La Suisse fait face à cinq cybermenaces majeures

TECHNOLOGIE L'Office fédéral de la cybersécurité (OFCS) a publié hier son dernier rapport semestriel, insistant sur des attaques de plus en plus sophistiquées et personnalisées

ANOUCH SEYDTAGHIA

Messages WhatsApp, e-mails, appels téléphoniques ou encore smartphones insuffisamment mis à jour, les vecteurs d'attaque des cybercriminels sont multiples. Et de plus en plus, ils prennent le temps de mener des agressions numériques personnalisées, afin d'augmenter leurs chances de succès. D'où l'importance, pour les entreprises et les particuliers, d'être non seulement en alerte permanente, mais de mieux protéger ses appareils. Tel est, en substance, le message qu'a voulu transmettre hier l'Office fédéral de la cybersécurité (OFCS).

Il n'y a pas eu d'explosion des signalements de cyberincidents en 2025 auprès de l'office: il y eut 64 733 annonces l'an dernier, soit 3% de plus qu'en 2024. Derrière ce chiffre, qui n'est qu'un reflet de la situation réelle, se cachent toutefois des attaques qui semblent être plus dévastatrices. Les cyberattaques «se caractérisent par une meilleure coordination ainsi qu'une efficacité et une précision en hausse», affirme Florian Schütz, directeur de l'OFCS. Voici cinq tendances repérées ces derniers mois.

1 De redoutables rançongiciels

En octobre dernier, la Confédération alertait sur le groupe de criminels appelé Akira. Environ 200 entreprises suisses avaient alors été victimes d'attaques par son rançongiciel, pour un préjudice de plusieurs millions de francs. En 2025, 138 attaques par *ransomware*s, logiciels chiffrant et volant les données, ont été signalées à l'OFCS. Les hackers du groupe Akira exploitent des failles dans les équipements de cybersécurité SonicWall, notamment les VPN d'entreprise, pour s'introduire dans les réseaux sans autorisation. Ces attaques réussissent surtout parce que de nombreuses organisations tardent à appliquer les correctifs. «La menace que font peser les rançongiciels reste d'autant plus élevée que les groupes criminels sont en mesure d'exploiter très vite les vulnérabilités ou les accès compromis. Même si à ce jour aucun des groupes connus ne s'en prend spécifiquement à la Suisse, les attaques opportunistes constituent la norme et touchent donc également les organisations suisses», note l'OFCS.

«Les cyberattaques se caractérisent par une meilleure coordination ainsi qu'une efficacité et une précision en hausse»

FLORIAN SCHÜTZ, DIRECTEUR DE L'OFFICE FÉDÉRAL DE LA CYBERSÉCURITÉ

2 Des fraudes financières dévastatrices

Il existe une myriade de types de fraudes. Et en termes de préjudice financier, «le phénomène de la fraude à l'investissement en ligne reste le plus dommageable», déplore l'office. Il y eut 848 signalements liés à ces arnaques en 2025, un chiffre stable. Mais la tendance est à la hausse en ce qui concerne les arnaques à la récupération, où les malfaiteurs cherchent à faire croire aux victimes de fraudes à l'investissement en ligne qu'elles pourront récupérer l'argent volé. Tandis qu'au premier semestre 2025, 145 cas de «fraude au remboursement» avaient été signalés, leur nombre a largement doublé durant la période sous revue, avec 325 cas signalés, avertit l'OFCS.

3 De fausses antennes de téléphonie mobile

L'année passée, une nouvelle forme de diffusion de l'hameçonnage et de la fraude en ligne a été observée pour la première fois en Suisse. Cette technique s'appelle «SMS Blaster»: les cyberagresseurs se baladent avec un appareil de la taille d'un boîtier d'ordinateur qui se fait passer pour une antenne de téléphonie mobile et incite les téléphones portables situés à proximité à se connecter à lui. Une fois la connexion établie, l'appareil pris pour cible est rétrogradé au protocole 2G obsolète. Les pirates exploitent une vulnérabilité et envoient des SMS contenant différents types d'arnaques. Il faut donc se méfier de tous les SMS reçus: même si des malfaiteurs utilisant des SMS Blaster ont été arrêtés en Suisse, le phénomène ne disparaît pas.

4 Des appareils piratés à distance

Attention à vos modems, routeurs ou même caméras de surveillance: tous ces objets connectés peuvent être contrôlés à distance par des pirates, qui peuvent les utiliser pour mener des attaques contre des tiers, ou infiltrer les réseaux internes de leurs victimes. L'OFCS alerte ainsi sur la menace croissante due aux réseaux proxy ORB (pour *operational relay boxes*) qui touche la Suisse. Le nombre d'appareils compromis faisant partie de ces réseaux ne cesse d'augmenter, note l'office. «La plupart du temps, ces réseaux sont créés et exploités par des organisations spécialisées agissant sur mandat de tiers. Ces derniers disposent ainsi, moyennant rémunération, d'infrastructures prêtes à l'usage (*proxy-network-as-a-service*). Cette solution permet aux acteurs malveillants de dissimuler efficacement l'origine de leurs activités», avertit l'OFCS.

5 Des infrastructures critiques sous pression

Depuis un an, soit le 1er avril 2025, les exploitants d'infrastructures critiques (tels les aéroports, centrales nucléaires ou grandes chaînes de supermarchés) sont soumis à l'obligation de signaler toute cyberattaque dans les vingt-quatre heures. En un an, 325 signalements sont parvenus à l'OFCS. Parmi les attaques les plus fréquemment annoncées, se trouvent le piratage (20%), les attaques par déni de services (qui bombardent les sites de requêtes) (16%), les vols de données d'accès (12%), les malwares (10%), les fuites de données (10%) et les rançongiciels (9%). L'OFCS ne donne pas de détails supplémentaires sur ces attaques.