KELA DATASHEET

金融業界を狙う

サイバー犯罪の脅威

2023年、医療業界はサイバー犯罪者が特に狙う標的となりました。一部のサイバー犯罪者は医療業界を標的から除外しているものの、病院や診療所、メンタルヘルス関連組織、製薬会社をはじめ、多数の医療関連組織はサイバー攻撃に対して脆弱な状態にあります。また医療業界で扱われるデータは、他の業界とは異なるリスクを抱えています。例えば、氏名や電子メールアドレス、社会保障番号、財務情報などの個人情報については、他の業界でも侵害が発生する可能性があります。しかし医療業界でデータ侵害が発生した場合は、より機密性の高いデータ（検診報告書や、診療目的で撮影した身体の画像、医療スキャン、心理アセスメント、その他極めて個人的な情報など）に不正アクセスされる可能性があります。また重要性が高い業務や、人命にかかわる業務がサイバー攻撃によって中断の危機にさらされることもあります。

医療機関で発生するインシデントには、サイバー犯罪者から直接の標的として攻撃されるパターンと、普段からビジネスパートナーとして利用しているサードパーティが攻撃され、その二次被害に遭うパターンがあります。最近では、シェアードサービスを提供するIT企業が攻撃を受けたことにより、カナダにある5つの病院で日々の業務に支障が生じた事例もありました。

2023年の終わりを迎えるにあたり、KELAはランサムウェア攻撃やネットワークアクセスの販売、データ侵害、ハクティビストグループの攻撃など、昨年から医療業界を標的にしている持続的脅威について詳細な調査を行いました。

ランサムウェア攻撃

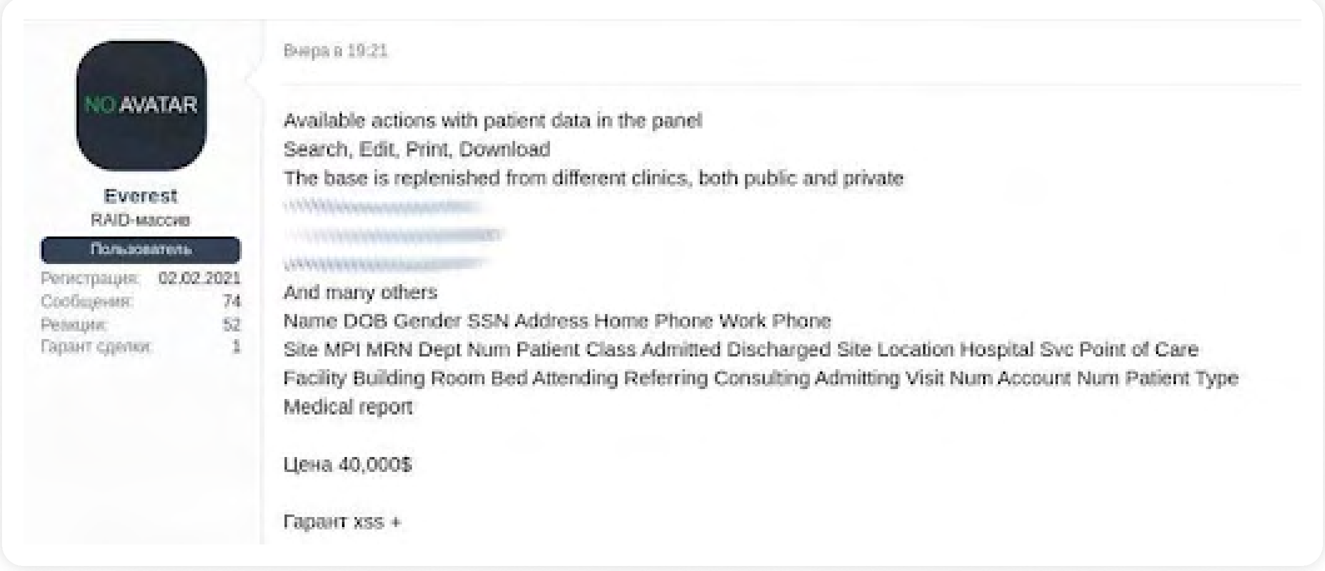
医療機関がランサムウェア攻撃を受けた事例では、検査結果や電子化された医療記録が閲覧不可能となったり（事例1、2）、治療が遅れたり、患者を他の病院へ搬送する事態を余儀なくされるなどの様々な事態に発展しました。また地方の小規模な病院がランサムウェア攻撃を受けた事例では、その後病院が永久的な閉鎖に追い込まれたものもありました。

サイバー犯罪者は、医療機関が治療の中断を避ける目的で交渉に応じたり、身代金を支払う可能性があると認識しています。そのため、医療機関が直面しているランサムウェア攻撃のリスクは甚大と言えます。KELAが調査を行った結果、ランサムウェア攻撃やデータリーク攻撃を実行するアクターは継続的に医療業界を標的としていること、そして同業界における2021年以降の被害組織数は800を超えることが判明しました。さらに2023年においては、ランサムウェア攻撃を受けた医療業界組織は400超に上り、「標的にされた業界」の3位にランクインしています。医療業界の被害組織を国別にみると、「標的にされた国」の1位は米国であり、2023年に同業界で発生したランサムウェア攻撃の約68%を占めました（また米国は、全ての業界において「標的にされた国」の1位となっています）。医療業界を標的にしたランサムウェア攻撃を犯行グループ別に分類すると、1位は「LockBit」、2位は「Clop」、3位は「Alphv」、4位は「BianLian」となり、この4グループが2023年に同業界で発生したランサムウェア攻撃の約45%を実行していたことが判明しました（4位のBianLianは、攻撃件数で毎回上位にランクインしているグループではありません。しかし今年、同グループは2つの業界を集中的に攻撃しており、医療業界はそのうちの1つとなっています）。

ネットワークアクセスの販売

初期アクセスブローカーは、ランサムウェアグループが侵害するネットワークのアクセスを提供しており、ランサムウェア・アズ・ア・サービス（RaaS）のサプライチェーンにおいて重要な役割を果たしています。KELAが調査したところ、2023年に売り出された医療業界のネットワークアクセスは85件超となりました。そしてそれらのアクセスを国別に分類した結果、初期アクセスブローカーが主に標的とした国は米国であり、全アクセスの半分以上が同国のものであることが判明しました。

売り出されていた医療業界のネットワークアクセスには、公的機関や政府組織、民間企業や病院のものが含まれており、脅威アクターに悪用された場合は、患者のデータを検索されたり、編集される可能性があります。



Everest
RAID-массив
Пользователь
Регистрация: 02.02.2021
Сообщения: 74
Реакции: 52
Гарант сделки: 1

Вчера в 19:21

Available actions with patient data in the panel
Search, Edit, Print, Download
The base is replenished from different clinics, both public and private

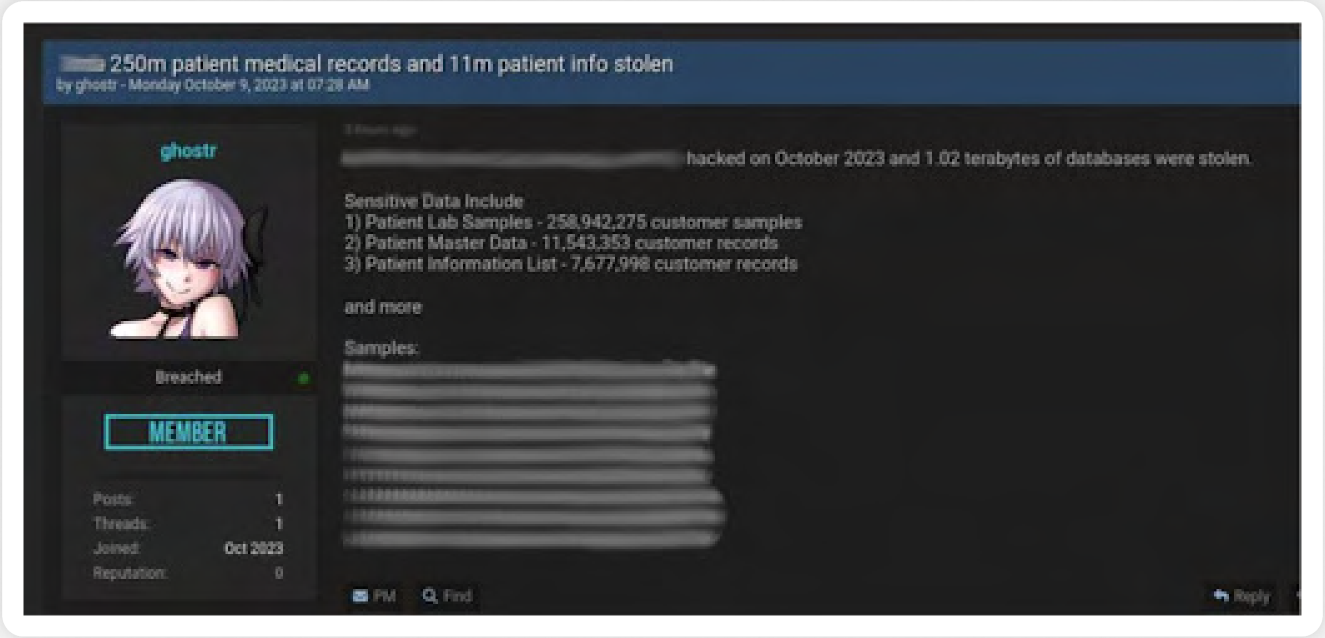
And many others
Name DOB Gender SSN Address Home Phone Work Phone
Site MPI MRN Dept Num Patient Class Admitted Discharged Site Location Hospital Svc Point of Care
Facility Building Room Bed Attending Referring Consulting Admitting Visit Num Account Num Patient Type
Medical report

Цена 40,000$

Гарант xss +

データリーク

医療業界の組織が保有している機密データには、脅威アクターにとって非常に有益な情報も含まれており、スピアフィッシングをはじめとするフィッシング攻撃や、ソーシャルエンジニアリングなどに悪用される可能性があります。また、個人データを窃取された患者を恐喝するといったデータリーク攻撃を実行される可能性もあります。アンダーグラウンドでサイバー犯罪者が交わしているやり取りからは、医療関連データの需給が相当な量に上ることがうかがえ、またKELAの調査でも、脅威アクターが医療機関から窃取した個人識別情報（PII）や個人の医療関連情報などを無料で公開したり、売りに出していることを確認しています。それら情報の具体的な例としては、氏名や性別、年齢、住所、検診結果、患者の検査用サンプル、薬局関連データ、クレジットカードのフルデータ、電子メールアドレスと平文パスワードのセットなどが挙げられます。



250m patient medical records and 11m patient info stolen
by ghostr - Monday October 9, 2023 at 07:28 AM

ghostr
Breached
MEMBER
Posts: 1
Threads: 1
Joined: Oct 2023
Reputation: 0

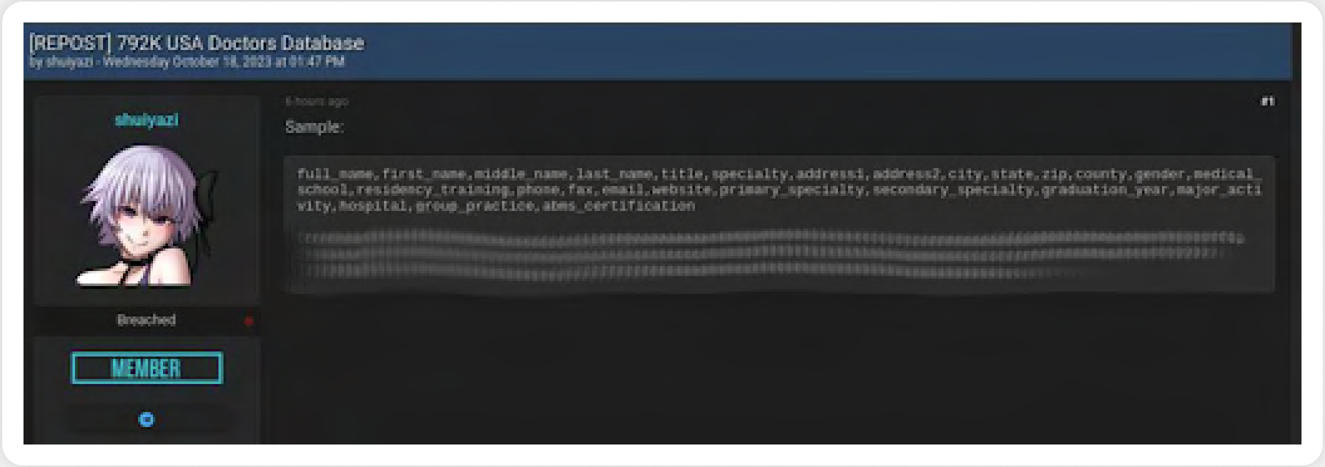
hacked on October 2023 and 1.02 terabytes of databases were stolen.

Sensitive Data Include
1) Patient Lab Samples - 258,942,275 customer samples
2) Patient Master Data - 11,543,353 customer records
3) Patient Information List - 7,677,998 customer records

and more

Samples:

脅威アクターは、患者のみならず医師のデータもリークしています。例えば某サイバー犯罪フォーラムでは、医師の専門分野や出身校、勤務先病院、米国専門医認定機構（ABMS）による認定、個人情報（氏名や住所、電話番号、電子メールアドレスなど）をはじめ、様々な情報を含むとされるデータベースが投稿されていました（下図参照）。



[REPOST] 792K USA Doctors Database
by shuiyazi - Wednesday October 18, 2023 at 01:47 PM

shuiyazi
Breached
MEMBER

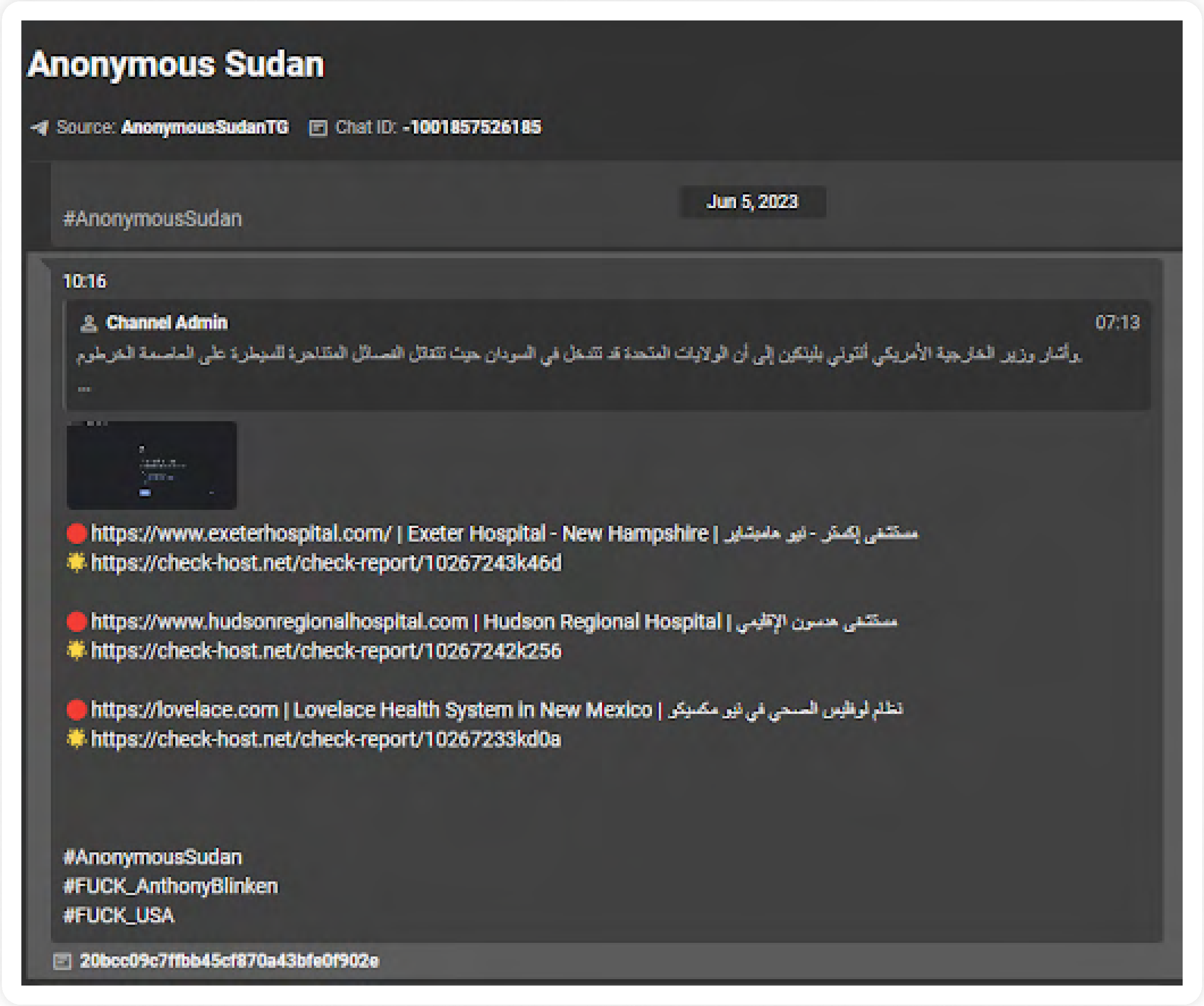
6 hours ago
#1
Sample:

```
full_name,first_name,middle_name,last_name,title,specialty,address1,address2,city,state,zip,county,gender,medical_
school,residency_training,phone,fax,email,website,primary_specialty,secondary_specialty,graduation_year,major_acti
vity,hospital,group_practice,abms_certification
```

DDOS攻撃とハクティビズム

DDoS攻撃も、医療業界を脅かす深刻な脅威となっています。DDoS攻撃で想定される被害としては、オンラインで提供しているサービスが中断されることにより、甚大な経済的損失が生じたり、評判や信用が失墜することなどが挙げられます。DDoS攻撃の実行犯は、金銭を動機とする脅威アクターの場合もあれば、思想的な動機をもとに特定の国や企業を攻撃するハクティビスト（例えばイスラエル対ハマスや、ロシア対ウクライナの紛争に関与しているハクティビストグループなど）の場合もあります。

2023年10月7日から始まったイスラエル対ハマスの紛争では、イスラエルにある病院（ShebaMedical Center、RambamHospital、HerzogMedical）のウェブサイトがDDoS攻撃の標的となりました。また、現在も続いているロシア対ウクライナの紛争では、「AnonymousRussia」や「AnonymousSudan」をはじめとする親ロシア派のハッカーグループが、ウクライナを支援する国々の機関を標的とした攻撃を指揮しており、米国では多数の病院のウェブサイトが彼らの標的となりました。



Anonymous Sudan
Source: AnonymousSudanTG
Chat ID: -1001857526185

#AnonymousSudan
Jun 5, 2023

10:16
Channel Admin
07:13
وأشار وزير الخارجية الأمريكي أنتوني بلينكن إلى أن الولايات المتحدة قد تتدخل في السودان حيث تتقاتل الفصائل المتناحرة للسيطرة على العاصمة الخرطوم
...

🔴 https://www.exeterhospital.com/ | Exeter Hospital - New Hampshire | مستشفى إكستر - نيو هامبشاير
https://check-host.net/check-report/10267243k46d

🔴 https://www.hudsonregionalhospital.com | Hudson Regional Hospital | مستشفى هدسون الإقليمي
https://check-host.net/check-report/10267242k256

🔴 https://lovelace.com | Lovelace Health System in New Mexico | نظام لوفليس الصحي في نيو مكسيكو
https://check-host.net/check-report/10267233kd0a

#AnonymousSudan
#FUCK_AnthonyBlinken
#FUCK_USA

20bcc09c7ffbb45cf870a43bfe0f902e

KELAのプラットフォームで表示した投稿のスクリーンショット

推奨される対策＆リスク緩和策

セキュリティ研修：職員を対象に、サイバーセキュリティの基本（フィッシングメールの見分け方や安全性の高いパスワードの作成・管理方法、オンラインで機器や情報を安全に使用する方法など）について学ぶ研修を実施します。

定期的なバックアップ：重要なデータやシステムのバックアップを定期的に取り、オフライン環境で適切に保存して、ランサムウェア攻撃による影響を緩和します。

多要素認証（MFA）：追加のセキュリティ対策として、機密性の高いデータやシステムへのアクセスに多要素認証を実装します。これにより、脅威アクターが不正入手した資格情報を悪用することが困難になります。

インシデント対応計画：医療業界に即した包括的なインシデント対応計画を策定・更新し、定期的に演習を実施して準備体制を確認します。

セキュリティ監査・評価：第三者の専門家によるセキュリティ監査および評価を定期的に実施し、客観的な評価と脆弱性の特定を行います。

協力体制と情報共有：他の医療機関と協力体制を構築して脅威インテリジェンスを共有し、医療業界に特化したサイバー脅威インテリジェンスコミュニティに参加します。

エンドポイントの保護：ウィルス対策やEDR、行動分析などの機能を有する高度なエンドポイント保護ソリューションを導入し、マルウェアに対する防御を強化します。

サイバー犯罪ソースの監視：サイバー犯罪ソースを監視し、データベースのダンプやアカウント情報、ランサムウェア攻撃に関する投稿、サイバー犯罪の傾向などに関する情報を入手します。

KELA

www.kelacyber.com • marketing@ke-la.com • +972-3-970-2720

Copyright© 2024 KELA