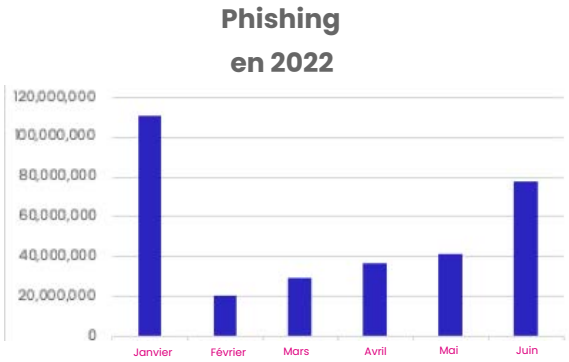
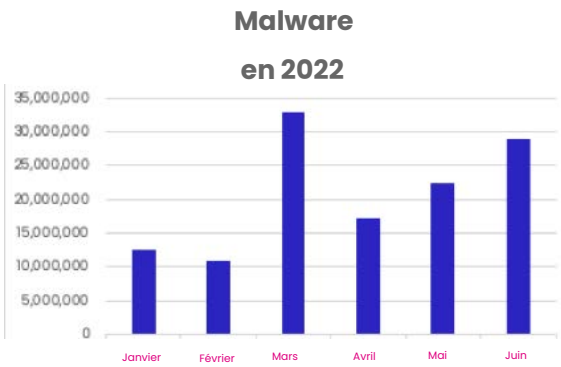
Alerte dans le monde de la santé : les cyberattaques contre les établissements de santé français se multiplient

Pour les établissements de santé du monde entier, et particulièrement en France, le risque cyber a changé. En effet, la pandémie de COVID-19 les a forcés à migrer de nombreux services dans le cloud. Les cybercriminels ont sauté sur l'occasion et se sont empressés d'en faire leur cible de prédilection. Alors que le retour à la normale se profile, le monde de la santé reste convoité par les hackers, qui n'hésitent pas à multiplier les attaques sophistiquées basées sur des ransomwares et les stratégies de vol de données.

Mi-avril 2022, 9 hôpitaux de la région Grand Est ont ainsi été compromis. Les autorités craignent que les données volées ne soient utilisées pour lancer des attaques de phishing ciblées contre les patients.[1]



"Les hackers ont envoyé 32,9 millions d'emails contenant des malwares en mars 2022"



En août 2022, LockBit, un groupe de hackers à l'activité prospère, s'est attaqué à un hôpital de l'Essonne en faisant tomber tous ses systèmes à l'exception de sa téléphonie. Cette fois-ci, en plus des craintes liées au vol de données, des patients ont dû être évacués. Objectif de l'attaque ? Le paiement d'une rançon de 10 millions de dollars.[2]
Ces exemples ont fait couler beaucoup d'encre, mais ils suivent un schéma bien trop fréquent, que ce soit en France ou dans d'autres pays du monde. Si les cybercriminels s'attaquent si volontiers aux établissements de santé, c'est parce que ces derniers dépendent de l'informatique pour fournir des services aussi urgents qu'importants.

Parallèlement à ces offensives, le 1er semestre 2022 marque aussi une explosion du nombre d'emails contenant des malwares, un vecteur d'attaque majeur. Les hackers ont ainsi envoyé 32,9 millions d'emails de ce type en mars 2022, soit une augmentation de 201 % en un mois.[3]

Dans le même temps, le nombre d'emails de phishing, un autre vecteur fréquemment utilisé contre les établissements de santé, a lui aussi fortement augmenté en 2022, pour atteindre 77 millions en juin. Au total, les emails contenant des malwares et les emails de phishing ont atteint les neuf chiffres au cours du premier semestre 2022, avec 125 millions pour les premiers et 315 millions pour les seconds.[4]

Le retour d'Emotet, qu'Europol considère comme le malware le plus dangereux de la planète, est particulièrement inquiétant pour les autorités sanitaires.[5] D'après le Centre de coordination de la cybersécurité pour le secteur de la santé américain (HC3), les chevaux de Troie sont souvent utilisés contre les établissements de santé, et les souches issues d'Emotet sont particulièrement représentées dans ce domaine.[6]
C'est en Europe que les emails infectés par Emotet ont été les plus nombreux au premier semestre 2022, avec 119 978 exemplaires observés.

[1] Malwarebytes. « Hospitals taken offline after cyberattack ». 26 avril 2022.

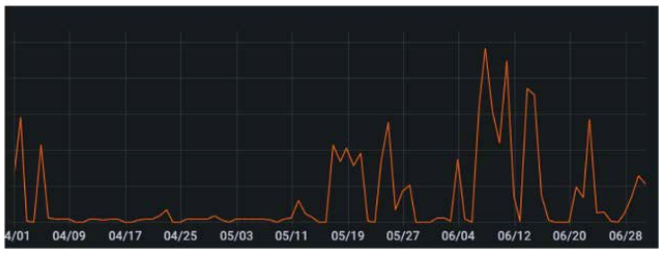
[2] The Record. « LockBit ransomware group implicated in crippling attack on French hospital ». 24 août 2022.

[3 & 4] Vade. Rapport sur le phishing et les malwares - T2 2022. 24 août 2022.

[5] Europol. « World's most dangerous malware EMOTET disrupted through global action ». 27 janvier 2021.

[6] Health Sector Cybersecurity Coordination Center. « The Return of Emotet and the Threat to the Health Sector ». 2 juin 2022.

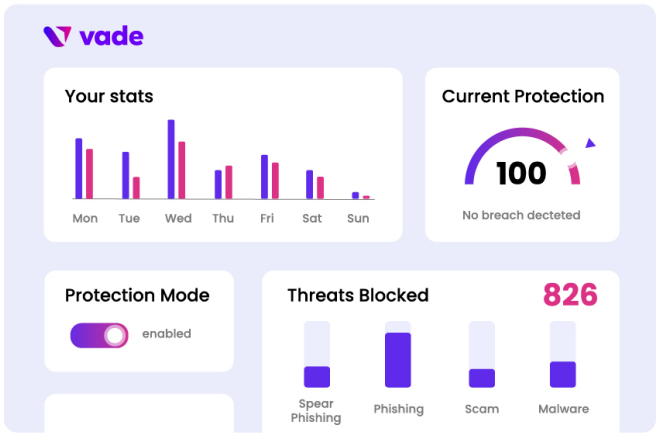
"C'est en Europe que les emails infectés par Emotet ont été les plus nombreux au premier semestre 2022, avec 119 978 exemplaires observés."



Protégez votre établissement et vos patients

Les attaques par ransomware bloquent des systèmes informatiques stratégiques dont les établissements de santé ont besoin pour fonctionner. Tout système ou appareil informatique peut être touché par un ransomware, mais c'est via l'email que les ransomwares s'infiltrent majoritairement. 54 % des fournisseurs de services informatiques managés affirment que les emails de phishing constituent la principale cause d'infections par des ransomwares.[6]

Depuis un simple email, un ransomware peut rapidement paralyser un hôpital et dégrader les soins aux patients. Les dossiers médicaux sont eux aussi exposés, car ils sont très recherchés sur le marché noir. Il s'agit également d'un moyen de pression pour les cybercriminels lors de la négociation d'une rançon.



Solutions Vade

Vade est une entreprise de cybersécurité spécialisée dans le développement de technologies de détection des menaces grâce à l'intelligence artificielle. Présente dans le monde entier, elle protège un milliard de messageries professionnelles et personnelles et propose aux marchés des FAI, PME et MSP des solutions et produits autonomes qui permettent de renforcer la cybersécurité et d'accroître l'efficacité informatique.

Que vos emails soient gérés sur site ou dans une solution comme Microsoft 365, l'ajout d'un niveau de cybersécurité supplémentaire peut éviter qu'une tentative d'attaque ne se transforme en violation. Les solutions de cybersécurité de Vade pour l'email peuvent protéger votre hôpital ou établissement de santé des attaques par email malveillant, notamment :

Phishing/Spam :

Vade scanne tous les éléments de l'email, y compris les adresses, liens, images et pièces jointes, bloquant les attaques de phishing avancées et le spam qui contournent les autres solutions.

Malware/Ransomware :

Vade analyse les caractéristiques malveillantes de l'email, des pages web, des fichiers partagés et des pièces jointes afin de détecter les malwares et ransomwares en temps réel, sans retarder pour autant la remise des emails.

Spear phishing (Business Email Compromise) :

Vade examine la totalité de l'email à la recherche d'anomalies qui ne peuvent être détectées par simple scan de l'URL ou des pièces jointes, notamment des noms affichés factices et du contenu textuel suspect.

Pour en savoir plus sur les solutions permettant de protéger votre hôpital ou votre organisation de santé contre les cyberattaques véhiculées par les emails, *contactez Vade sans plus attendre.*

À propos de Vade :

- 1 milliard de boites mails protégées
- 100 milliards d'emails analysés par jour
- 1400 + partenaires dans le monde
- Renouvellement annuel de 95 %
- 17 brevets internationnaux actifs

En savoir plus :

www.vadesecure.com

Contact :

Service commercial

sales@vadesecure.com