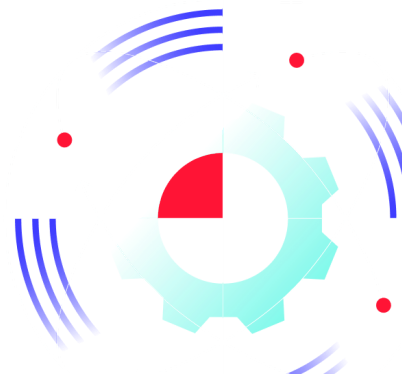


Cybercrime's Anatomy les menaces sur le monde de la santé

gatewatcher.com/lab/cybercrimes-anatomy-les-menaces-sur-le-monde-de-la-sante/



Introduction

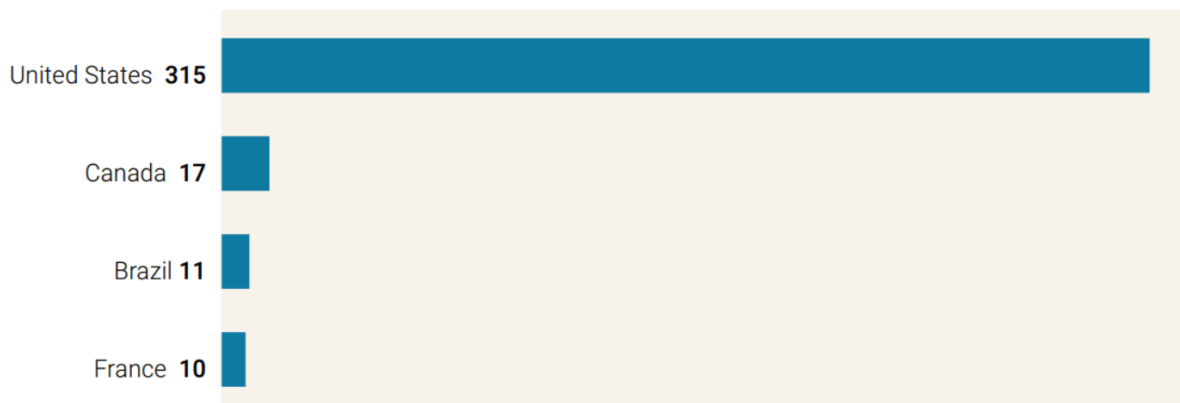
En 2023, les attaques visant le domaine de la santé ont atteint un niveau de visibilité sans précédent.

Bien que le ciblage de ces systèmes ne soit pas nouveau, la France a été particulièrement touchée par un nombre significatif d'incidents au cours de cette période.

Ce constat est partagé par de nombreux organismes. Dans les deux derniers rapports du Healthcare-ISAC relatif aux incidents survenus au troisième et quatrième trimestre 2023, l'hexagone se place au 4ème rang des pays les plus touchés par ces cyber-attaques. Le Healthcare Information Sharing and Analysis Center (ISAC) est une organisation qui favorise la collaboration et le partage d'informations sur les menaces et les vulnérabilités liées à la cybersécurité dans le secteur de la santé.

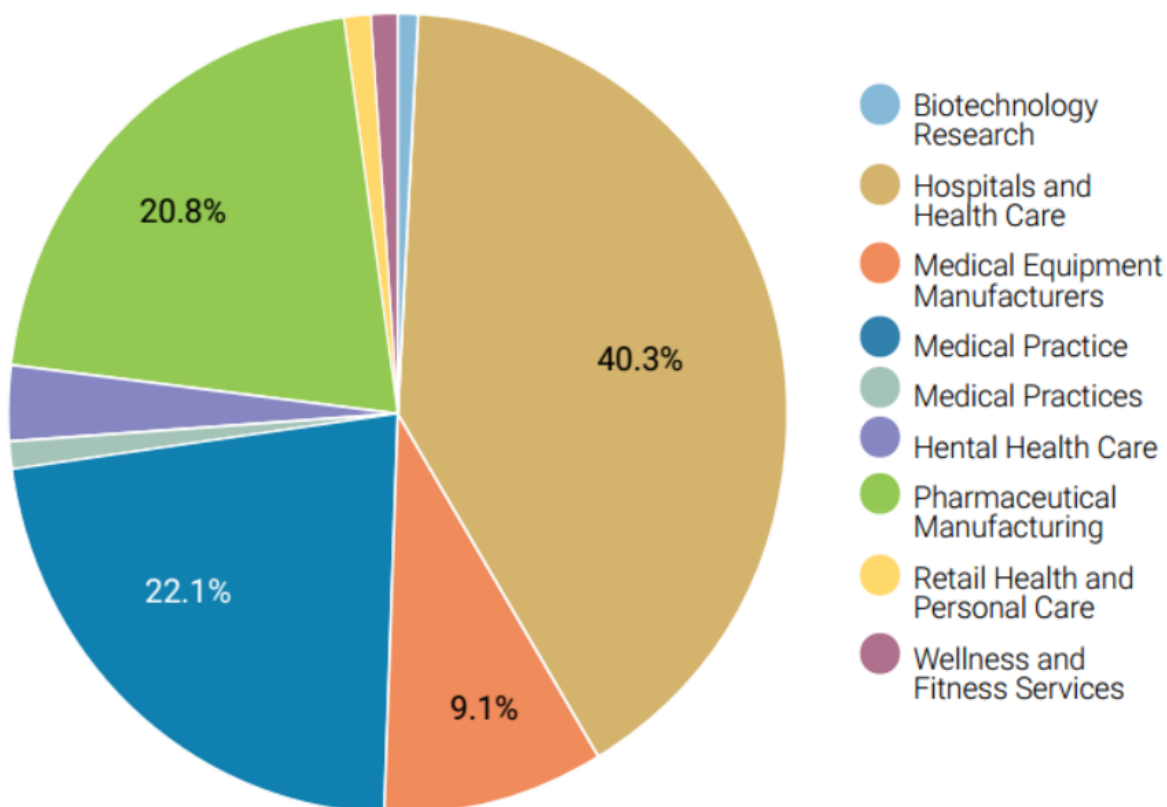
Même si ces chiffres peuvent paraître dérisoires comparé à ceux des Etats-Unis, il est nécessaire de noter que ces données concernent toutes les entreprises et institutions publiques du secteur de la santé. Le nombre d'entreprises privées et d'infrastructures publiques américaines étant plus élevé dans ce secteur, il est normal que l'écart soit aussi important. Aussi, le H-ISAC, largement composé d'entités américaines, pourrait induire un biais dans la perception de ces incidents.

Pour mieux appréhender la diversité des sous-secteurs de la santé, le diagramme suivant a



Top 4 Des Pays Les Plus Ciblés Par Des Cyberattaques Selon Le H Isac

été extrait du même rapport, montrant la répartition des cyberattaques par sous-domaines :



Représentation De La Répartition Des Secteurs Les Plus Ciblés Dans Le Domaine De La Santé

Aussi, pour comprendre pourquoi le secteur de la santé est particulièrement ciblé par les attaquants, il est crucial de se pencher sur les cybermenaces qui lui sont spécifique.

En combinant les informations issues de divers rapports provenant de l'ENISA (agence européenne chargée de la sécurité des réseaux et de l'information) et du H-ISAC concernant le paysage des menaces, les types de menaces suivants ont été identifiés :

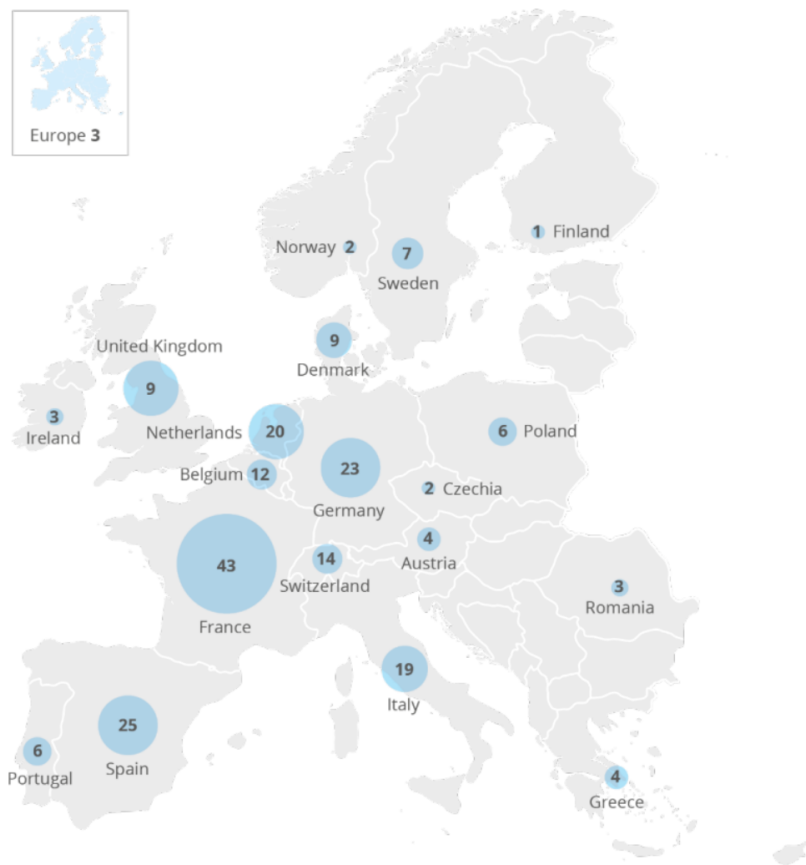
- Le ransomware

- Le cybercrime (notamment les activités des brokers)
- L'hacktivisme

Avant de détailler les activités et les motivations des différents types d'acteurs identifiés précédemment, il convient de se pencher sur la définition de leurs activités.

Les acteurs ransomware

Figure 2: Map of incidents observed (January 2021 to March 2023)



Cartes Des Incidents Ransomware Provenant Du Rapport Sur Le Secteur De La Santé De L'enisa

En 2023, du CHU de Rennes à celui de Brest en passant par celui de Saint-Renan, les attaques ransomware ciblant des hôpitaux ont fait les gros titres des journaux. Les différences entre les différentes attaques interrogent quant à la pluralité des modes opératoires et aux profils des acteurs à l'origine de ces attaques.

On distingue principalement deux types d'acteurs dans le domaine du ransomware : les services de de Ransomware as a Service (Raas), et les groupes de ransomware traditionnels. Bien que ces distinctions aient déjà été abordées dans différents rapports et bulletins de sécurité, il est à noter que la différence réside dans leurs organisations internes et l'intégration d'acteurs extérieurs, les affiliés, dans le cas du RaaS.

Les infrastructures de santé sont particulièrement vulnérables aux ransomwares, car elles opèrent des systèmes avec un mélange complexe d'informatique de bureau et d'équipements biomédicaux spécifiques. Ces systèmes étant intriqués, si l'on bloque un maillon de la chaîne en chiffrant une grande quantité de données, des vies peuvent être mises en danger.

Au-delà du chiffrement, les établissements de santé travaillent au quotidien avec des données sensibles relatives aux patients et au personnels. Si ces informations sont divulguées, elles peuvent permettre à un acteur malveillant d'obtenir de précieuses informations afin de mener des campagnes de piratages de grande ampleur. Par exemple, s'il est identifié qu'un grand nombre de patients utilisent le médicament donné et qu'un acteur possède leurs adresses emails, il est tout à fait imaginable de mettre en place des campagnes de phishing autour d'une fausse alerte relative à une campagne de rappel du médicament pour des raisons sanitaires.

Que ce soit par simple extorsion ou par double voire triple extorsion, la menace de la publication des données conjuguée à la sensibilité des systèmes rend les établissements de santé particulièrement vulnérables.

Les brokers

Le cybercrime va désigner toutes les activités malveillantes lucratives d'un point de vue cyber. Même si le ransomware fait partie du cybercrime, son modèle économique et son importance en font une entité importante que l'on peut traiter spécifiquement. Dans le contexte de cet article, nous réduirons le cybercrime aux activités des Initial Access Broker (IAB) et aux autres types de brokers de données personnels.

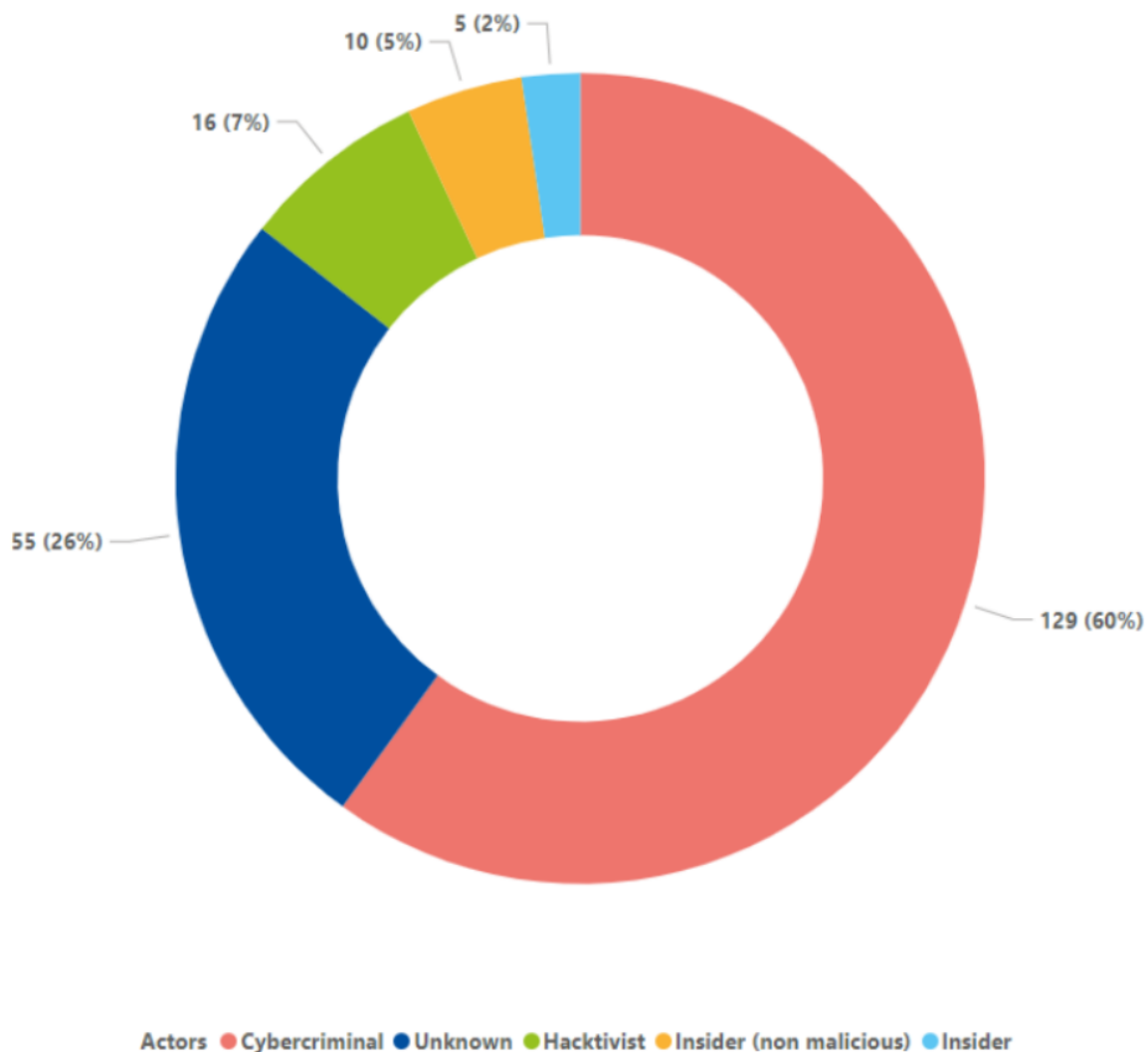
Un broker est un revendeur ou un intermédiaire entre un vendeur et un acheteur. Dans ce contexte, deux types de profils :

- Les revendeurs de données, dont l'objectif est de revendre des bases de données récupérées lors d'attaques. Certaines fois, ces bases de données sont simplement des fragments tirés d'autres bases de données plus conséquentes et achetées auparavant. Cette sphère du cybercrime n'est pas exempte de profiteurs qui tentent de revendre des bases de données open source. Ces derniers se font généralement bannir des forums/marketplace assez rapidement.
- Les revendeurs d'accès qui cherchent à vendre des accès de type rdp, vpn, ssh, ou autres, à des machines voire à des systèmes d'information complets. Ils jouent un rôle crucial dans le processus d'attaque en facilitant grandement les accès initiaux aux systèmes

Ces brokers peuvent parfois collaborer avec des groupes plus larges de ransomware, leur fournissant un accès aux données nécessaires pour mener leurs attaques.

Les hacktivistes

Les hacktivistes sont des cybercriminels avec des revendications particulières. De fait, ils ciblent rarement les hôpitaux, et autres infrastructures médicales, qu'elles soient publiques ou privées. Leur choix se tourne plutôt vers des ministères ou des entreprises pharmaceutiques. Ces acteurs représentent une frange minoritaire des acteurs malveillants, comme le montre le schéma suivant provenant du rapport de l'ENISA :



Répartition Des Acteurs Malveillants Ciblant Le Domaine De La Santé (enisa Threat Landscape)

Après avoir identifié les différents types d'acteurs, l'accent est désormais mis sur les cybercriminels. Les motivations complexes de ces derniers, par rapport à d'autres tels que les hacktiviste, restent à préciser.

L'appât du gain

Sur la base du rapport de l'ENISA, ainsi que de leurs observations, rapports de réponse aux incidents et surveillance constante des menaces, l'agence européenne a créé le graphique suivant :

Il est observé que l'aspect financier constitue l'une des principales motivations des cybercriminels. En complément de ces observations, des recherches ont été menées sur divers forums agissant comme des places de marché, dans le but d'estimer le prix de vente de ces données et l'intérêt qu'elles suscitent.

Dans cette première capture, les deux types de brokers précédemment mentionnés sont visibles. Certains acteurs proposent à la vente des données médicales, en l'occurrence il s'agit ici des données d'une clinique de chirurgie plastique. D'autres offrent des accès à des SI d'entreprises ou de centres médicaux. Les prix varient grandement en fonction des données, des cibles et de leur localisation. Dans la capture d'écran précédente, les données marchandées émanant d'entreprise européennes et américaine sont les plus onéreuses.

Cependant et dans de rare cas, il est possible de trouver des annonces qui regroupent base de données et accès, comme le montre cette deuxième capture :

Bien que ces transactions soient opérées sur des forums et que la modération de ces derniers n'influe pas sur les fils de discussion, ce n'est pas le cas de tous les sujets relatifs au domaine de la santé.

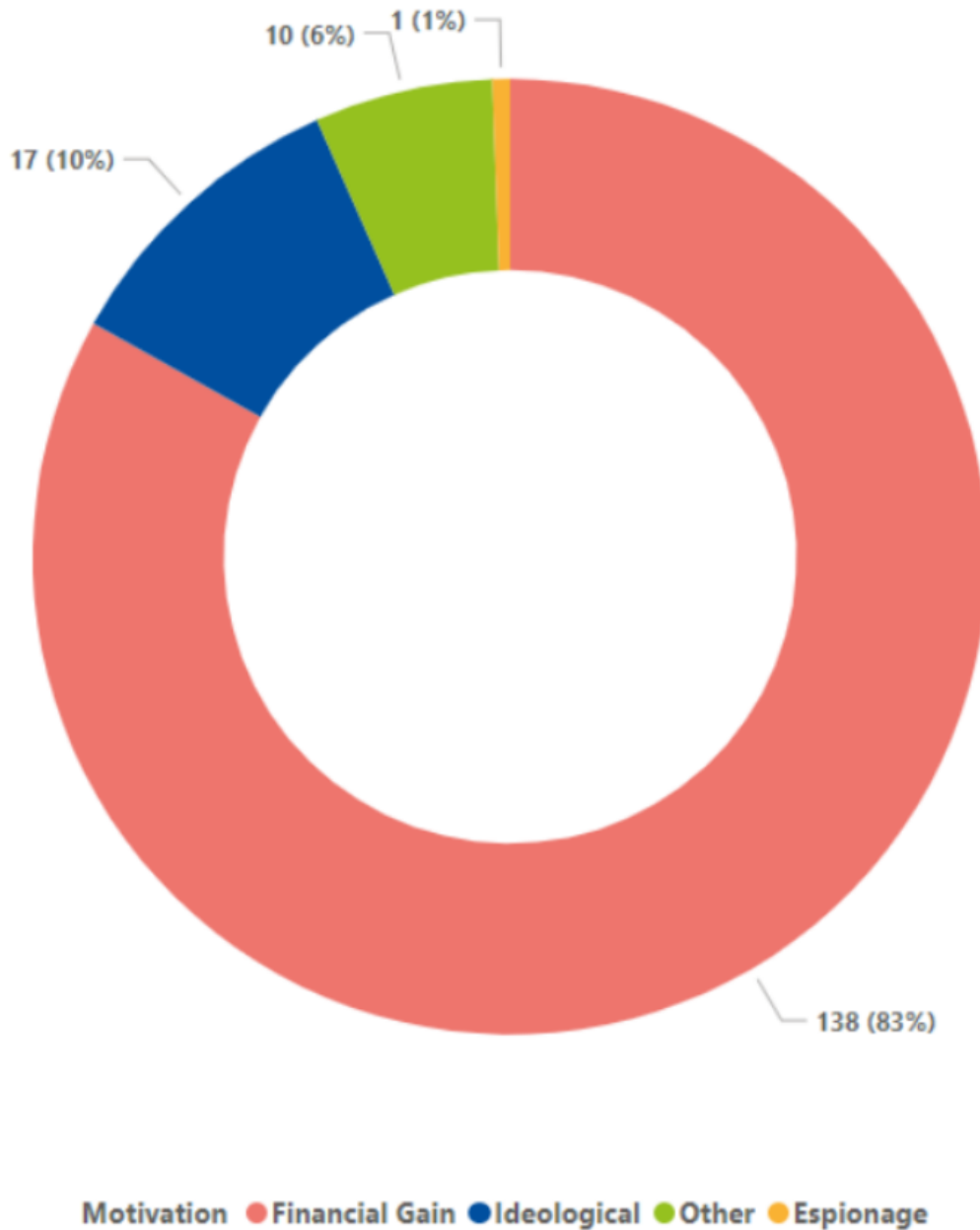
Dans le post suivant, une personne ayant fait une compromission demande l'avis d'un forum pour connaître les potentiels étapes qu'il pourrait réaliser dans la suite de son attaque.

Les réactions à ce post sont diverses, certains désavouant totalement la démarche et invitant l'auteur à faire preuve d'empathie pour les victimes potentielles, d'autres demandant simplement davantage d'informations.

La plupart du temps, les administrateurs clôturent rapidement ces sujets pour éviter tout débordement pouvant attirer l'attention sur le forum et ses utilisateurs.

Au-delà de l'aspect éthique posé par le ciblage d'établissements de santé, c'est l'informatique de gestion qui est généralement visé par les attaques.

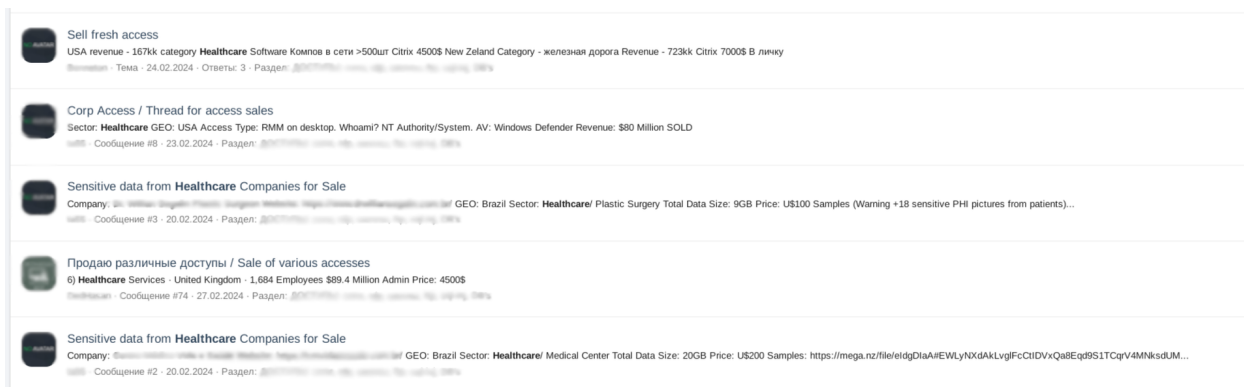
Aucune discussion spécifique n'a, en effet, été observée concernant des protocoles



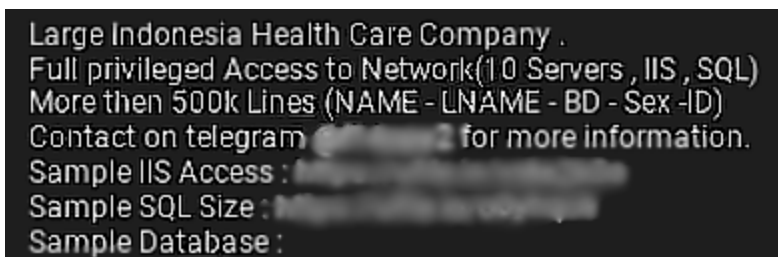
Threat Landscape De L'enisa, Motivations Des Acteurs Malveillants Ciblant Le Domaine De La Santé

médicaux particuliers comme le HL7 ou le Dicom, utilisés dans l'imagerie médicale, ce qui peut amener à s'interroger sur l'expertise techniques des attaquants.

Bien que l'imagerie médicale ne soit pas immédiatement associée à une source de données personnelles à laquelle on pense, les serveurs de stockage des résultats de scanner et autres contiennent un bon nombre d'informations qui seraient exploitable. Par exemple, les fichiers Dicom, s'ils ne sont pas anonymisé contiennent un nombre considérable d'informations sensibles sur les patients qui, une fois extrait, peuvent se revendre à prix d'or.



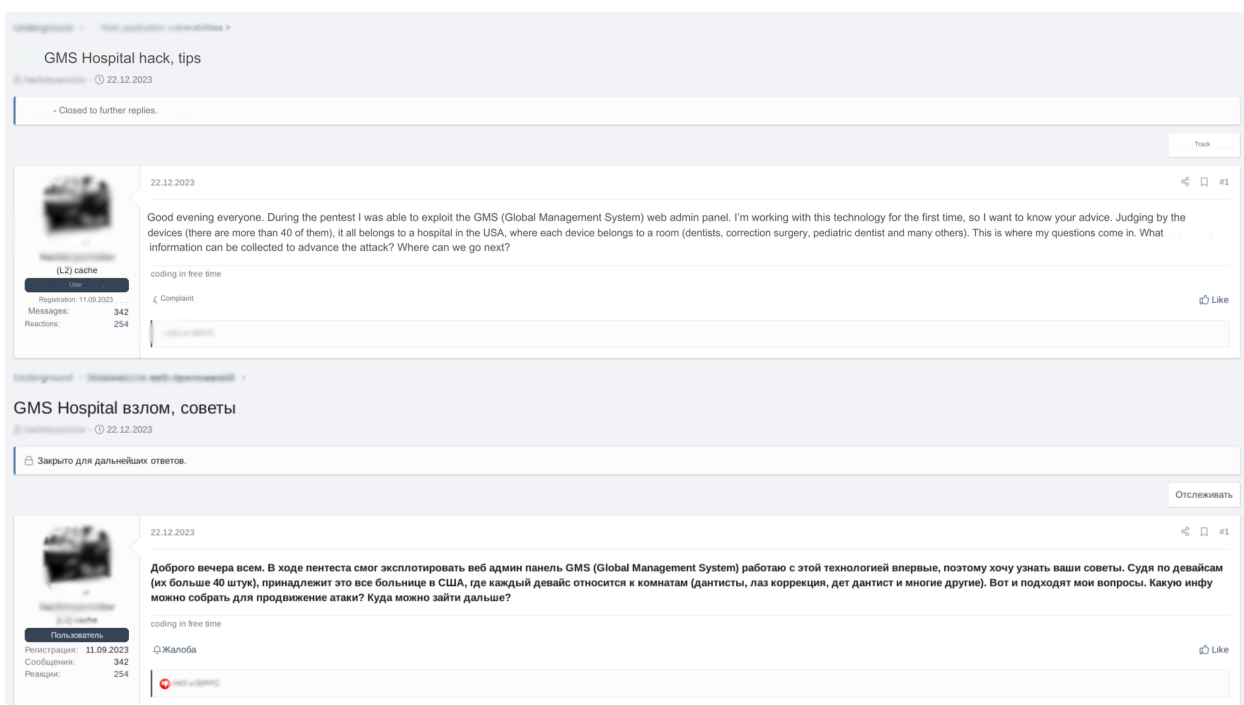
Capture D'écran D'annonce De Vente De Données Médicale Sur Le Darknet



Dans un autre registre, la suppression ou la modification de ces fichiers par des cybercriminels peuvent impacter le bon fonctionnement des infrastructures.

Capture D'écran D'annonce De Vente De Données Médicale

L'imagerie médicale et les



Capture D'écran D'un Post Demandant De L'aide Dans Le Cadre D'une Une Action Offensive Contre Un établissement De Santé

protocoles spécifiques aux appareils biomédicaux sont des domaines qui mériterait une attention plus approfondie dans de futurs articles, étant donné leur importance et le manque de connaissances à son sujet.

I don't think that the point is in his specifics about dentists and "laser corrections", if his further question is to collect information for attack and further advancement. In general, we are talking about a medical institution, and this means the health and lives of people. The foundations of our community's work are built on simple principles and straightforward logic. After all, you can also try to parse a manifesto about working in RU. Recently I read a comment in TG, where someone was sincerely surprised, "Well, he wanted to buy a database of grannies' numbers, and you are all white and fluffy, when are you buying up logs for mining?" Like, what is the difference between the villains who terrorize pensioners and those who terrorize foreign cryptans. I will not comment on this statement or impose my opinion, since everyone perceives this to the best of their conscience and upbringing. The same applies to medical institutions. I think that by default, this should be cut off at the genetic level, or stopped at the administrative level. There is not even any talk about morality. Well, damn there should be simple human concepts. What if the villain got into the honey, where, God forbid, your loved one/relative/mother was? It doesn't matter whether it's dentistry or intensive care. There is a risk of harm to human health.

The author of that closed topic should leave the forum with pissing rags, and don't just close the topic.

Не думаю, что суть в его конкретике о дантистах и "лаз коррекция", если дальше его вопрос заключается в сборе инфы для атаки и дальнейшего продвижения. В общем и целом речь идёт о медицинском учреждении, а это здоровье и жизни людей. На простых принципах и прямой логике построены основы работы нашего комьюнити. Ведь так же можно пытаться разобрать манифест о работе по ру. Недавно читал комментарий в TG, где некто искренне удивлялся "ну хотел он купить базу номеров бабулек, а вы все беленькие и пушистые, когда логи скупаете на отработку?". Мол чем отличаются злодеи, кто кошмарит пенсионеров, от тех кто кошмарит забугор криптанов. Я не буду комментировать это высказывание или навязывать свое мнение, поскольку каждый подобное воспринимает в меру своей совести и воспитания. Так же обстоит дело о мед учреждениях. Считаю, что по дефолту такое должно отсекается на генетическом уровне, либо пресекаться на административном. О моральном даже речи не идёт. Ну блить простые людские понятия же должны быть. А если бы злодей проник в мед, где, не дай бог, был твой близкий/родственник/мать? Не важно, стоматология это или реанимация. Есть риск нанести вред здоровью людей.

Автора того закрытого топика ссаными тряпками прочь с форума, а не просто закрывать тему.

Réaction Au Post Précédent Demandant De L'aide Concernant Une Action Offensive Contre Un établissement De Santé

L'approche systématique et problématique des acteurs ransomware

Lorsqu'on aborde les sujets liés aux fuites d'informations, il est impossible de ne pas évoquer les ransomwares. Même si les données de santé sont marchandées à prix d'or sur les forums, la plupart des groupes ransomware ne revendent pas ces données et les publient en libre-accès si la rançon n'a pas été payée.

Le fait de divulguer gratuitement les informations des victimes au lieu de les monétiser peut sembler illogique. Il s'explique par le fait que le processus de publication des acteurs ransomware est normé et les données de santé n'ont pas de traitement spécifique dans les processus de double extorsion lancés à grande échelle.

En effet, pour que le principe de chantage fonctionne, l'effacement des données contre une rançon, il faut que l'acteur publie systématiquement les données dès lors que le temps de paiement imparti est dépassé. Ce processus étant appliqué à toutes les cibles sans distinction, même si les données ont une valeur importante à la revente, elles seront publiées et accessibles de tous.

Dès lors, il est légitime de se demander si certains attaquants ont décidé d'aller plus loin que le chiffrement et l'exfiltration de ces données en adoptant une stratégie « verticale » différenciée pour les établissements de santé

Prenons l'exemple du CHU de Rennes. Le site vitrine du groupe BianLian, à poster l'annonce de rançon suivante :

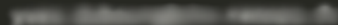

Outre les informations des données récupéré, e montant estimatif des revenus fournis par le groupe est important pour les threat actors.

Le CHU de Rennes est un hôpital public possédant plusieurs sites, mais il est loin de réaliser un bénéfice. En examinant, le rapport de la Cour des comptes sur les résultats financiers des hôpitaux, on peut constater que les infrastructures de santé publiques sont généralement en déficits :

Chu De Rennes

<https://chu-rennes.fr>

Chu de Rennes offers a wide range of clinical services that include rehabilitation, neurosurgery, obstetrics, pediatrics, and elderly care.

Contact Email: 
Phone Number: 

Revenue: \$8 Millions

Data Volume: 300 Gb

Data description:

- * HR.
- * Accounting.
- * Financial data.
- * Personal data.
- * Technical documents.

Announce Sur Le Site Vitrine De Bianlian Au Sujet Du Chu De Rennes

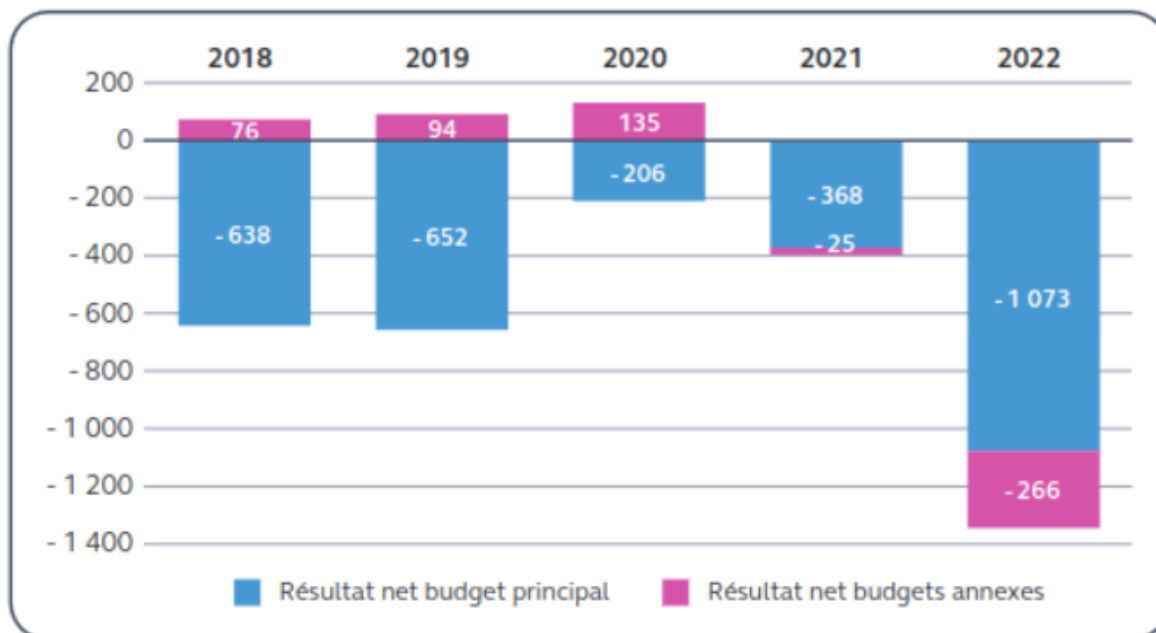
Pour estimer le chiffre d'affaires global d'un établissement de santé, il serait nécessaire de considérer l'ensemble du système public derrière les CHU, ce qui n'est clairement pas faisable par le groupe d'attaquants.

Ainsi, nous pouvons remettre en question la pertinence de ce chiffre. Ce revenu est calculé en fonction des données financières accessibles au groupe, lui permettant finalement de fixer le montant de la rançon. Cette approche pourrait être efficace pour une entreprise privée. Par exemple, récemment, la société de santé Optum a versé 22 millions de dollars au groupe AlphaV pour éviter la divulgation de données de santé.

Toutefois, dans notre cas, la rançon serait calculée sur la base de chiffres disproportionnés. Cela illustre parfaitement l'hypothèse que certains groupes cybercriminels n'ont aucune idée des infrastructures qu'ils ciblent. Ils semblent agir par pur opportunisme, sans vraiment mesurer les conséquences de leurs actes ou la valeur réelle des données exfiltrées.

Nous ne pouvons pas confirmer si les données ont été effectivement divulguées ou si un accord a été conclu entre le groupe et le CHU pour éviter cela. Parfois, après des négociations, certains groupes acceptent de fournir les clés de déchiffrement sans demander de rançon, ou choisissent d'eux même de ne pas divulguer les données, mais cela reste rare.

Résultats nets des hôpitaux publics de 2018 à 2022* (en M€)



* Y compris produits issus des dons d'équipements de protection individuelle pour 300 M€ en 2020 et 20 M€ en 2021

Source : Cour des comptes à partir de la base de données de la DGFIP

Résultat Des Résultats Nets Des Hôpitaux Publics Par La Cour Des Comptes

Conclusion

Au travers les informations exposées dans cet article, une mise en lumière a été faite sur les menaces pesant sur le milieu de la santé. L'étude des cas spécifiques de cybercriminels revendant des données, ou agissant au cœur d'opération ransomware afin d'extorquer leurs victimes, a été privilégiée.

Au-delà de ce volet lucratif, il a été constaté que d'autres acteurs utilisent des personnes à l'intérieur d'hôpitaux, ou se font passer pour des médecins pour réaliser des opérations malveillantes. Le contexte difficile dans lequel se trouvent ces infrastructures accroît considérablement le risque d'attaque par ingénierie sociale.

Nous n'avons pas non plus évoqué la possibilité d'actions malveillantes réalisées par des acteurs étatiques. En effet, ces derniers pourraient, par exemple, compromettre des appareils biomédicaux. Ces actions ciblées, mises en place à des fins de déstabilisation, pourraient avoir un impact important sur les patients visés. Qu'ils soient citoyens ou présidents, n'importe qui pourrait devenir une victime.

Nous pourrions aussi parler d'acteurs étatiques, qui à des fins de déstabilisations, pourraient collecter des données ou perturber le bon fonctionnement d'un établissement ciblant une personne clé ayant besoin de soin.

Malheureusement, il reste difficile de jauger précisément les capacités opérationnelles requises pour réaliser de telles attaques en raison d'un manque de données.