

PUBLICITÉ

ACCUEIL > CYBER Réservé aux abonnés

Yves Nicolet, procureur fédéral: «Le combat contre les cybercriminels se fait à armes inégales. Mais nous obtenons parfois des succès»

Alors que la Suisse est ravagée par des cyberattaques de toutes sortes, que font les autorités? Yves Nicolet, procureur fédéral chargé de la lutte contre la cybercriminalité auprès du Ministère public de la Confédération, défend l'action de ses services



«Notre travail est plus compliqué qu'il y a 5 ans, parce que les technologies d'attaques se sont nettement démocratisées et deviennent accessibles quasiment à tout le monde», affirme Yves Nicolet. — © Zoé Jobin pour Le Temps



Anouch Seydtaghia

Publié le 10 avril 2026 à 20:26. / Modifié le 11 avril 2026 à 21:40.

🕒 10 min.



Résumé en 20 secondes ⓘ



- Yves Nicolet affirme que des condamnations de cybercriminels sont possibles malgré les obstacles techniques et juridiques, citant un développeur britannique condamné à sept ans de prison.
- L'entraide judiciaire internationale prend trop de temps face à la volatilité des données numériques, mais le projet e-evidence de l'UE devrait améliorer la situation.
- Les arrestations récentes de membres du groupe de ransomware 8Base en Thaïlande démontrent que les cybercriminels ne sont jamais totalement à l'abri.

Yves Nicolet, procureur fédéral: «Le combat contre les cyber...

Un article de Anouch Sey...



00:09

1.0x

15:30

|ElevenLabs

Des SMS frauduleux, des appels suspects, des e-mails contenant des arnaques, des publicités promettant des rendements miraculeux... Sans cesse, nous sommes ciblés par des pirates informatiques, trouvant des subterfuges de plus en plus sophistiqués pour tenter de nous soutirer des sommes allant de centaines à des dizaines de milliers de francs. Au niveau des entreprises, les attaques peuvent causer des pertes se chiffrant en millions. En face, que font les autorités? Y a-t-il un espoir de poursuivre des pirates agissant pour des multinationales du cybercrime? Yves Nicolet est procureur fédéral chargé de la lutte contre la cybercriminalité auprès du Ministère public de la Confédération (MPC). Rencontré en marge du Forum Forward organisé en mars par *Le Temps*, il affirme que son combat porte des fruits.

Publicité

Le Temps: Nous avons souvent l'impression d'une impunité quasi totale des auteurs de cybercrimes, car ils sont impossibles à identifier et à appréhender. Est-il réellement possible de se battre contre eux?

Yves Nicolet: Je comprends ce sentiment, mais la réponse est oui. Il est clair que les auteurs agissent depuis l'étranger, qu'ils utilisent des serveurs informatiques comme vecteurs d'attaques, disséminés partout autour de la planète. Cela ne nous empêche pas de les identifier et, dans certains cas, d'obtenir des condamnations. Récemment, l'action du MPC et de Fedpol a permis de condamner à une peine privative de liberté de sept ans, un développeur et distributeur de kit d'hameçonnage en Grande-Bretagne. Mais il est vrai qu'il est complexe, pour les autorités de poursuite pénale, d'obtenir des fournisseurs de données qu'ils nous aident à remonter aux auteurs de ces forfaits. Nous devons bien sûr utiliser l'entraide judiciaire internationale pour tenter d'obtenir des informations. Le problème, c'est que ce processus prend beaucoup trop de temps. En face, les auteurs évoluent très vite, les données sont volatiles, et souvent conservées peu de temps. Dans le meilleur des cas, une réponse peut nous parvenir après quelques mois. Dans le pire des cas, nous recevons parfois les réponses des années après, voire jamais.

Nous disposons certes d'une Convention sur la cybercriminalité qui me permet, comme procureur suisse, de contacter directement un prestataire étranger, pour autant qu'il soit sur le sol d'un Etat membre de la convention et qu'il accepte de transmettre les données demandées. Mais s'il refuse de coopérer, on se heurte à un mur et il faut alors recourir à l'entraide judiciaire avec les inconvénients mentionnés plus haut. Cela devrait s'améliorer, puisque l'Union européenne a créé un paquet législatif, appelé «e-evidence», permettant d'ordonner aux prestataires de nous transmettre des données avec un

caractère contraignant. Il faut espérer que la Suisse pourra en bénéficier dans les années à venir, car les moyens actuellement à disposition ne sont pas suffisants en termes de collecte de preuves électroniques à l'étranger.

Vous avez ainsi face à vous un nombre très important d'obstacles...

Oui, il y a énormément de barrières. On peut les comparer à la facilité qu'ont les auteurs, eux, de passer les frontières, de se protéger par des mécanismes innombrables d'anonymisation... Ils utilisent des VPN, des proxys, des réseaux comme Tor ou des botnets, soit des réseaux d'ordinateurs infectés que les auteurs utilisent pour s'anonymiser. Tout cela rend notre tâche très compliquée. Le combat contre les cybercriminels se fait à armes inégales. Mais grâce à une bonne collaboration au niveau national et international, nous obtenons tout de même des succès.

Lire aussi: [Encore beaucoup trop naïfs, les Suisses sont victimes de cyberarnaques perfides combinant faux sites web, SMS et appels téléphoniques](#) 

Et en plus, on a l'impression que les outils techniques des hackers sont devenus plus puissants encore?

Oui, notre travail est plus compliqué qu'il y a 5 ans, parce que les technologies d'attaques se sont nettement démocratisées et deviennent accessibles quasiment à tout le monde. En face, nous avons dû nous adapter. Maintenant, la plupart des polices des cantons possèdent des unités de cybercriminalité dédiées, avec des spécialistes hautement qualifiés. Au niveau fédéral, des enquêteurs spécialisés et des analystes techniques expérimentés ont également été engagés.

Malgré ces soutiens, avez-vous parfois des moments de découragement face à des succès qui sont quasi invisibles?

Dans la lutte contre le cybercrime, les moments de découragement passent vite, notamment en raison des perspectives encourageantes. A titre d'exemple, les techniques permettant de tracer les flux de cryptomonnaies se sont améliorées. Cela nous permet, dans les affaires de rançongiciels (*ransomware*) par exemple, de beaucoup mieux identifier et comprendre les structures mises en place par les auteurs. La coopération nationale et internationale, indispensable dans le domaine cyber, a également gagné en efficacité en s'intensifiant ces dernières années. Le rôle de l'Agence européenne de police, Europol, et celui de son pendant judiciaire, Eurojust, sont déterminants et permettent de garantir un échange d'informations fluide. Grâce à la collaboration entre les différentes autorités nationales et internationales concernées, à titre d'exemple, les principaux leaders du groupe de ransomware 8Base ont pu être arrêtés en février 2025 en Thaïlande et extradés vers la Suisse, plus tard dans l'année. Ce groupe avait causé des dégâts importants dans notre pays, et ces arrestations ont été un succès majeur pour l'enquête menée sous la direction du MPC.

Lire aussi: [Déjà ciblée de manière intensive par les cyberattaques, la Suisse doit s'attendre à pire encore en 2026](#) 

Mais avez-vous des moyens suffisants, en Suisse, pour combattre des cybercriminels aux ressources quasi illimitées?

Pendant des années, nous avons réclamé davantage d'enquêteurs spécialisés en cyber au niveau fédéral. Ce message a finalement été entendu et le parlement a décidé de renforcer les effectifs de Fedpol, permettant ainsi d'augmenter le nombre d'enquêteurs spécialisés. Au niveau du Ministère public de la Confédération, nous sommes deux procureurs et trois procureurs assistants. Nous sommes actuellement encore en mesure de gérer les procédures en cours, étant précisé que seules les affaires d'une certaine complexité et de grande ampleur relèvent de la compétence du MPC. Pour que nous nous saisissions d'un dossier au niveau fédéral, il faut qu'il concerne une série de cas commis par les mêmes auteurs dans plusieurs cantons, causant des dommages économiques importants et dont les auteurs agissent depuis l'étranger en usant de processus techniques complexes.

A vous entendre, cela pourrait concerner l'immense majorité des cyberattaques commises en Suisse, non?

Nous décidons au cas par cas. Dans la majorité des cas, les procédures sont menées au niveau cantonal. Nous prenons régulièrement en charge des attaques par *ransomware* qui font souvent des dégâts importants un peu partout dans le pays, touchant de nombreuses entreprises. En publiant un communiqué de presse conjoint en octobre 2025, plusieurs autorités fédérales, dont le MPC, ont émis une alerte sur le groupe de pirates Akira, qui a attaqué plus de 200 entreprises, causant des millions de francs de perte. Le cas était important et nous avons pris en main ce dossier dès 2024 en rassemblant les dossiers cantonaux et en poursuivant au niveau fédéral les investigations initiées par les cantons. L'enquête est en cours.

Mais dans le cas d'Akira, si on veut être un peu provocateur, on peut se dire que la Confédération en était réduite à diffuser un message de prévention, l'espoir d'appréhender ce groupe de pirates étant quasi nul...

Je vois les choses différemment: la prévention, en matière de cybercriminalité, est l'une des premières armes pour lutter contre ce fléau. Sensibiliser les entreprises par rapport aux normes de sécurité, mais aussi les individus, est capital. Un e-mail d'apparence anodine, un SMS reçu, un système mal sécurisé, un mot de passe trop simple à découvrir... Il faut vraiment que l'on augmente notre niveau de sécurité. Le Ministère public, qu'il soit cantonal ou fédéral, n'a pas pour mission de faire de la prévention, laquelle n'entre en principe pas dans ses compétences. Mais si on peut s'y associer, il ne faut pas hésiter.

Revenons à ce groupe de hackers appelé Akira: avez-vous l'espoir de pouvoir, au moins, lui compliquer la vie?

Ce communiqué avait un objectif de prévention, mais aussi celui d'inciter d'autres victimes à nous contacter. Cela permet d'en savoir plus sur ce groupe et de nourrir la coopération nationale et internationale dans le cadre des procédures menées à leur rencontre. Et cela nous permet d'augmenter notre force de frappe. Il s'agit de ne pas baisser les bras: si plusieurs pays parviennent à identifier des cybercriminels, on augmente sensiblement les possibilités de les faire arrêter et juger. D'autre part, il a également été possible dans certains cas de saisir des serveurs utilisés par les pirates et de parvenir ainsi à détecter et stopper des attaques en cours.

Mais de nombreux groupes de hackers se trouvent en Russie ou sont protégés par Moscou. Ils semblent bénéficier d'une impunité quasi totale, non?

Dans le contexte actuel, il n'y a plus d'entraide judiciaire entre la Russie et la Suisse. Quant à la protection éventuelle de Moscou ou l'influence de l'Etat russe, honnêtement, je n'ai pas d'éléments factuels établis à ce sujet. Ce ne sont que des suppositions. Mais l'absence d'entraide avec Moscou est un gros problème, puisque certains pirates agissent depuis la Russie.

Ils sont ainsi intouchables?

Ce n'est pas un obstacle absolu, car les cybercriminels se déplacent. Ils ne restent pas nécessairement dans un seul pays toute leur vie. A un moment donné, ils vont en sortir et voyager. Si on arrive à les identifier, on les met sous mandat international, et c'est là qu'ils peuvent tomber. Pour citer un exemple, la collaboration entre le MPC, Fedpol, Europol et d'autres partenaires nationaux et internationaux a permis d'identifier des membres du groupe NoName057 (16) dans le cadre de la procédure menée en Suisse et de saisir des ordinateurs. Et comme évoqué plus tôt, plusieurs membres du groupe 8Base ont récemment été arrêtés, ce qui démontre que les auteurs de cybercrimes ne sont jamais complètement à l'abri.

Une question sur la récente mise en consultation de deux ordonnances sur la surveillance de la correspondance par poste et télécommunication. Comme d'autres, Andy Yen, directeur de Proton, s'y était vigoureusement opposé, craignant une surveillance de masse. Quelle est votre opinion?

Lire aussi: [«Des entreprises sous-estiment les cyberrisques, voire les nient, alors même que nous les contactons de manière répétée»](#) 

Parler de surveillance de masse en Suisse, à mon sens, c'est pratiquement méconnaître, d'une part, les conditions liées à l'application de la loi, qui sont extrêmement strictes, et, d'autre part, un problème de ressources qui est évident. Nous n'aurions pas en permanence accès aux données d'un fournisseur de services numériques. La loi est et sera toujours extrêmement restrictive. Une surveillance de masse, pour moi, revient à ce que l'Etat surveille en temps réel tous les contacts, toutes les conversations de tous les particuliers. C'est matériellement et juridiquement impossible en Suisse actuellement.

De nouvelles versions de ces deux ordonnances repartent en consultation. Vous donneront-elles des pouvoirs supplémentaires bienvenus, de votre point de vue?

Plutôt que de pouvoirs, je parlerais d'informations. On ne peut pas ouvrir une procédure sur la seule impression que «quelque chose s'est produit». Il doit exister des soupçons étayés par des faits. On doit avoir des traces, des informations qui nous disent que cette société, ou cette administration, ou cette entité, a été attaquée. Si c'est le cas, on peut ouvrir une procédure. Et c'est dans le cadre de cette procédure que nous devons aller chercher ces informations. C'est uniquement à cette fin qu'on va demander à des fournisseurs de services numériques de conserver des données, puis de nous les donner, si

elles sont liées à un individu qui pourrait avoir commis cette infraction. Donc c'est extrêmement restrictif. Et effectivement, avoir davantage d'informations, pour les autorités de poursuite pénale, est évidemment un avantage. Et je pense que c'est aussi un avantage pour la sécurité intérieure de la Suisse et, par conséquent, pour l'ensemble de la société. Mais au final, c'est la politique qui décide, et nous travaillons avec les moyens qui sont mis à notre disposition.

On voit de plus en plus de personnes attirées par des investissements frauduleux, notamment en cryptomonnaies, et tout perdre. Comment luttez-vous contre ce fléau?

Oui, c'est un phénomène qui provoque énormément de dégâts en Suisse. Il y a des discussions pour savoir si des cas doivent être traités au niveau cantonal ou fédéral. De tels cas ne relèvent toutefois pas de ma division et du domaine cybercriminalité au sens étroit, mais de la division «Criminalité économique». Les cantons travaillent vraiment de manière intensive à essayer de trouver des solutions, notamment pour regrouper ces enquêtes.

Roblox est une plateforme de jeux très prisée des ados et est ciblée par des pédocriminels. Comment luttez-vous contre eux?

C'est un type de cybercriminalité qui ne relève pas du domaine de compétence du MPC. Mais je peux dire que, de manière générale, il existe des moyens de traquer ces cyber-pédocriminels, notamment via l'investigation secrète, ou ce que l'on nomme plus communément les enquêtes sous couverture. Ce sont des mesures mises en œuvre en principe par les polices et les ministères publics cantonaux, qui permettent à des enquêteurs de se faire passer pour des adolescents ou des adolescentes, et de surveiller, voire de repérer éventuellement, des criminels en ligne. La police est présente sur les réseaux.

Fin 2024, les autorités fédérales ont perquisitionné le domicile d'une personne enquêtant sur des piratages, et qui renseignait des médias, et saisi son matériel informatique. Ces mesures prises à son égard n'étaient-elles pas trop dures?

L'action du Ministère public de la Confédération, à l'instar des autres autorités de poursuite pénale en Suisse est strictement fondée sur le Code de procédure pénale (CPP). Toutes les mesures qui ont été prises dans le contexte évoqué étaient conformes au cadre légal en vigueur.

Bio express

1970 Naissance à La Chaux-de-Fonds.

1994 Licence en droit à l'Université de Lausanne.

1995 à 2001 Greffier du juge d'instruction puis au Tribunal d'accusation.

2001 à 2005 Juge d'instruction dans le canton de Vaud.

2005 à 2011 Substitut du juge d'instruction du canton de Vaud.

2011 à 2016 Procureur dans le canton de Vaud dans le domaine de la criminalité économique et de la cybercriminalité.

2016 à 2020 Procureur fédéral chargé de la criminalité économique et de la cybercriminalité.

1er janvier 2020 au 30 juin 2024 Procureur fédéral spécialiste dans le domaine de la cybercriminalité au MPC.

Dès le 1er juillet 2024 Procureur fédéral responsable du domaine de la cybercriminalité au MPC.

NOS LECTEURS ONT LU ENSUITE