Relatório

Alerta de saúde

Os ataques cibernéticos estão visando o setor de saúde

intel Security

Sumário

Este relatório foi pesquisado e redigido por:

Advanced Programs Group
Christiaan Beek
Charles McFarland
Raj Samani

Introdução

Todos conhecem a natureza não perecível dos dados médicos. Sejam registros médicos ou propriedade intelectual da próxima droga milagrosa, quando esses dados caem nas mãos de criminosos, não é fácil recuperá-los. Por que dados médicos estão sendo roubados? Eles são visados ou são simplesmente um dano colateral, como parte de um ataque diferente? Se são visados, isso sugere que há uma demanda e, se há uma demanda, deve haver um retorno de investimento. Qual é o cenário completo?

Este relatório de pesquisa é sobre o roubo de dados no setor de saúde. Descrevemos, especificamente, o mercado de dados roubados no setor de saúde e examinamos as motivações por trás desse roubo.

No relatório de pesquisa *O mercado oculto de dados* do McAfee Labs, examinamos violações de dados envolvendo o roubo de dados financeiros, especialmente informações de cartões de pagamento. Nesse relatório, não encontramos dados médicos à venda. Sabíamos que dados médicos estavam sendo roubados, mas ainda não os tínhamos visto em "mercados clandestinos". Agora, após investigações adicionais, podemos mostrar o que encontramos.

— Raj Samani, CTO da Intel Security para a Europa, Oriente Médio e África

@Raj_Samani
@McAfee_Labs

Escondido em plena vista

Pelo relatório *O mercado oculto de dados*, soubemos que existe um mercado de dados roubados e que seus negócios estão indo muito bem. O fluxo crescente de dados roubados e organizações comprometidas levou a uma queda drástica nos preços desses dados, sem perspectivas de estabilização. De fato, o volume de dados de cartões de pagamento resultou em interessantíssimos modelos de negócios, conforme vendedores tentam atrair compradores.

Nossa pesquisa nos surpreendeu pela ausência generalizada de dados médicos no baú de dados roubados colocados à venda. Não procuramos especificamente por tais dados à venda, mas esperávamos encontrá-los porque sabíamos que eles estavam sendo roubados. A ausência de dados médicos à venda nos levou a este relatório de pesquisa.

Em vez de simplesmente mostrar capturas de tela de dados médicos pessoais roubados e colocados à venda (supondo que os encontrássemos), fomos mais longe para compreender quais outras partes no setor de saúde estão sendo comprometidas. Por exemplo, empresas farmacêuticas estão sendo atacadas?

Em fevereiro, postamos o blog "Ransomware Targets Health Care Sector" (O ransomware visa o setor de saúde), no qual discutimos um incidente de ransomware contra um hospital dos EUA. O blog afirma que, agora, o ransomware está visando organizações — ao contrário da abordagem indiscriminada do passado — e que o setor de saúde já é alvo de criminosos cibernéticos. Embora este relatório examine dados médicos roubados colocados à venda, outros tipos de ataque estão sendo perpetrados contra organizações de saúde.

Antes de nos aprofundarmos nas descobertas, precisamos esclarecer uma coisa: não é nossa intenção causar inquietação. Nosso objetivo é documentar o cenário de ameaças para que as organizações de saúde possam agir. Para o setor de saúde, isso é fundamental porque não podemos simplesmente trocar de registros médicos como fazemos quando cartões de pagamento são roubados. Com efeito, a natureza não perecível dos registros médicos tornam estes particularmente valiosos. Como nossa capacidade de reduzir o impacto de uma violação de dados médicos é significativamente reduzida, precisamos fazer todo o possível para reduzir a probabilidade de ataques bem-sucedidos. O primeiro passo nesse processo é compreender a ameaça.

Dados médicos à venda?

A primeira questão a examinar é se os dados médicos roubados estão sendo colocados à venda. Nossa hipótese inicial era, simplesmente, de que não estávamos olhando os lugares certos em nossa pesquisa anterior. Essa hipótese provou ser verdadeira. Rapidamente descobrimos fornecedores da Web clandestina colocando à venda imensos volumes de dados médicos roubados. Em alguns casos, sua disponibilidade foi amplamente divulgada. Na figura 1, um vendedor colocou à venda um banco de dados contendo dados médicos pessoais de 397.000 pacientes. O que esse volume de dados inclui é descrito detalhadamente pelo vendedor na figura 2.

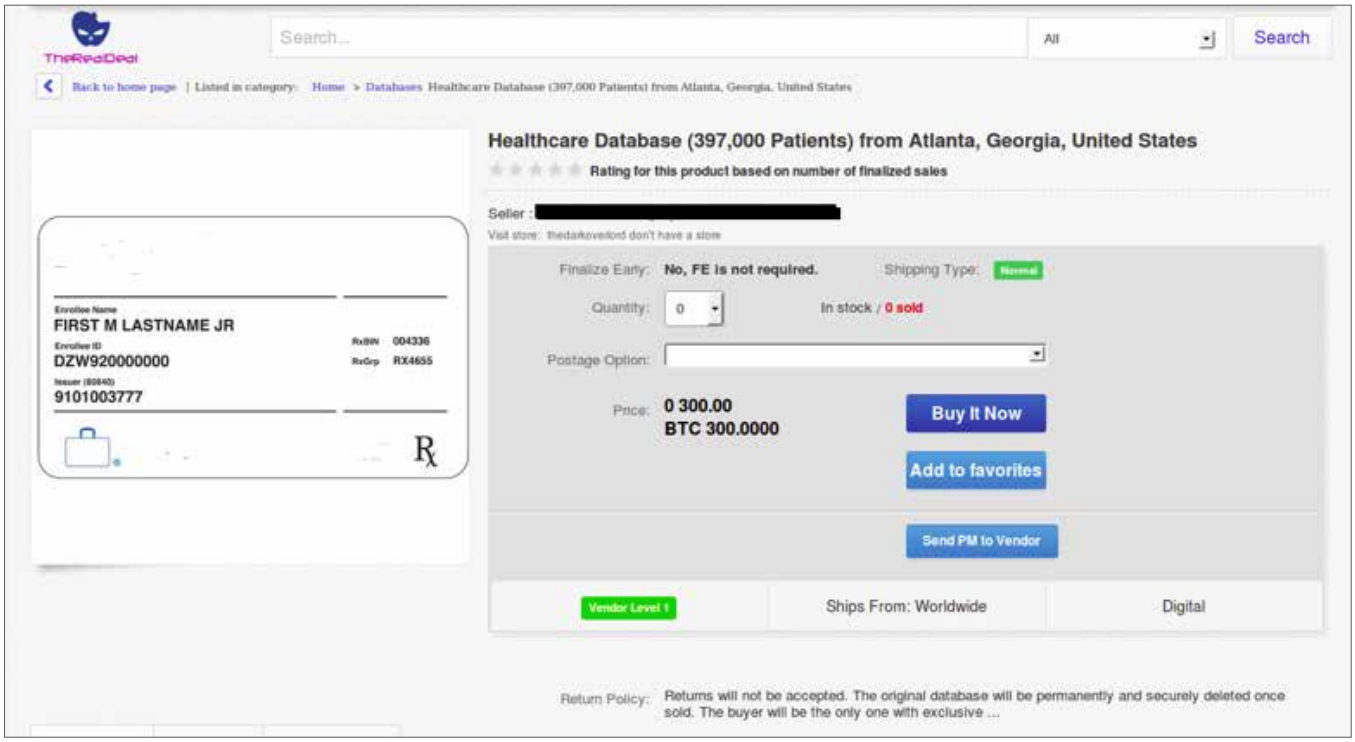


Figura 1: um banco de dados médicos à venda.

Figura 2: campos de dados de um volume de dados médicos.

No exemplo anterior, não só os nomes e endereços dos pacientes estão incluídos, mas também dados sobre seus fornecedores de assistência médica, tanto principais quanto secundários, bem como outros dados que podem ser de algum valor para potenciais compradores. O custo de tais registros é marcante: em comparação com outros volumes de dados, o preço dos dados médicos é consideravelmente maior. Detalhes podem ser encontrados mais adiante neste relatório.

Não faltam volumes de dados para examinar. A figura 3 contém uma oferta de venda de dados médicos pessoais de uma organização de saúde situada em Farmington, Missouri (EUA). Essa oferta é do mesmo vendedor citado nas figuras 1 e 2.

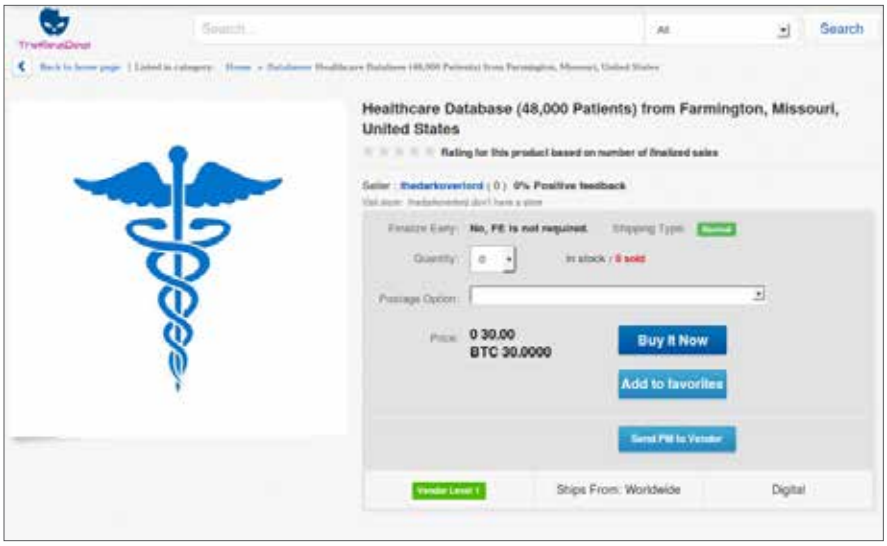


Figura 3: detalhes de uma segunda violação.

Esse vendedor não para por aí e oferece um terceiro banco de dados de registros médicos pessoais roubado de uma outra organização de saúde comprometida, conforme indicado na figura 4.

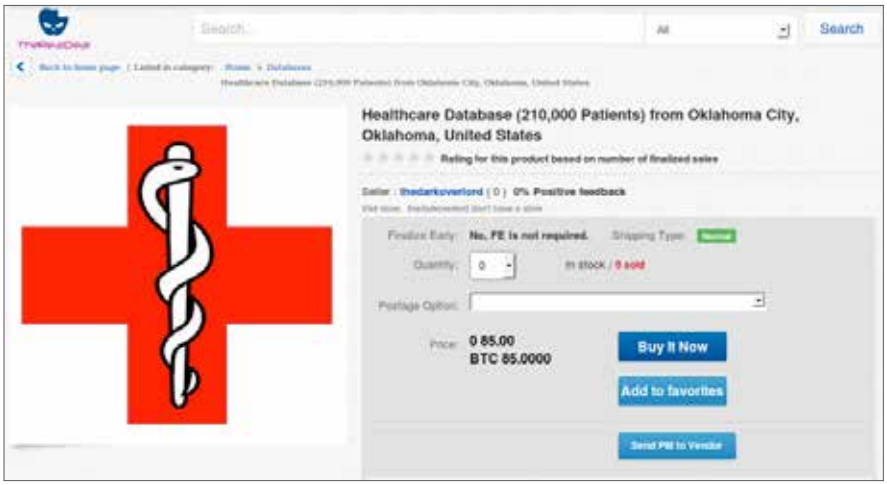


Figura 4: detalhes de uma terceira violação.

Você talvez esteja se perguntando por que afirmamos que o vendedor realmente roubou os dados. Descobrimos que o vendedor ofereceu indícios de acesso às organizações violadas. Em uma entrevista com o Deepdotweb.com, várias capturas de tela foram fornecidas, uma das quais mostramos na figura 5.

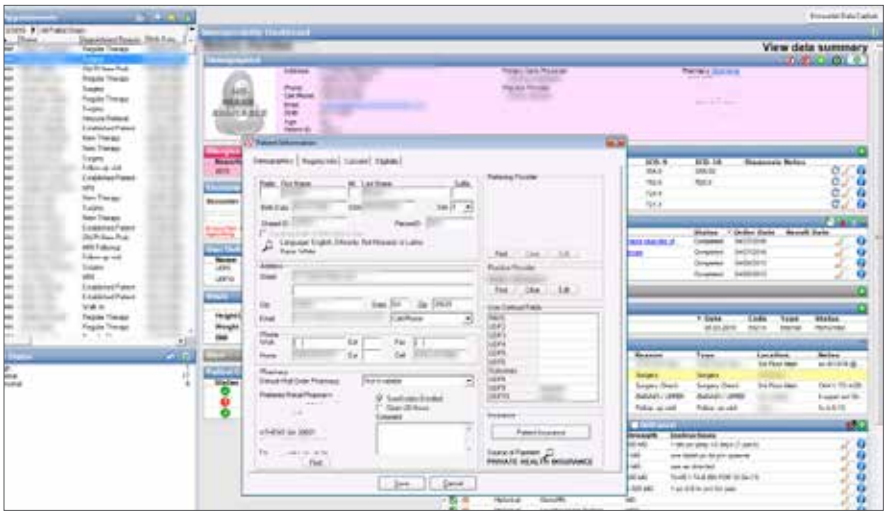


Figura 5: dados de uma organização de saúde violada.

Esse vendedor parece estar explorando uma vulnerabilidade no protocolo de desktop remoto para comprometer essas organizações.

Simplesmente roubar dados médicos é apenas parte da história. Apesar das tentativas de Hollywood de mostrar que o trabalho dos hackers se resume a digitar caracteres aleatórios em um teclado por alguns minutos, a verdade é bem diferente, exigindo muito mais tempo e empenho. Além disso, os criminosos cibernéticos pensam em termos de retorno do investimento. Para esse vendedor, a capacidade de gerar lucro para pagar pelo tempo investido (e, possivelmente, por quaisquer ferramentas necessárias) pode ser o principal fator de motivação. Em uma entrevista dada por esse vendedor ao Motherboard, ele parece ter sido bem recompensado pelo tempo gasto. O vendedor afirmou que "alguém quis comprar, especificamente, todos os registros da [seguradora]." O vendedor explicou que esse trabalho lhe rendeu US$ 100.000 líquidos até agora.

Esse episódio sugere duas coisas. Primeiro, registros médicos roubados estão à venda (como já esperávamos) e, segundo, existe claramente uma demanda por esses dados. Essa conclusão não se baseia em apenas um vendedor. Não precisamos ir muito longe para encontrar mais evidências.

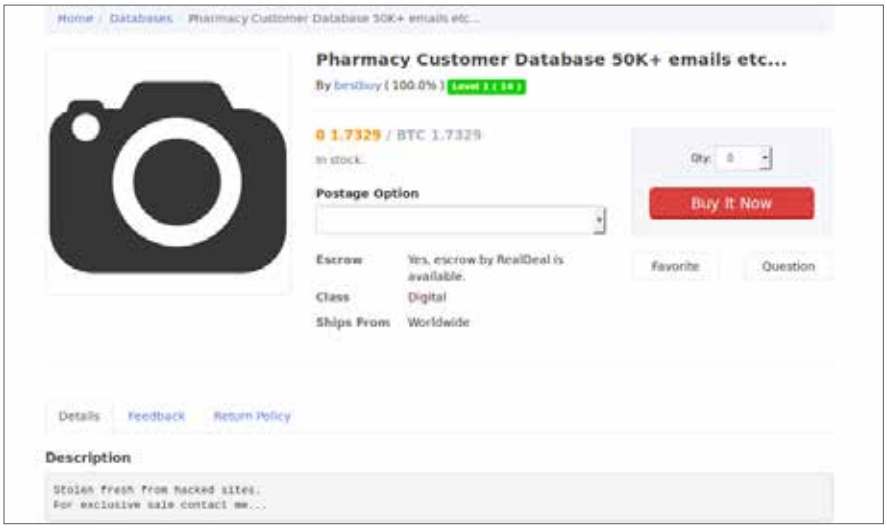


Figura 6: mais dados à venda.

O vendedor do volume de dados anterior não é o mesmo dos exemplos anteriores, embora a oferta esteja no mesmo mercado. O vendedor parece estar ativo, com 100% de feedback positivo em 15 interações até o momento. Essas avaliações positivas foram provavelmente obtidas como vendedor, conforme claramente indicado pelo feedback recente.

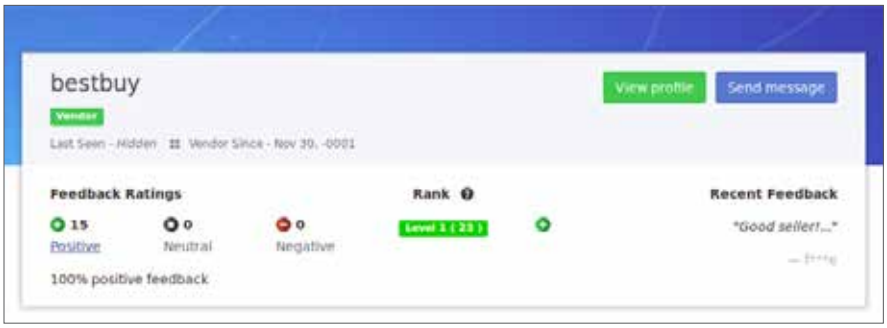


Figura 7: feedback positivo para este vendedor.

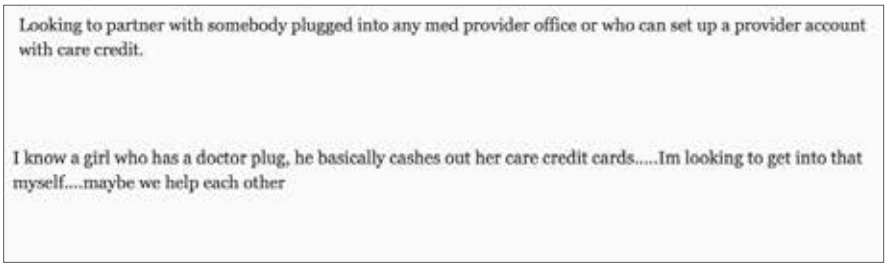
Podemos concluir que dados médicos de todo o setor de saúde estão sendo roubados e vendidos. Eles não só estão sendo vendidos, como também estão sendo abertamente anunciados para venda. Em determinados casos, o vendedor até se vangloria do comprometimento utilizando mídias sociais.

Enquanto redigíamos este relatório, a conta de Twitter do usuário anterior não estava mais funcionando. Contudo, há relatos de que os indivíduos por trás da conta voltaram com um volume de dados de uma outra organização de saúde comprometida. Ou pode se tratar de um imitador. Vimos notícias, em meados de setembro, de mais uma organização de saúde sendo extorquida sob a ameaça de divulgação de registros comprometidos. Esse vendedor parece comunicar-se primeiro com uma organização violada ameaçando divulgar os dados médicos roubados, a não ser que uma taxa seja paga.

Soubemos, por outras fontes, de muitos outros exemplos de dados médicos roubados de organizações de saúde e colocados à venda. Existe, claramente, um mercado para dados médicos roubados.

O elemento interno

Em determinados fóruns da Web clandestina, há evidências de que criminosos procuram elementos internos nas organizações de saúde. No exemplo seguinte, mostramos que elementos internos estão sendo procurados para estabelecer uma conta com a CareCredit, uma empresa de cartões de crédito para financiamento de assistência médica. A rigor, não se trata de dados médicos, tendo mais a ver com as fraudes de cartões de pagamento que discutimos em nosso relatório *O mercado oculto de dados.*


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

Os dados médicos valem mais?

Os dados financeiros (por exemplo, informações de cartões de pagamento) têm muitos mercados estabelecidos. O preço corrente por um único registro de informações "fullz" — pacotes completos de informações de identificação individual, com nomes, números de CPF, datas de nascimento e números de contas — variam de US$ 14 a mais de US$ 25 por registro. Vendedores menos estabelecidos têm baixos preços iniciais; vimos recentemente preços em torno de US$ 20 por registro para compras de pequeno volume. Preços no atacado podem ser ainda mais baixos, chegando a US$ 3 por cartão para venda em massa. Por outro lado, os registros médicos parecem ser altamente variáveis e vão de uma fração de centavo a US$ 2,42 por registro. Esse preço é significativamente menor que os preços de cartões de pagamento individuais, mas apenas ligeiramente menor que preços de cartões no atacado.

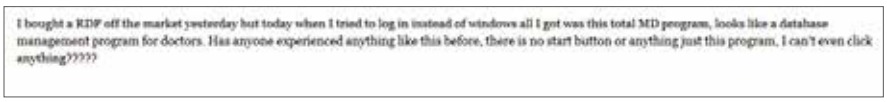
Esses preços indicariam que dados médicos não valem tanto quanto dados financeiros? Talvez, mas os mercados são diferentes. Alguns vendedores tiram proveito de mercados paralelos para aumentar seus lucros. No fórum de mercado clandestino AlphaBay, o usuário Oldgollum vendeu 40.000 registros médicos por US$ 500, mas removeu especificamente os dados financeiros, os quais eram vendidos separadamente. Oldgollum está, efetivamente, tentando obter o máximo dos dois mercados. Os dados financeiros também podem ser vendidos individualmente ou em massa. Os dados médicos parecem ser vendidos apenas em massa por enquanto, o que reduz o preço por registro a algo próximo dos preços de cartões no atacado. Certamente, os dados médicos agregam valor à transação. Os vendedores procuram assegurar a obtenção de lucro máximo de ambos os mercados e não esperam vender a preços maiores a qualquer dos lados.

Dados financeiros não são o único tipo de dados que podemos usar para comparar dinâmicas de mercado. Pegue, por exemplo, dois casos recentes de volumes de contas de mídias sociais, ambos vendidos em massa, contendo entre 65 milhões e 167 milhões de contas, mas também obtendo apenas frações de centavo por registro. Vazamentos ainda mais recentes envolvendo fóruns de Bitcoin têm preços semelhantes por registro. Nossas descobertas sobre dados médicos excedem esse valor, mas ainda não vendem à cotação de mercados estabelecidos, como o de cartões de pagamento. Os dados médicos roubados parecem ainda estar se consolidando, mas o ecossistema atual já possui um valor por registro maior que em mercados de dados contábeis não financeiros. Os dados médicos valem mais? Eles parecem valer algo entre volumes de bancos de dados tradicionais e dados de cartões de pagamento. Quando os dados médicos contêm dados financeiros, pode ser ser mais lucrativo vendê-los separadamente do que conjuntamente.

O cibercrime como serviço na área de saúde

Quando o McAfee Labs publicou o relatório de pesquisa Cybercrime Exposed (A exposição do crime cibernético), o conceito de "cibercrime como serviço" era uma ideia relativamente nova. O fato de que os componentes de um ataque cibernético podem ser terceirizados não era amplamente conhecido. Atualmente isso não é mais novidade e o cibercrime como serviço é um modelo de negócios bem divulgado. Esse modelo de negócios aplica-se igualmente ao setor de saúde.

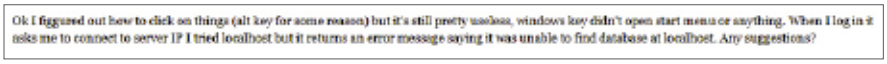
Agora vemos o cibercrime como serviço operando no setor de saúde, com evidências de que vulnerabilidades estão sendo vendidas e de que organizações estão sendo comprometidas na forma de um serviço. Vejamos uma troca on-line que parece elementar, mas que discute o roubo de um grande volume de dados médicos pessoais de pacientes que ignoram que suas informações foram roubadas por um criminoso "como serviço".


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?????

A vulnerabilidade RDP no primeiro comentário é a mesma falha de protocolo de desktop remoto que foi explorada por nosso vendedor na primeira seção. O(s) indivíduo(s) que buscaram ajuda receberam alguma orientação:


export the DB and sell it for profit obv

Trata-se de uma instrução bastante simples. No entanto, parece que a solicitação foi consideravelmente mais tática:


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?

A discussão continuou e, após uma interação de suporte adicional, o autor da postagem original conseguiu solucionar o problema:


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

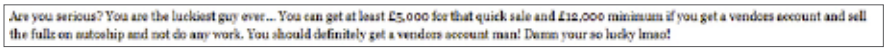
Thanks to some much needed help from [redacted] we were able to access the medical database which contains over 1000 FULLZ!!!!!!!

see pic below:

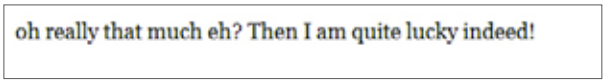
[URL]http[redacted]

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

A resposta a essa postagem demonstra algo que ilustramos na primeira seção: a existência de uma demanda de mercado.


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!

Colocando isso em perspectiva, um ladrão cibernético com pouca qualificação técnica compra ferramentas para explorar uma organização vulnerável, utiliza essas ferramentas com um pouco de suporte técnico gratuito e, em seguida, extrai 1.000 registros que podem lhe render £ 12.000 (aproximadamente R$ 45.670). Se quiséssemos uma comprovação de que o cibercrime como serviço está em alta no setor de saúde, essa interação seria um claro exemplo. Após mais mensagens congratulatórias, o criminoso cibernético pareceu um pouco surpreso com a renda que ele(a) conseguiu gerar com a venda dos dados médicos roubados:


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

Nesse exemplo, o processo poderia ter sido ainda mais simples. Em vez de "comprar o RDP", o atacante poderia simplesmente ter adquirido uma conta pertencente a uma organização de saúde.

Atualmente, conforme indicamos em *A exposição do crime cibernético,* os criminosos cibernéticos não precisam ter muito conhecimento técnico, apenas meios para pagar pela ajuda de alguém que tenha a experiência necessária. De fato, existe uma variedade de vendedores oferecendo dados roubados a compradores que não precisam se envolver em ataques diretos contra organizações:


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.

Vimos inúmeros compradores reclamando que os "wares" comprados dos vendedores nunca aparecem. Em uma postagem de um reputado vendedor do fórum Exploit, com maioria de falantes de russo, um vendedor falava sobre obtenção de informações de uma rede de hospitais. O assunto do tópico, traduzido do russo, é "Acesso RDP à rede de hospitais dos EUA". O vendedor estava traficando listas de pacientes, fornecedores, e-mails, números de CPF, datas de nascimento, registros médicos e outras informações. O vendedor também oferecia vários bancos de dados de informações que incluíam dados semelhantes. Ele postou em fóruns e mercados como Altenen, Lampeduza e vários fóruns sobre roubo de números de cartões de crédito desde 2011 e tem um histórico de venda de informações de identificação pessoal. Portanto, há um alto grau de confiança de que os dados médicos colocados à venda são verdadeiros.

Com esses exemplos, detalhamos atividades criminosas cuja motivação é ganho financeiro, com caminhos claros para monetização. Evidentemente, os compradores de dados roubados podem ter outras motivações, mas da violação à revenda de dados roubados, a motivação desses atacantes é claramente financeira.

Embora dados pessoais ou confidenciais sejam valiosos, é provável que propriedade intelectual ou outros tipos de dados relacionados à medicina tenham um valor mais alto. Poderíamos escrever um relatório completo somente sobre esse tópico, mas por enquanto faremos apenas uma abordagem rápida.

Setores farmacêutico e de biotecnologia em destaque

Exigir resgate de organizações de saúde ou visá-las para roubo de dados pessoais é um fenômeno relativamente recente. Visar empresas farmacêuticas e de biotecnologia para roubo de propriedade intelectual parece ser algo bem mais consolidado. Os primeiros casos remontam a 2008, com relatos de que os dados cobiçados incluem "informações sobre medicamentos experimentais, fórmulas químicas e dados confidenciais de todos os medicamentos vendidos no mercado dos EUA". Fica claro que o valor econômico de tais informações é consideravelmente maior que o mercado de meros centavos por registro identificado por este e outros relatórios.

Oportunidades como essa aparentemente justificam o custo de uma operação de roubo cibernético que "empregue centenas de pessoas e faça uso de pelo menos 1.000 servidores". Tais ataques não visam exclusivamente empresas do setor privado. Por exemplo, o órgão de fiscalização de alimentos e medicamentos dos EUA (Food and Drug Administration) "esteve entre os mais visados devido ao seu papel como ponto de partida para colocação de novos produtos no mercado". Para compreender a proporção das tentativas de invasão, uma requisição sob a lei de liberdade da informação (Freedom of Information Act) revelou "1.036 incidentes relatados entre 2013 e 2015. Destes, metade envolveram acesso ilegítimo e não autorizado a computadores da FDA. Quase 21% foram classificados como sondagens ou varreduras — semelhantes ao phishing — e 19% foram intrusões de malware".

O malware parece ser um vetor de ataque comum nas tentativas de comprometer redes farmacêuticas e de biotecnologia, mas em outros casos, elementos internos maliciosos foram utilizados para extrair dados com objetivo de lucro. Em um caso, por exemplo, o ladrão cibernético "pretendia usar as informações para lançar suas próprias empresas concorrentes."

Tivemos o cuidado de não especular em termos de atribuição porque isso requer investigações que vão além de indicadores técnicos. Apesar de pesquisas de terceiros fazerem afirmações sobre fontes de ataques com base em tais indicadores, nossa intenção é demonstrar o valor de tais dados e que perpetradores de ameaças, aparentemente com muitos recursos, são bem-sucedidos em suas atividades.

O uso de malware foi discutido em um envio de formulário 8-K pela Community Health Systems para a Securities and Exchange Commission dos EUA. Eles afirmaram que "malware sofisticado" atacou o sistema da empresa. O envio destacou que o atacante "buscava propriedade intelectual valiosa, como dados de desenvolvimento de equipamentos e dispositivos médicos". A equipe forense encarregada da investigação relatou que "esse grupo costuma visar empresas das áreas de defesa e aeroespacial, construção e engenharia, tecnologia, serviços financeiros e saúde".

Na maioria dos casos, o spear phishing antecede a infecção, conforme demonstrado em um ataque contra o National Research Council. Nesse exemplo, o ataque "começou com a coleta de endereços de e-mail válidos de funcionários do conselho de pesquisa", segundo um estudo realizado pelo centro canadense de resposta a incidentes cibernéticos. O ataque foi seguido pela instalação de malware, depois que os destinatários clicavam em links maliciosos. Apesar de sua simplicidade, o phishing parece ser um tema recorrente mesmo quando o objetivo é o roubo de propriedade intelectual, segredos comerciais e outras informações próprias ou confidenciais.

Nossa pesquisa prossegue sobre ataques contra empresas de saúde cujo objetivo é o roubo de propriedade intelectual. Podemos debater a motivação e os perpetradores por trás desses ataques, mas não há dúvida de que as empresas farmacêuticas e de biotecnologia precisam estar atentas porque seus ativos mais valiosos estão na mira de autores de ameaças determinados. Como declarou o vice-presidente da Reliance Life Sciences, "os hackers gostam de empresas farmacêuticas, pois temos ativos críticos de grande valor, como [direitos sobre propriedade intelectual] e fórmulas de vários medicamentos. Além disso, fazer parte de uma grande indústria também nos torna um alvo preferencial.

Conclusão

Os exemplos de um mercado oculto de dados médicos roubados representa apenas a ponta do iceberg. Omitimos muitas outras categorias e serviços, mas esperamos que esses exemplos tornem claras algumas ameaças. Neste relatório, abordamos dados relacionados à saúde roubados e colocados à venda. Mostramos que criminosos cibernéticos também compram produtos que viabilizam ataques. Isso inclui a compra e o aluguel de explorações e kits de exploração que abastecem um número enorme de infecções por todo o mundo.

Quando lemos sobre violações de dados, o ramo do crime cibernético pode parecer tão distante da vida cotidiana que é tentador ignorarmos a mensagem. No entanto, o crime cibernético é meramente uma evolução do crime tradicional. Devemos superar nossa apatia e prestar atenção à recomendação de combatermos o malware e outras ameaças. Caso contrário, informações de nossas vidas digitais podem aparecer para revenda a qualquer um com uma conexão de Internet. Contudo, no que se refere a dados médicos, a possibilidade de recuperar nossas informações é consideravelmente menor do que com outros dados. Por exemplo, quando a loja varejista Target foi violada em 2013, os cartões comprometidos das vítimas foram cancelados e novos cartões de pagamento foram emitidos. Isso limitou o dano às pessoas porque os cartões inundaram o mercado clandestino e foram rapidamente colocados à venda. Para dados médicos e informações pessoais, a estratégia de recuperação não é assim tão simples. Por isso é fundamental que adotemos medidas proativas para reduzir a probabilidade de que tais dados sejam roubados.

Uma questão problemática nesse tópico é a falta de evidências que indiquem a motivação por trás da aquisição de dados médicos roubados. Com informações de cartões de pagamento, temos documentado que os números de cartões roubados são utilizados para perpetrar fraudes contra as vítimas. No decorrer de nossas investigações, identificamos onde determinados dados são buscados para verificar os endereços das vítimas. Porém, ainda não identificamos usos específicos para compras de dados médicos em massa. Continuaremos nossa pesquisa nesse assunto, porque ele merece bastante atenção, e postaremos atualizações à medida que encontrarmos mais dados.

Sobre a Intel Security

A McAfee agora é parte da Intel Security. Com sua estratégia Security Connected, sua abordagem inovadora para a segurança aprimorada por hardware e a exclusiva Global Threat Intelligence, a Intel Security está sempre empenhada em desenvolver soluções de segurança proativas e comprovadas e serviços para a proteção de sistemas, redes e dispositivos móveis para uso pessoal ou corporativo no mundo todo. A Intel Security combina a experiência e o conhecimento da McAfee com a inovação e o desempenho comprovados da Intel para tornar a segurança um elemento essencial em toda arquitetura e em cada plataforma de computação. A missão da Intel Security é oferecer a todos a confiança para viver e trabalhar de forma segura no mundo digital.

www.intelsecurity.com

McAfee. Part of Intel Security.
Av. das Nações Unidas, 8.501 - 16° andar
CEP 05425-070 - São Paulo - SP - Brasil
Telefone: +55 (11) 3711-8200
Fax: +55 (11) 3711-8286
www.intelsecurity.com