

Pirater la santé, c'est attaquer les personnes. Pour élaborer les politiques nécessaires et assurer aux victimes un droit à réparation, il est essentiel d'évaluer la portée et l'impact des cyberattaques dirigées contre la santé. Le **Cyber Incident Tracer (CIT) #HEALTH** est une plateforme visant à remédier au déficit d'information concernant les cyberattaques perpétrées contre le secteur médical à l'échelle mondiale – des attaques qui perturbent les soins de santé, compromettent les données médicales sensibles et portent atteinte aux patients, aux professionnels de la santé ainsi qu'aux structures et organisations de ce secteur.

La plateforme fournit des éléments concrets pour comprendre les cyberattaques contre la santé. Elle vise à mettre en lumière ce type d'attaques ainsi que leur impact sur les gens et la fourniture des soins. En effet, le manque de données et de connaissances sur cet impact a compliqué l'élaboration de politiques dans ce domaine. Les conséquences des cyberincidents sur les individus n'ayant jusqu'ici pas été correctement évaluées, le monde n'a pas pris de mesures adéquates pour garantir la sécurité dans le cyberspace. De telles mesures sont pourtant essentielles pour que les gens puissent être pris en charge médicalement sans avoir à craindre pour leur sécurité et le respect de leur vie privée.

Les cyberattaques contre la santé ont des conséquences sur les personnes. Des retards ou des interruptions dans les soins peuvent être fatals pour certains patients, et les professionnels de la santé, qui ont fait vœu de sauver des vies et ne peuvent plus remplir leur mission, souffrent de répercussions psychologiques. Ces attaques ont aussi pour effet d'éroder la confiance que le public place dans le secteur médical. Leurs auteurs misent sur la peur et la vulnérabilité de leurs cibles.

La plateforme contient des données sur les cyberattaques contre la santé à partir de juin 2020. Elle est mise à jour chaque semaine. Des informations sur la méthodologie utilisée sont disponibles sur la plateforme CIT.

Access à la plateforme Cyber Incident Tracer (CIT) #HEALTH

[La plateforme](#) fournit des données concrètes pour comprendre les cyberattaques dirigées contre des institutions du secteur de la santé, en particulier les centres de soins, les entreprises de développement et de fabrication de matériel médical, et les entreprises pharmaceutiques.

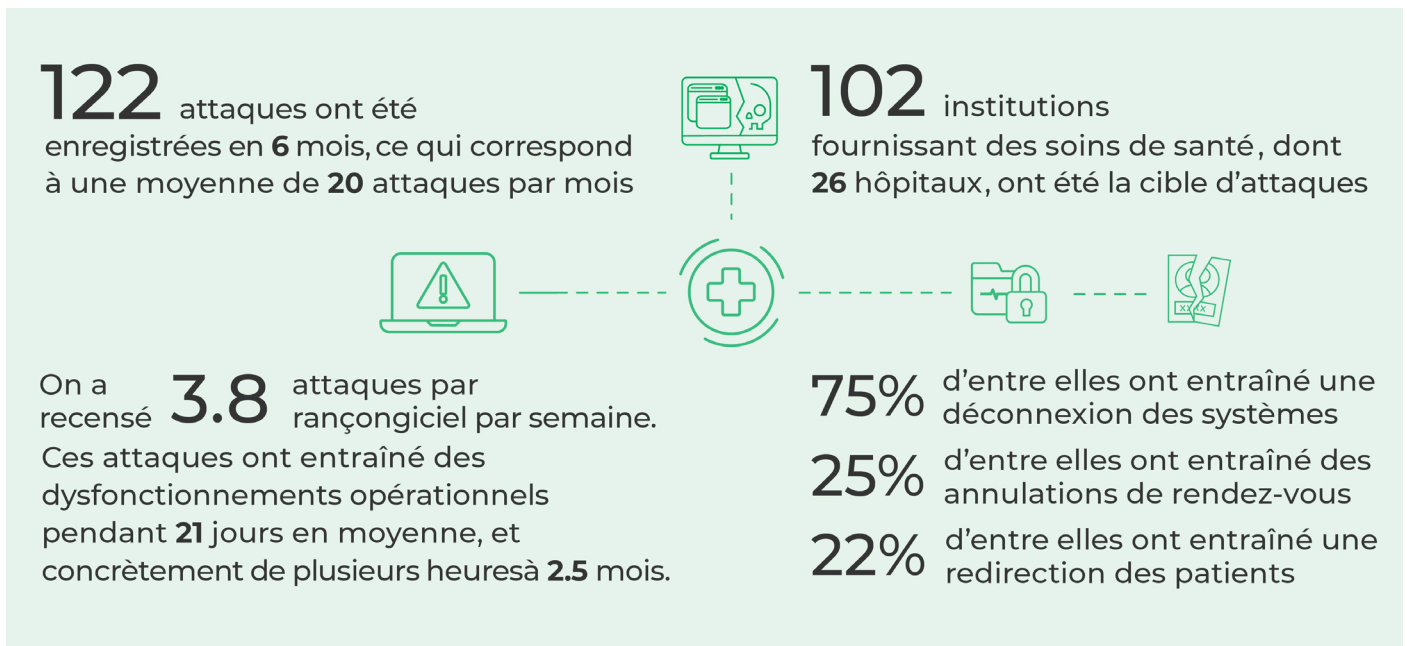


Cyber Incident Tracer #HEALTH

Since January 2021, **244** healthcare organizations across **33** countries have been cyberattacked, including **32** ransomware, **1** malware and **4** unknown attacks. There were cases where accounts were compromised and data thefts incidents

Attack Type | Country | From | To

L'analyse des données concernant les cyberattaques perpétrées au cours des six premiers mois de 2021 a fait ressortir les éléments suivants :



Les pays ne recueillent et ne communiquent pas tous des données sur les cyberattaques de la même manière.

Mesurer la portée et l'impact sociétal des cyberattaques contre la santé permettra de faire changer les choses et d'empêcher que de nouvelles attaques de ce type se produisent. Associez-vous à l'appel à l'action du CyberPeace Institute.

Si vous souhaitez soutenir l'action du CyberPeace Institute, nous vous invitons à lire nos appels à l'action et notre appel au soutien ci-dessous.

Appel à l'action adressé aux gouvernements

Des mesures doivent être prises pour mettre un terme aux cyberattaques contre la santé. La santé est un droit fondamental et un bien commun que les autorités publiques ont le devoir de protéger.

Des mesures adaptées doivent être mises en œuvre pour faire respecter les normes de conduite et le droit international dans le secteur de la santé. Les infrastructures médicales sont indispensables et doivent être protégées contre tout type d'attaque.

Investissez des ressources pour armer le secteur de la santé contre les cybermenaces.

Contribuez à des initiatives qui visent à mieux faire connaître l'impact réel des cyberattaques contre la santé sur les gens et sur la fourniture des soins.

Veillez à ce que les auteurs de cyberattaques répondent de leurs actes et à ce qu'ils soient arrêtés. Veillez aussi à ce que les procédures judiciaires soient transparentes et efficaces pour que les

Appel à l'action adressé aux institutions du secteur de la santé

Tenez-vous informé des cybermenaces qui existent et parez-les de manière proportionnée. Procédez à des analyses des vulnérabilités, à des évaluations et à des opérations visant à corriger les bugs.

Informez toutes les parties prenantes concernées des vulnérabilités. Mettez en sécurité les vecteurs et points d'attaques potentiels. Signalez rapidement les incidents et leur impact sur la fourniture des soins. Informez vos patients et/ou vos clients quand leurs données ont été compromises.

Appel à l'action adressé aux industriels

Intégrez les sécurités nécessaires (« sécurité dès la conception » et « sécurité par défaut ») aux produits destinés au secteur médical sur l'ensemble de la chaîne d'approvisionnement. Sponsorisez la recherche technologique sur « les réseaux zéro-confiance », la mise en place et la surveillance de l'authentification continue grâce à la biométrie comportementale, afin que les hôpitaux soient moins tributaires des vulnérabilités de leur chaîne d'approvisionnement.

Notre priorité est de réduire l'impact des cyberattaques sur la vie des gens dans le monde entier. Aidez-nous dans cette entreprise – nous avons besoin de votre soutien !

Vous pouvez soutenir notre mission en faisant un don: donate@cyberpeaceinstitute.org ou sur [cyberpeaceinstitute.org](https://www.cyberpeaceinstitute.org)

Mission du CyberPeace Institute

Le CyberPeace Institute est une organisation non gouvernementale indépendante et neutre dont la mission est de garantir les droits des personnes à la sécurité, à la dignité et à l'équité dans le cyberspace. L'Institut travaille en étroite collaboration avec les partenaires concernés pour réduire les méfaits des cyberattaques sur la vie des gens dans le monde entier, et leur fournir une assistance. En analysant les cyberattaques, l'Institut met en évidence leur impact sociétal ainsi que la manière dont les lois et les normes internationales sont violées, et promeut un comportement responsable pour faire respecter la paix dans le cyberspace.

CyberPeace Institute

Campus Biotech Innovation Park
Avenue de Sécheron 15
1202 Geneva, Switzerland



[cyberpeaceinstitute.org](https://www.cyberpeaceinstitute.org)



[@CyberPeace Institute](https://www.linkedin.com/company/cyberpeaceinstitute)



[@CyberpeaceInst](https://twitter.com/CyberpeaceInst)

Adaptez vos prix selon les ressources des professionnels de santé afin d'éviter de créer des inégalités entre ceux qui ont les moyens de mettre en place la cybersécurité et ceux qui ne les ont pas.

Soutenez les initiatives qui offrent un accès à la cybersécurité aux établissements de santé n'ayant pas les capacités, les ressources ou les aptitudes pour assurer leur protection.

Renforcez la transparence et la vigilance dans le partage d'informations sur les vulnérabilités.

Notre appel au soutien

Nous continuons de développer la plateforme CIT. Dans ce contexte, nous recherchons des partenaires à même de nous soutenir pour la collecte de données, le développement technique de la plateforme, la mise au point d'une méthodologie empirique pour évaluer l'impact des cyberincidents sur les individus et la société en général, ainsi que la définition d'une méthode pour catégoriser les attaques et en identifier les auteurs.

Si vous pouvez nous aider dans ces différentes étapes, merci de nous contacter à l'adresse suivante : cit@cyberpeaceinstitute.org