Awareness,
a major weapon of defense

Jérôme Notin,
GIP ACYMA

Abstract:
During our everyday uses of digital technology in our personal and occupational environments, we are constantly faced with actions motivated by criminal intent. To protect ourselves, two complementary pillars have to be set up: the technical tools for protection and the awareness of each and everyone. What is the government doing to raise awareness on a large scale? What targets do cybercriminals choose? Why is awareness necessary?

Launched in October 2017, https://www.cybermalveillance.gouv.fr was set up to assist the private persons, firms, local authorities and associations, not to mention the "operators of vital importance", whom cyberattacks have targeted.[1] This website ensues from a national cybersecurity strategy presented by the government in June 2015.[2] It assignment is threefold:

- boost the awareness and prevention of problems related to cybersecurity by promoting the right practices and issuing alerts;
- provide assistance to victims to help them diagnose problems, offer them simple and adapted advice, and orient them toward competent services (or even toward specialized service-providers in the victim's local area); and
- observe threats in order to detect and anticipate trends as they emerge and respond to them.

This organization has taken the form of a "group of public interest" (GIP: *groupement d'intérêt public*) called ACYMA. This private-public partnership brings together parties from the state and "civil society" who are committed to the fight against malevolent action in cyberspace. ANSSI (Agence Nationale de la Sécurité des Systèmes d'Information, under the Prime Minister's Office) and the Ministry of the Interior helped design the website. Other members are: the ministries of Justice and of the Economy and Finance, the State Secretariate in charge of digital technology and several NGOs (*e.g.*, associations for protecting consumers or assisting victims), trade groups, insurance firms, software editors and so forth. Besides their financial support, the members — more than forty in July 2019 — reinforce and foster the GIP's activities.

[1] This article has been translated from French by Noal Mellott (Omaha Beach, France). All websites were consulted in February 2020.

[2] The objectives were set in the *National Strategy for Cybersecurity* published in October 2015: *La Stratégie nationale pour la sécurité du numérique* (Paris: Prime Minister's Office), 44p. available via https://www.ssi.gouv.fr/uploads/2015/10/strategie_nationale_securite_numerique_fr.pdf.

As its actions have expanded, Cybermalveillance.gouv.fr has, owing to its originality and the services provided, proven its ability to respond to the expectations of these various parties. Nearly 29,000 persons looked for assistance on the platform in 2018. The number of requests grew fourfold: from 500 in January to nearly 4,000 in the last month of the year. During the first six months of 2019, the platform had already assisted more than 60,000 victims — twice the number as during all of 2018 but during half the time. Users have learned about our existence, whence tis strong growth.

By analyzing requests and exchanges, we have adjusted our actions to the expectations and reality in the field, in particular our actions for raising awareness and issuing alerts about new threats.

What is original about this setup is that, when an incident occurs, the GIP usually intervenes upstream from the actions conducted by other government services. In this respect, its actions are a "sensor" that offers public authorities valuable information about cybercriminality, even in cases when the victims did not initially intend to file complaints — because they were unaware that the incident could serve as grounds for a legal action, because they thought that a legal action would have few chances of succeeding but would waste time, or because, ashamed of having fallen victim, they feared the fallout on their image. Cybermalveillance.gouv.fr intervenes by systematically asking victims to file a complaint once a breach of the law has been averred, helping them wend their way through procedures and providing advice that comes out of its close collaboration with the Ministry of the Interior.

Among its strong points is that Cybermalveillance.gouv.fr can detect a trend from events that, if taken separately, might be overlooked but, once taken together, shed light on a serial phenomenon. During its first months of operation, the website helped identify a massive scam thanks to the technical reports on interventions made by its registered service-providers. In most cases, victims have the impression of being targeted by a scam but do not imagine filing a complaint for the reasons already indicated. Our detection of this cybercrime and our exchanges with the services of the ministries of the Interior and of Justice led the Paris district attorney's office to open an investigation in March 2018. This investigation, conducted by C3N (the center for fighting against online criminality in the National Gendarmerie), led to the arrest of three persons whose actions targeted nearly 8,000 victims and to the confiscation of approximately two million euros in early February 2019.

Th ability to detect threats as soon as possible enables us to issue alerts on our website and on social networks (Twitter, Facebook, LinkedIn). Thanks to this GIP and the support of its members, several alerts have been widely reported in major media (*e.g.*, the evening news on television). This helps us reach as many potential victims as possible.

Choice targets: Very small, small and medium-sized firms

Though not exempt from the risks of cyberattacks, big firms and big public administrations are often better equipped to fend, both in terms of skills and technical means. Unfortunately, such is not usually the case with small and medium-sized firms or local authorities. These smaller entities are a choice target of cybercriminals, who try to maximize profits while minimizing efforts. Cyberattacks can have dramatic effects on smaller organizations, whose economic survival might be at stake.

Let us make an easy assumption: that a firm's priority is to conduct its business and that its information system is merely a "support" for this activity. However digitization has made information systems a highly critical component. Without an information system, most organizations cannot operate and would see their business activities grind to a halt. Nonetheless, the services surrounding the information system are often outsourced to companies that fiercely compete with each other by lowering prices when making offers. The offer of a lower price always attracts the client's attention. However this economic argument often entails a lower level of services, in particular for security.

As for cybercriminals, they are aware of this situation and of the resulting weaknesses that they can exploit for their own purposes. The stereotype of a lone pirate attacking a multinational corporation from his dormitory room is now (nearly) obsolete. Firms have to fend against a "cybercriminal ecosystem" that has taken shape around poles of competence. Some of these criminal groups have specialized in designing high-tech weapons for attacks; others, in probing information systems to detect loopholes and gateways; and still others in buying this information to put it to use or to place the "loot" acquired during an attack on the darknet, the haunt of cybercriminality where every- and anything is bought and sold.

Through its exchanges with victims and registered service-providers, Cybermalveillance.gouv.fr has observed that the cyberattacks conducted by criminal groups are increasingly "professional" and the damages, ever more substantial.

Ransomware provides a clear illustration of this trends in techniques and criminality. Initially, attacks of this sort usually took place through e-mail attachments or links with *phishing* messages (poorly written and not precisely targeted). The operations now being conducted against firms are completely different. Cybercriminals try, for example, to directly penetrate corporate information systems via points of access outside the firm (WiFi, telecommuting, telemaintenance). They manage to breach the system via unpatched software or by "cracking" passwords that are not robust enough. Once in the firm's information system, hackers might spend several days doing reconnaissance. They map the network in an effort to detect all major digital assets. They might steal these assets to sell them to other criminals who will know how to put them to use. Once the map is drawn, they launch the visible phase of the attack, usually not during normal working hours, which the hackers have already detected. They encrypt the firm's data starting with… its backups. As cybercriminals well know, every firm has backups, which, for reasons of convenience, can usually be directly accessed on line via the firm's network. In fact, many firms do not keep any other backups of recent data.

By the time offices open, all this information has been encrypted; the backups on the firm's servers, made inaccessible; and a message asking for a ransom is waiting. This ransom usually amounts to a share of the firm's sales — an "acceptable" share compared with the pending loss. Ransoms range from hundreds of euros for very small firms to thousands for local authorities and hundreds of thousands for small and medium-sized firms. Ransom demands vary as a function of the targeted firm's ability to pay; and this clearly proves that the perpetrators have not randomly chosen their target — that they have, since their breach of the information system, calculated the maximum they can extort.

Such an attack's effects are not limited to the financial loss of the ransom alone. After all, some victims are inclined to pay the ransom. However the firm should always factor in two other costs: the cost of production being shut down, perhaps for several days, while the information system is down; and the cost of repairing the system.

As these examples show, firms that are easily assumed to be focused on their core activity (business) and operational responsiveness might be inadequately prepared for cyberattacks. They will, therefore, be helpless when they fall victim to cybercriminals, whose actions are, as already pointed out, becoming more and more professional.

Awareness, a major line of defense

Awareness is still the best weapon against cyberattacks. It is essential for firms. Employees must be made aware of cyberthreats and of the practices they should adopt in order to detect them and fend them off. This exercise is often difficult, since the topics related to cybersecurity are usually felt to be boring and meaningless. Furthermore, users (regardless of their position in the firm, whether CEO or office clerk or even the firm's computer engineers) tend to see cybersecurity as a source of restrictions and constraints.

Taking the foregoing remarks (drawn from work with its members) as its starting point, Cybermalveillance.gouv.fr designed in 2018 the first part of its "awareness toolkit". Completed in June 2019, this kit contains short videos, graphics, practical fact sheets, reminders, etc. This educational tool, which may be downloaded for free, focuses on personal uses; but the topics discussed can also interest firms for professional use. For example, users who know how to detect and react to *phishing* messages will also know how to do so on the job. The kit concentrates on several themes: phishing (currently the major vector for attacks), password management (one of the principal walls protecting information systems), the security of mobile devices (smartphones, tablets, etc., with their specific, major points of vulnerability), the differences between personal and occupational uses, etc. A major decision was to release this kit under an Etalab 2.0 license, which allows for modifying, adding or deleting contents. Many entities have simply added their own logo to the kit in order to garner stronger support from their employees.

Among these efforts in favor of prevention and awareness, let us mention the preparedness for managing the crisis resulting from a cyberattack. Firms, especially smaller companies, are usually not adequately prepared to deal with such difficult and, for them, exceptional situations. Our platform offers advice about the major types of attacks.

For a firm, the question is no longer to know whether it will be attacked, but when. Will it be adequately prepared to prevent or handle the attack? Unfortunately, cybercrime does not just happen to someone else.