationale*, pp. 5-90, available via https://www.irsem.fr/data/files/irsem/documents/document/file/2283/Cahier_Bannelier_Christakis%20-%20Cyberattaques%20(FR).pdf.

BARLOW J.P. 1996 “A declaration of the independence of cyberspace” (San Francisco, CA: Electronic Frontier Foundation) available at https://www.eff.org/cyberspace-independence.

BONNEMAISON A. & DOSSE S. (2014) *Attention: Cyber! Vers le combat cyber-électronique* (Paris: Economica).

COLEMAN G. (2014) *Hacker, hoaxer, whistleblower, spy: The many faces of Anonymous* (Québec: Lux Éditions).

GICQUEL C. (2014) *Anonymous, la fabrique d un mythe contemporain* (Paris: Fyp Éditions).

GUEYE P. (2018) *Criminalité organisée, terrorisme et cybercriminalité. Réponses de politiques cybercriminelles* (Dakar: L’Harmattan Sénégal).

GUITON A. (2013) *Hackers. Au cœur de la résistance numérique* (Paris: Éditions au Diable Vauvert).

HUVERT E. & RAZON B. (2019) *Les Nouvelles Guerres. Sur la piste des hackers russes* (Paris: Arte Éditions/Stock).

QUEMENER M. & FERRY J. (2009) *Cybercriminalité: Défi mondial* (Paris: Economica).