Haute école spécialisée bernoise
Institute for Cybersecurity and Engineering ICE

Communication
2501 Bienne
Téléphone 032 321 62 11
mediendienst.ti@bfh.ch
bfh.ch/ti

COMMUNIQUÉ DE PRESSE

Bienne, le 1er juin 2021

abuse.ch incorporé à la BFH

abuse.ch, plateforme prisée et mondialement connue axée sur la protection contre les menaces cybernétiques, a conclu un partenariat avec la Haute école spécialisée bernoise BFH. Désormais, abuse.ch est géré en tant que projet de recherche par l'Institute for Cybersecurity and Engineering ICE. Les secteurs de l'administration, de l'industrie et de la recherche continuent d'avoir accès aux données Open Source gratuites ainsi qu'aux nouvelles possibilités de lutte contre les menaces cybernétiques.

Partout dans le monde, des autorités judiciaires ou policières comme le FBI ou le département de la justice américain ont remporté des batailles contre la cybercriminalité grâce à abuse.ch, la plateforme suisse à but non lucratif chargée de la protection contre les cyberattaques. Celle-ci connait une forte notoriété dans la communauté informatique internationale. À ce jour, abuse.ch a identifié et neutralisé des logiciels malveillants (« malwares ») sur plus de 1,2 million de pages internet et analysé plus de 40 millions de programmes malveillants. La plateforme communautaire a récemment conclu un partenariat avec la Haute école spécialisée bernoise BFH et sera désormais hébergée par l'Institute for Cybersecurity and Engineering ICE.

À l'avenir, abuse.ch sera géré et développé sous forme de projet de recherche de la BFH. « Avec abuse.ch, la BFH renforce ses compétences dans les domaines de la prévention, de la détection et de l'analyse des menaces cybernétiques », souligne le professeur Endre Bangerter, coresponsable de l'Institute for Cybersecurity and Engineering ICE. Grâce à la BFH, les milieux économiques et les pouvoirs publics profiteront ainsi de nouvelles opportunités de projet et prestations pour tiers dans le domaine de la cybersécurité. abuse.ch continuera de proposer des informations en libre accès (« Open Source Threat Intelligence ») fiables et gratuites aux administrations, partenaires industriels et fabricants de solutions de sécurité. « Avec abuse.ch, nous sommes désormais en mesure de protéger efficacement et à grande échelle les réseaux de nos partenaires industriels et de leur clientèle face aux menaces cybernétiques », souligne Endre Bangerter.

Roman Hüssy a fondé et dirigé abuse.ch pendant 15 années. Dorénavant, il continuera de gérer le projet en tant que collaborateur scientifique de l'ICE. « Grâce à la BFH, la plateforme communautaire continuera d'être exploitée à des fins non commerciales », précise Roman Hüssy. Mieux encore : « En tant que projet de recherche, abuse.ch bénéficiera des ressources nécessaires pour son développement futur et pour d'autres projets dans le domaine de la cybersécurité qui bénéficieront au final au grand public », souligne-t-il.

Contacts

Prof. Endre Bangerter, coresponsable de l'Institute for Cybersecurity and Engineering ICE, Haute école spécialisée bernoise, endre.bangerter@bfh.ch, tél. +41 32 321 64 78

Roman Hüssy, collaborateur scientifique à l'Institute for Cybersecurity and Engineering ICE, Haute école spécialisée bernoise, roman.huessy@bfh.ch, tél. +41 31 848 54 15

Michelle Buchser, spécialiste en communication, Haute école spécialisée bernoise, Technique et informatique, michelle.buchser@bfh.ch, tél. +41 32 321 62 11

Informations complémentaires :

- Page de projet de la BFH
- www.abuse.ch

abuse.ch

La compétence centrale d'abuse.ch est l'« Open Source Threat Intelligence », terme qui désigne les données et informations en libre accès liées aux menaces cybernétiques. Ces informations aident les milieux économiques et les organisations à mieux se protéger contre d'éventuelles cybermenaces. Opérateurs de télécommunications, sociétés, fournisseurs de solutions de sécurité informatique : de nombreuses entreprises utilisent les données partagées par abuse.ch afin de protéger leurs réseaux internes ou ceux de leurs client-e-s. Grâce à l'utilisation généralisée de ces données, abuse.ch touche directement ou indirectement un vaste nombre d'organisations ou d'internautes, contribuant ainsi de manière décisive, depuis sa création voilà 15 ans, à la cybersécurité à travers le monde depuis sa création.

Les pouvoirs publics utilisent les données d'abuse.ch pour améliorer leur hygiène informatique nationale, par exemple en cherchant et « nettoyant » des sites internet utilisés pour propager des logiciels malveillants (« malware »). La justice n'est pas en reste : des autorités judiciaires du monde entier utilisent les données fournies par abuse.ch pour leurs enquêtes dans le domaine de la cybercriminalité.

abuse.ch a plusieurs projets communautaires à son actif. En voici une sélection :

- **URLhaus :** plateforme proposant des informations sur les sites internet utilisés par les cybercriminels pour propager des logiciels malveillants (« malware»).
- **MalwareBazaar :** plateforme sur laquelle des chercheurs et chercheuses en sécurité informatique peuvent partager leurs données sur les malwares actuels.
- **ThreatFox :** plateforme de partage d'informations techniques liées aux menaces cybernétiques en cours (Indicators Of Compromise – IOCs).

L'infrastructure d'abuse.ch comporte actuellement environ 55 serveurs et 200 bacs à sable (« sandboxes »). Tous les mois, le projet génère un trafic réseau de plus de 130 To et traite près de 300 millions de requêtes HTTP. abuse.ch répond quotidiennement à quelque 2 millions de demandes API et génère 100 Go de données compressées.