レポート

病院が危ない

医療機関を狙うサイバー攻撃

intel Security

目次

執筆者:

Advanced Programs Group
Christiaan Beek
Charles McFarland
Raj Samani

はじめに

医療データは簡単に価値を失うものではありません。医療記録でも新薬の知的財産でも、犯罪者の手に渡ってしまえば、そう簡単に取り戻すことはできません。医療データはなぜ盗まれるのでしょうか。それ自体が目的なのか、他の攻撃で利用するためなのか。データ自体が狙いであれば、データに対する需要があり、盗み出す価値があるのでしょう。全体像はどうなっているのでしょうか。

このレポートでは、医療業界で発生しているデータ侵害について解説します。特に、医療データが売買されているマーケットとその動機について詳しく見ていきます。

McAfee Labsのレポート『目に見えないデータの経済性』では、金融関連のデータ、特に決済カード情報のデータ侵害について解説しました。このレポートの執筆時点では、医療データの売買は確認できませんでした。医療データが盗まれていることは把握していましたが、闇市場で発見できませんでした。このレポートでは、その後の調査で判明したことを報告します。

— Raj Samani、Intel Security EMEA担当CTO

@Raj_Samani
@McAfee_Labs

普通の場所が一番目立たない

『目に見えないデータの経済性』で解説しているように、盗まれたデータを扱うマーケットが存在し、売り買いが盛んに行われています。侵害を受ける組織は後を絶たず、盗まれるデータの量も増加しています。その反面、売買されるデータの価格は急落し、いつ底を打つのか見えない状態です。しかし、盗まれた決済カードのデータ量を見ると、買い手を惹きつける魅力的なビジネス モデルであることに変わりはありません。

販売されているデータを調べたところ、不思議なことに、この宝庫の中に医療データは含まれていませんでした。特に意識して探したわけではありませんが、盗まれている事実を把握していただけに、この結果は意外なものでした。このレポートを作成した理由はこの点にあります。

医療データを売買しているサイトが存在することは想定していましたが、今回は単にスクリーンショットを提示するだけでなく、もう少し深く掘り下げた調査を行い、医療業界で攻撃を受けている組織の種類（たとえば、製薬会社など）も調査しました。

2月に「医療分野をターゲットにするランサムウェア」という記事をブログに掲載し、米国の病院を狙うランサムウェアについて紹介しました。最近のランサムウェアは、以前のような不特定多数ではなく、特定の組織を狙って攻撃を行っています。病院も例外ではありません。今回のレポートでは、盗まれた医療データの売買を採り上げていますが、医療分野に対する攻撃はこれに限ったものではありません。

詳しい調査結果を報告する前に、明確にしておかなければならないことがあります。このレポートは、不安感を煽ることを意図したものではありません。このレポートの目的は、医療業界の組織が適切な対策を実施できるように、現在の脅威状況を説明することにあります。クレジットカードが盗まれた場合と異なり、医療記録を簡単に変更することはできません。この点が医療記録の価値を高めています。医療データが侵害された後では、その影響を軽減することは不可能です。攻撃を受ける前に、あらゆる手段を講じてリスクを排除する必要があります。その最初のステップが、脅威を正しく把握することです。

盗まれた医療データが売られている

まず最初に確認すべきことは、盗まれた医療データが実際に売買されているのかどうか、という点です。前回の調査で見つからなかったのは、調査した場所に問題があった可能性があります。この推測どおり、盗まれた医療データを大量に販売するダークウェブがすぐに見つかりました。この中には、広く宣伝しているサイトもありました。図1は、397,000人分の医療データを販売しているデータベースです。図2は、このデータベースで販売されているデータの詳細です。

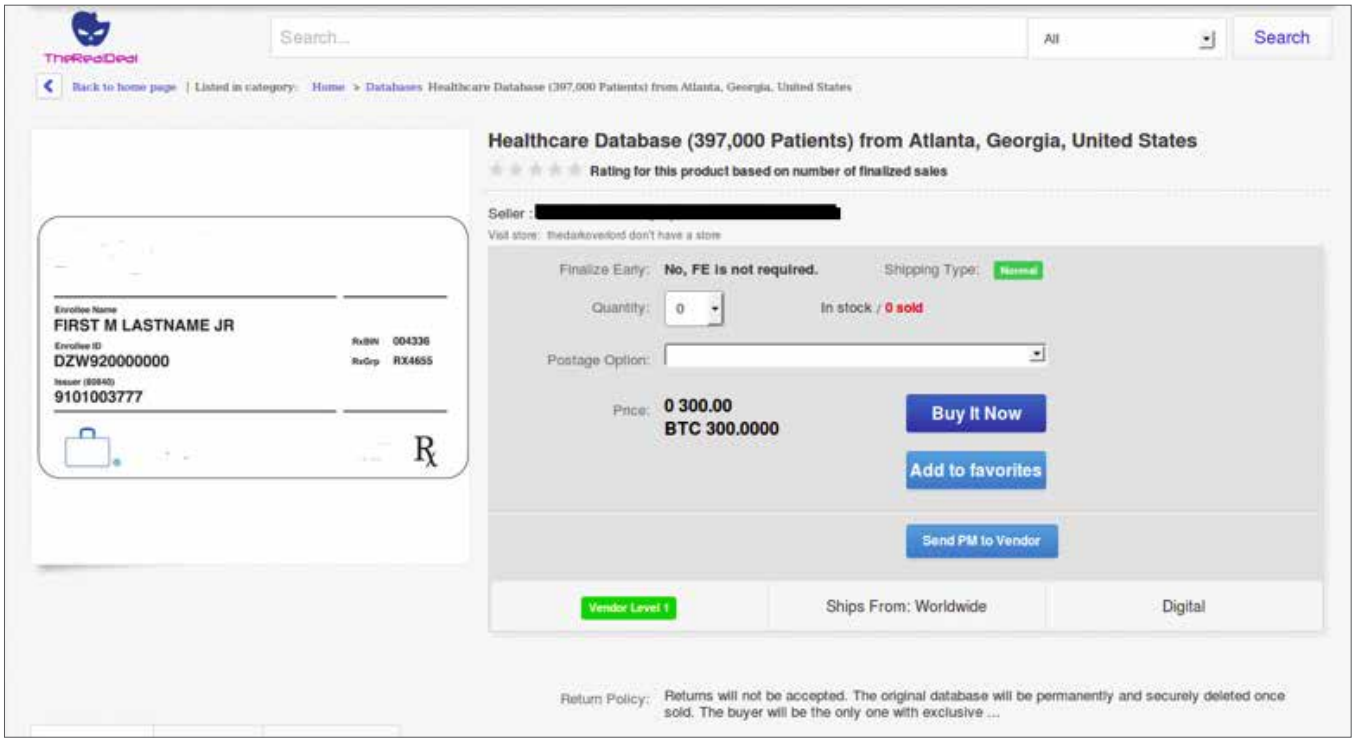


図1: 販売に使用されている医療データのデータベース

図2: 医療データの内容

これを見ると、患者の氏名や住所だけでなく、患者が契約している保険会社のデータなど、買い手の興味を惹きつけるデータも含まれています。価格を見ると、他のデータダンプに比べると、かなり高めに設定されています（詳細は後述）。

調査するデータの量に不足はありません。図3のサイトでは、ミズーリ州ファーミントンにある病院から盗まれた医療データが販売されています。このデータは、図1や図2で示した人物と同じ販売者が提供しています。

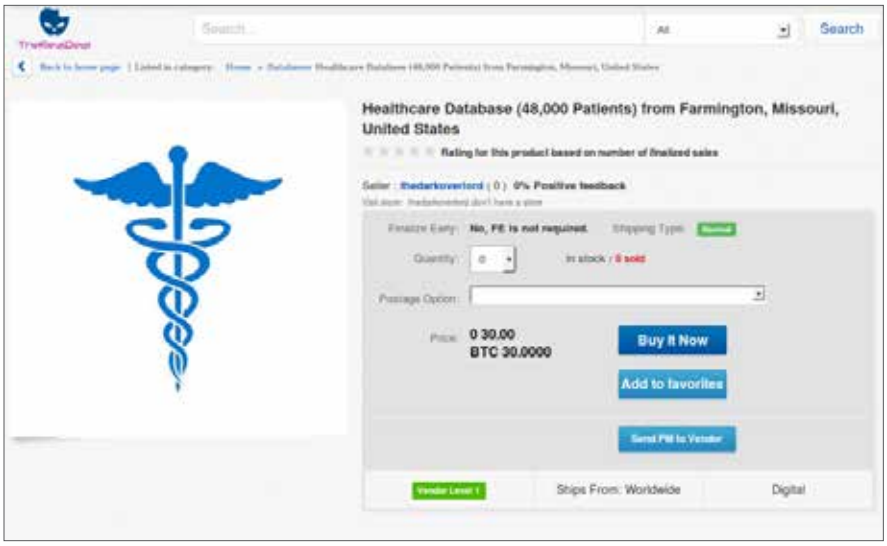


図3: 2つ目のデータベース

この販売者はさらに3つ目のデータベースを公開しています。このデータベースでは、別の病院から盗まれたデータが販売されています（図4）。

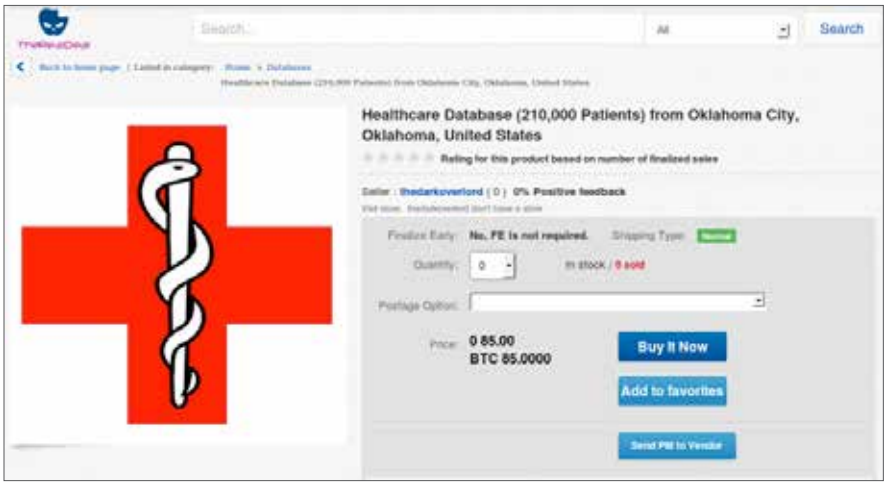


図4: 3つ目のデータベース

データが実際に販売されていることを示す必要はないと感じるかもしれませんが、これは販売者が侵害された組織にアクセスした証拠となります。図5のスクリーンショットは、Deepdotweb.comから大量に入手した画像の一つです。

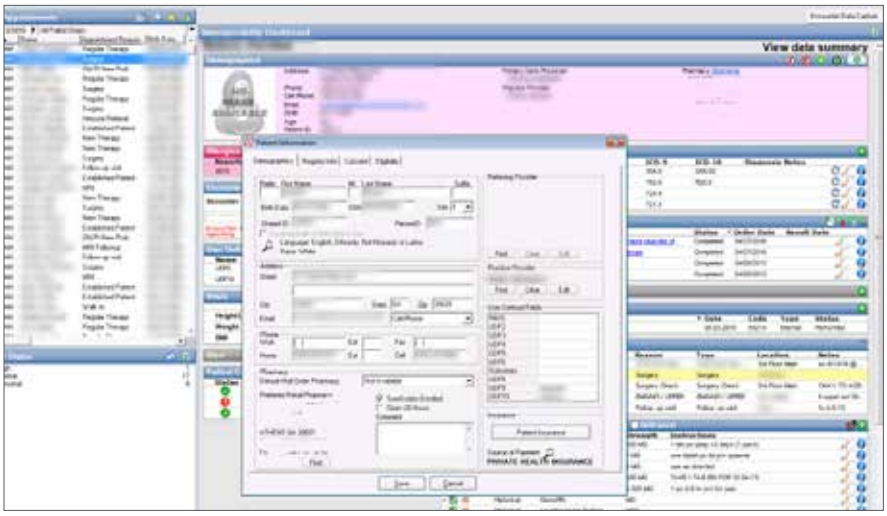


図5: 医療機関から盗まれたデータ

この販売者は、リモート デスクトップ プロトコルの脆弱性を悪用してこれらの組織に侵入したようです。

医療データの窃盗は攻撃の一部に過ぎません。ハリウッド映画でキーボードを叩きながらハッキングしているシーンが出てきますが、実際はそれほど簡単なものではなく、侵入するまでには多くの時間と労力が必要になります。サイバー犯罪者は費用対効果も常に考えています。この販売者の場合、時間やツールへの投資に見合うだけの利益を得られたのでしょう。この販売者とMotherboardのインタビューによると、この販売者は、時間に見合う十分な報酬を得ているようで、「ある保険会社のデータをすべて買った人物もいて、$100,000ほど儲けた」と話しています。

この話から2つのことが分かります。一つは、盗まれた医療記録が販売されていること、もう一つは、このようなデータに対する需要が確実にあることです。この結論は、この販売者の話だけを基にしているわけではありませんが、これ以上の証拠を探す必要はないでしょう。

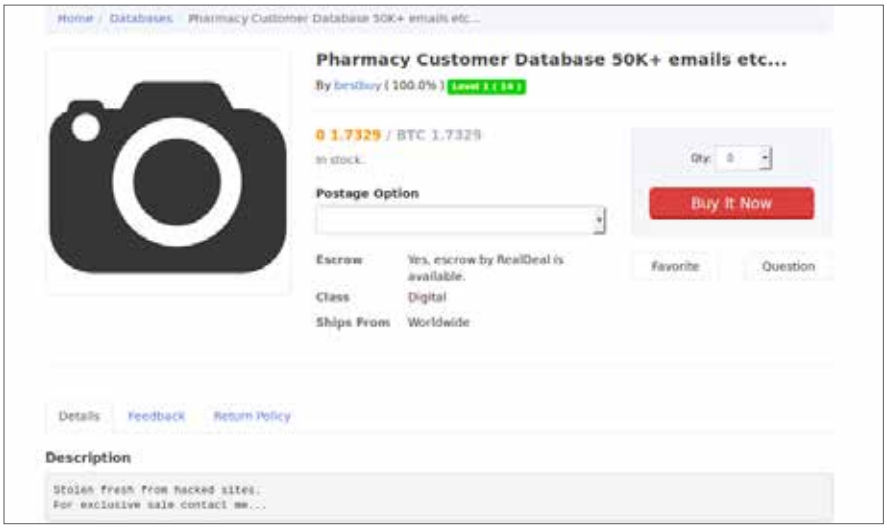


図6: 販売されているデータ

この販売者は前の例と異なる人物ですが、販売は同じマーケットで行われています。この販売者は現在も活動を続けているようで、現在までに15件のレビューがありますが、すべて肯定的な評価になっています。最近のフィードバックが表しているように、この人物は販売者として高い評価を得ています。

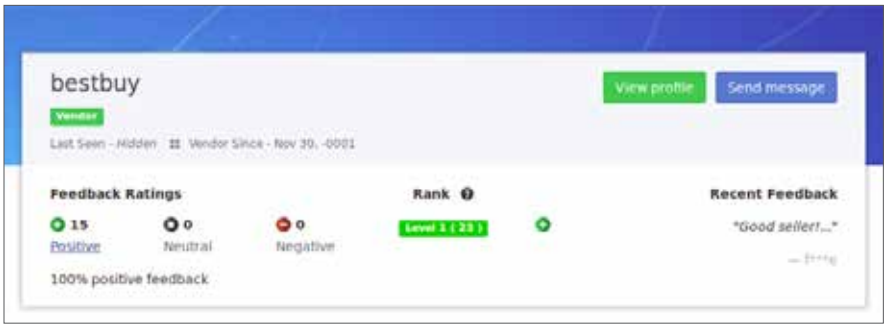


図7: 販売者の評価

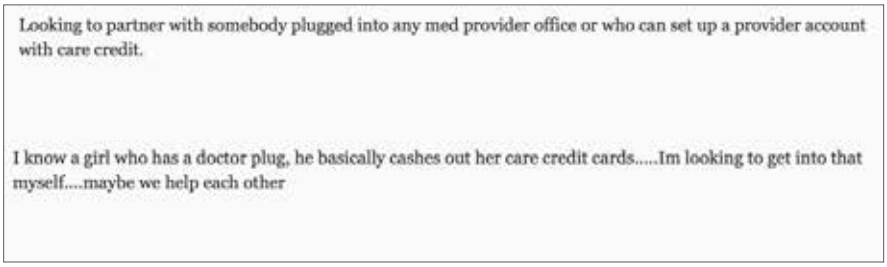
医療機関から医療データが盗まれ、販売されていることに間違いはありません。しかも、密かに販売されているのではなく、販売広告まで出ています。ソーシャル メディアで侵害行為を自慢している販売者もいます。

本稿の執筆時点で、このユーザーのTwitterアカウントは機能しなくなっていますが、このアカウントの人物が別の医療機関から盗み出したデータの宣伝をしているという報告もあります。模倣犯の可能性も否定できません。9月中旬のニュースで、別の病院が攻撃され、医療記録を流出させると脅されていることが明らかになりました。この販売者は、金銭を支払わないと盗み出した医療データを流出させると病院を脅迫したようです。

他の情報源からも、医療機関から盗まれた医療データの販売事例を数多く入手しました。盗まれた医療データを売買しているマーケットが実際に存在することは間違いありません。

内部協力者

あるダークウェブのフォーラムで、犯罪者が医療機関内の協力者を探していました。次の例では、医療専用のクレジットカード会社であるCareCreditのアカウントを取得するために内部協力者を探しています。これは、厳密にいうと医療データではありません。むしろ、『目に見えないデータの経済性』で説明した決済カード詐欺に近いものでしょう。


Looking to partner with somebody plugged into any med provider office or who can set up a provider account with care credit.

I know a girl who has a doctor plug, he basically cashes out her care credit cards.....Im looking to get into that myself....maybe we help each other

医療データの実施の価値

決済カード情報などの金融関連データには多くのマーケットが存在しています。個人の特定に必要な情報（氏名、社会保障番号、生年月日、口座番号など）をすべて含むレコードは現在、1件あたり14～25ドルで取引されています。新たに参入した販売者は低めの価格を設定していますが、小規模取引で1件あたり20ドルで売買されている例も確認しています。仕切値はさらに安く、まとめ買いの場合、カード1枚あたりの価格は3ドルほどになっています。医療データの価格はばらつきが激しく、1件あたり1セント未満から2.42ドルで取引されています。この価格は、決済カード情報に比べるとかなり安く、高いものでもカードの仕切値とあまり変わりません。

値段だけを見ると、医療データは金融関連データよりも価値が低いように見えます。これはマーケットの違いによるものでしょう。利益を上げるために複数のマーケットを同時に利用している販売者もいます。闇市場フォーラムのAlphaBayでは、Oldgollumというユーザーが40,000件の医療データを500ドルで販売していましたが、このデータに含まれる金融関連の情報は別売りになっていました。Oldgollumは、同じデータを切り売りして両方のマーケットから利益を上げています。金融関連データは個別でもバルクでも販売されていますが、医療データの場合、現時点でまとめ売りのみで、1件あたりの値段がカード情報の仕切値に近い価格になっています。医療データが付加価値になっていることは確かです。販売者は、両方のマーケットから最大の利益を引き出そうとしていますが、いずれのマーケットでも高額で売れるとは考えていません。

金融関連データ以外にもマーケットを比較する指標があります。たとえば、最近確認したソーシャルメディア アカウントの2つのデータダンプでは、いずれも6,500万から1億6,700万件のアカウントがまとめ売りされていましたが、1件あたりの価格は1ペニー未満に過ぎません。Bitcoinフォーラムなどの最近の漏えい事件でも、1件あたりの価格は似たようなものです。医療データの値段はこの金額を超えていますが、決済カードのような既存マーケットのレベルには達していません。盗まれた医療データの売買はまだ本格的ではありませんが、金融関連以外の他のデータと比べると、1件あたりの値段は高く設定されています。現在の医療データの価値は、これまでのデータベース ダンプと決済カード データの中間あたりではないでしょうか。医療データに金融関連データが含まれている場合、まとめて売るよりも別々に売ったほうが儲けが増えるようです。

医療業界を攻撃する犯罪サービス

McAfee Labsが『Cybercrime Exposed』（サイバー犯罪の現状）を公開した当時、「サービスとしての犯罪」は比較的新しい考え方で、サイバー攻撃の一部を外部に委託できることはあまり知られていませんでした。現在では、サービスとしてのサイバー犯罪は広く知られたビジネス モデルの一つとなっています。医療業界も例外ではありません。

医療業界に対する攻撃でも犯罪サービスが利用されています。脆弱性が販売され、多くの組織が侵害されています。オンラインで次のようなやり取りがあります。内容は初歩的なようですが、患者の医療データを大量に盗み出す方法が議論されています。被害者の多くは、自分たちの情報が犯罪サービスによって盗まれているとは思いもしないでしょう。

> I bought a RDP off the market yesterday but today when I tried to log in instead of windows all I got was this total MD program, looks like a database management program for doctors. Has anyone experienced anything like this before, there is no start button or anything just this program, I can't even click anything?????

最初のコメントにあるRDPの脆弱性は、最初のセクションで示した販売者が悪用したリモート デスクトップ プロトコルの欠陥と同じものです。助言を求めていた人物は次のようなアドバイスを受け取ります。

> export the DB and sell it for profit obv

これは非常に簡単な指示ですが、質問者はより戦術的な内容を聞きたかったようです。

> Ok I figgured out how to click on things (alt key for some reason) but it's still pretty useless, windows key didn't open start menu or anything. When I log in it asks me to connect to server IP I tried localhost but it returns an error message saying it was unable to find database at localhost. Any suggestions?

議論は続き、サポートのやり取りがあり、最終的にも問題を解決できたようです。


**********AMAZING UPDATE**********

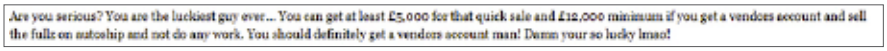
Thanks to some much needed help from [redacted] we were able to access the medical database which contains over 1000 FULLZ!!!!!!!

see pic below:

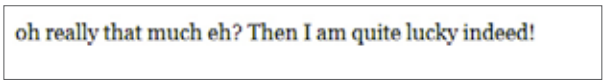
[URL]http[redacted]

Looking to sell the whole thing PM me if you're interested!

この投稿に対する返答を見ると、最初のセクションで説明したように、市場需要が確実に存在することが分かります。


Are you serious? You are the luckiest guy ever... You can get at least £5,000 for that quick sale and £12,000 minimum if you get a vendors account and sell the fullz on autoship and not do any work. You should definitely get a vendors account man! Damn your so lucky lmao!

たとえば、技術的に詳しくないサイバー犯罪者が、脆弱な組織を攻撃するためにツールを購入し、無料に近いテクニカル サポートを受けながら1,000件のレコードを盗み出し、12,000ポンド（約 1.526.600円）を稼いでいます。この例を見ても、医療業界に対する攻撃でも、サービスとしてのサイバー犯罪が積極的に利用されていることが分かります。成功を祝うメッセージを受け取った後、このサイバー犯罪者は、盗み出した医療データの販売で稼いだ金額に驚いたようです。


oh really that much eh? Then I am quite lucky indeed!

このケースでは、もう少し簡単に攻撃を実行できたかもしれません。たとえば、RDPの攻撃ツールを購入するのではなく、医療機関のアカウントを入手したほうが手間が省けます。

『Cybercrime Exposed』（サイバー犯罪の現状）で指摘したように、技術的な知識がそれほどなくてもサイバー犯罪が可能になりました。必要な知識は詳しい人から買えば十分です。事実、多くの販売者は、攻撃に直接関与する必要のない人物に盗まれたデータを販売しています。


Almost every week I have FRESH breaches in USA Healthcare/Insurance sector.
No specific requests (like specific clinic/hospital), no pieces selling, no timewasters, ONLY BULK, ETC.

多くの購入者は、何を購入したのか発覚することはないと話しています。有名な販売者がロシア語のフォーラムExploitに病院のネットワークから情報を盗み出す方法を投稿しました。スレッドのトピックは「米国の病院のネットワークにRDPでアクセスする方法」という内容でした。この人物は、患者のリスト、医療機関、メール アドレス、社会保障番号、生年月日、医療記録などの情報を販売していました。また、類似したデータを含む様々なデータベースも提供しています。この人物は、2011年からAltenen、Lampeduza などのフォーラムやカード詐欺フォーラムに投稿を繰り返し、個人情報の販売でも有名な人物です。盗まれた医療データを販売していることは間違いないでしょう。

金銭目的の犯罪活動を詳しく見てきましたが、そこには利益を得る明確な仕組みがあります。盗まれたデータを購入する理由は他にもあるかもしれませんが、侵入からデータの転売までの流れを見ると、これらの攻撃の目的が金銭であることは明らかです。

個人情報や機密データにも価値はありますが、知的財産や医療関連のデータのほうがより高い価値があるようです。このトピックだけで1冊のレポートになってしまいますが、今回はこのレベルで止めておきます。

バイオ企業/製薬会社が狙われている

医療機関の個人情報を狙ったランサムウェアや標的型攻撃が発生したのは比較的最近のことです。バイオ企業や製薬会社の知的財産を狙った攻撃は以前から行われています。最初の攻撃が確認されたのは2008年のことで、治験情報、化学式、米国で販売されている薬品の機密情報などのデータが狙われました。このような情報の経済価値が、このレポートで解説している1件あたり数セントの情報よりも高いことは明らかです。

非常に価値の高い情報であれば、数百人もの人数と1,000台以上のサーバーを使って攻撃を実行しても不思議ではありません。このような攻撃で狙われるのは民間企業だけではありません。たとえば、米国食品医薬品局（FDA）は、新製品の認可を行っているため、最も狙われる組織の一つとなっています。侵入の規模を調べるため、情報公開法に基づく請求を行ったところ、2013年から2015年の間に1,036件のインシデントが報告されていました。この中の半数は、FDAのコンピューターに対する不正アクセスです。また、21パーセントはプローブやスキャンで、19パーセントはマルウェアによる侵入でした。

バイオ企業や製薬会社のネットワーク侵入にはマルウェアがよく利用されていますが、内部の人間がデータの流出に関与していたこともあります。また、サイバー犯罪者が盗み出した情報をライバル会社に流したケースもあります。

犯人の特定には、技術的な情報だけでなく詳しい調査が必要になるため、確たる根拠もなく推測を行わないようにしていますが、技術的な情報に基づいて攻撃元を断定している調査機関もあります。しかし、犯人探しがこのレポートの目的ではありません。重要なことは、このようなデータは価値が高く、豊富なリソースを使用できる攻撃者が攻撃に成功しているという点です。

マルウェアの利用については、Community Health Systemsが米国証券取引委員会に提出したForm 8-Kに詳しく記述されています。この報告書では、巧妙なマルウェアによって会社のシステムが攻撃を受け、医療機器や機器の開発データなどの知的財産が狙われたと記載されています。調査を担当したフォレンジック チームは、「この手の犯罪組織は、航空宇宙、防衛産業、建築、エンジニアリング、テクノロジ、金融サービス、医療業界を狙っている」と報告しています。

米国学術研究会議への攻撃もそうですが、多くの場合、攻撃の前段としてスピア フィッシングが実行されています。カナダのサイバー インシデント対応センターの調査によると、このケースでは研究員のメールアドレスを収集することから攻撃が始まっています。収集したアドレスに不正なリンクを送付し、受信者がリンクをクリックすると、マルウェアがインストールされています。簡単な手口ですが、知的財産や企業秘密などの重要な情報を狙う場合にスピア フィッシングが繰り返し実行されています。

医療業界の知的財産を狙う攻撃については引き続き調査を行っていきます。攻撃の動機や攻撃者については様々な見方があるかもしれませんが、製薬会社やバイオ企業は引き続き警戒が必要であることは確かです。付加価値の高い資産を持つこれらの企業が狙われることは間違いありません。「ハッカーは製薬会社が好きなようだ。当社には[知的財産権]や薬品の化学式など、付加価値の高い資産がある。業界の大手であることもその理由の一つかもしれない。」と、Reliance Life Sciencesのバイスプレジデントは話しています。

まとめ

このレポートでは、盗まれた医療データの経済価値について説明しましたが、これは氷山の一角に過ぎません。脅威を明確に示すため、多くの事例からサンプルを取捨選択し、盗まれた医療データが販売されている状況について説明しました。サイバー犯罪者は攻撃を実行するための製品を購入しています。たとえば、エクスプロイトやエクスプロイト キットを購入またはレンタルして、世界中に感染を広げようとしています。

データ侵害のニュースを見るたびに、サイバー犯罪に対する注意が薄れているように感じます。しかし、サイバー犯罪は従来の犯罪が発展したものです。無関心を克服し、マルウェアなどの脅威に対する注意喚起を行っていく必要があります。デジタルライフから盗み出された情報は、インターネットに接続できれば、誰でも簡単に購入することができます。医療データの場合、被害を受けた後の復旧は他のデータほど簡単ではありません。たとえば、2013年に小売業のTargetで発生した攻撃では、被害者の多くがカードを破棄し、新しい決済カードの再発行を依頼しました。闇市場は大量のカード情報で溢れ、すぐに売買されましたが、個人への被害は限定的でした。医療データや個人情報の場合、復旧はそれほど簡単ではありません。このようなデータに対しては、事前に十分な対策を行い、盗難のリスクを回避するべきです。

この問題で難しい点は、医療データを盗む真の動機が明らかにならないことです。決済カード情報の場合、盗まれたカード番号は詐欺行為に利用されます。今回の調査で、特定のデータが被害者の住所の特定に利用されていることが判明しました。しかし、現時点では大量に購入された医療データの使い道は特定できていません。この問題については引き続き調査を行っていきます。新たな発見があり次第、情報を提供していく予定です。

Intel Securityについて

マカフィーはIntel Securityとなりました。Intel Securityは、Security Connected戦略、セキュリティにハードウェアを活用した革新的なアプローチ、また独自のGlobal Threat Intelligenceにより、世界中のシステム、ネットワーク、モバイル デバイスを守るプロアクティブで定評あるセキュリティ ソリューションやサービスを提供しています。Intel Securityは、マカフィーの優れたセキュリティ技術とインテルの革新性と信頼性の融合により、すべてのアーキテクチャとコンピューティング プラットフォームにセキュリティを統合します。Intel Securityは、すべてのユーザーが日々の生活でも職場でも、デジタル世界を安心して利用できるようにすることを目指しています。

www.intelsecurity.com

McAfee. Part of Intel Security.
マカフィー株式会社
東京本社　〒150-0043 東京都渋谷区道玄坂 1-12-1 渋谷マークシティウエスト 20F
TEL 03-5428-1100（代） FAX 03-5428-1480
西日本支店　〒530-0003 大阪府大阪市北区堂島 2-2-2 近鉄堂島ビル 18F
TEL 06-6344-1511（代） FAX 06-6344-1517
名古屋営業所　〒450-0002 愛知県名古屋市中村区名駅 4-6-17 名古屋ビルディング 13F
TEL 052-551-6233（代） FAX 052-551-6236
福岡営業所　〒810-0801 福岡県福岡市博多区中洲 5-3-8 アクア博多 5F
TEL 092-287-9674（代）
www.intelsecurity.com

2016年10月