Bericht

Gefahren für das Gesundheitswesen

Cyber-Kriminelle nehmen das Gesundheitswesen ins Visier

intel Security

Inhalt

Dieser Bericht wurde recherchiert und geschrieben von:

Advanced Programs Group
Christiaan Beek
Charles McFarland
Raj Samani

Einführung 3
Gut sichtbar verborgen 4
Medizinische Daten im Angebot? 4
Der Insider 9
Sind medizinische Daten mehr wert? 9
Cybercrime-as-a-Service im Gesundheitsbereich 10
Biotechnologie/Pharmazie im Blicklicht 12
Fazit 13

Einführung

Jeder hat schon einmal von der Unveränderbarkeit medizinischer Daten gehört. Unabhängig davon, ob es um unsere Patientendaten oder das geistige Eigentum zum neuesten Wunderheilmittel geht – wenn diese Daten in die falschen Hände gelangen, lässt sich das kaum rückgängig machen. Warum werden medizinische Daten gestohlen? Sind diese Daten das eigentliche Ziel oder lediglich Kollateralschaden? Wenn diese Daten gezielt gestohlen wurden, besteht offensichtlich eine Nachfrage. Und das bedeutet, dass diese Daten Rendite versprechen. Was steckt dahinter?

Dieser Forschungsbericht untersucht Datendiebstahl im Gesundheitswesen. Dabei gehen wir insbesondere auf den Markt für gestohlene Daten aus dem Gesundheitswesen sowie auf die Motive für den Diebstahl ein.

Im McAfee Labs-Forschungsbericht *Das heimliche Geschäft mit Daten* untersuchten wir die Datenkompromittierungen durch den Diebstahl von Finanzdaten, insbesondere Zahlungskarteninformationen. Bei den Recherchen zu diesem Bericht fanden wir keine medizinischen Daten, die zum Kauf angeboten wurden. Wir wussten, dass medizinische Daten gestohlen wurden, fanden sie jedoch nicht auf den Schwarzmärkten. Nach weiteren Nachforschungen können wir nun unsere Erkenntnisse darlegen.

– Raj Samani, Intel Security-CTO für Europa, Naher Osten und Afrika

@Raj_Samani
@McAfee_Labs

Gut sichtbar verborgen

Im Bericht *Das heimliche Geschäft mit Daten* erfuhren wir, dass es einen Markt für gestohlene Daten gibt und dieses Geschäft sehr gut läuft. Tatsächlich hat der zunehmende Strom kompromittierter Unternehmen und gestohlener Daten zu einem derartigen Preisverfall geführt, dass wir uns fragen, ob diese Daten nicht irgendwann kostenlos weitergereicht werden. Die Suche nach Käufern hat aufgrund der enormen Anzahl von Zahlungskartendaten einige faszinierende Geschäftsmodelle hervorgebracht.

Bei unseren Nachforschungen waren wir überrascht, dass keine medizinischen Daten in der Schatztruhe der gestohlenen Daten zu finden waren, die zum Verkauf stehen. Auch wenn wir nicht konkret nach diesen Daten suchten, so erwarteten wir aufgrund der bekannt gewordenen Diebstähle doch zumindest, entsprechende Angebote zu finden. Die Abwesenheit medizinischer Daten motivierte uns zu diesem Forschungsbericht.

Statt einfach Screenshots von Angeboten für gestohlene persönliche medizinische Daten zu erstellen (vorausgesetzt, dass wir solche Angebote finden), wollten wir besser verstehen, welche anderen Parteien innerhalb des Gesundheitswesens kompromittiert werden. Werden zum Beispiel auch Pharmazie-Unternehmen angegriffen?

Im Februar veröffentlichten wir den Blog-Beitrag *Ransomware Targets Health Care Sector* (Ransomware greift das Gesundheitswesen an), in dem wir über Ransomware-Angriffe auf Krankenhäuser in den USA berichteten. In diesem Blog-Beitrag weisen wir darauf hin, dass Ransomware jetzt auf Unternehmen abzielt (statt auf den bisherigen breit gefächerten, wahllosen Ansatz) und auch das Gesundheitswesen ins Visier nimmt. Mit anderen Worten: Auch wenn wir uns in diesem Bericht auf die zum Verkauf angebotenen medizinischen Daten konzentrieren, sind Gesundheitsorganisationen zusätzlich noch anderen Angriffen ausgesetzt.

Bevor wir unsere Erkenntnisse erläutern, möchten wir eines klarstellen: Es ist nicht unsere Absicht, Angst zu verbreiten. Stattdessen möchten wir mit diesem Bericht die aktuellen Bedrohungen dokumentieren, damit Gesundheitsorganisationen geeignete Maßnahmen ergreifen können. Dies ist im Gesundheitswesen ganz besonders wichtig, da wir medizinische Daten – im Gegensatz zu Zahlungskarten – nach einem Diebstahl nicht einfach ändern können. Vielmehr sind medizinische Daten nicht veränderbar und daher ganz besonders wertvoll. Und da es kaum Möglichkeiten gibt, die negativen Folgen einer Kompromittierung medizinischer Daten zu vermindern, müssen wir alles daran setzen, die Wahrscheinlichkeit eines erfolgreichen Angriffs zu verringern. Deshalb besteht der erste Schritt darin, die Bedrohung zu verstehen.

Medizinische Daten im Angebot?

Die erste Herausforderung sind die Untersuchungen dazu, ob medizinische Daten zum Verkauf angeboten werden. Zunächst vermuteten wir, dass wir bei unseren bisherigen Nachforschungen einfach an den falschen Stellen suchten – was sich bewahrheitete. Schnell stellten wir fest, dass die „Dark Web"-Anbieter gestohlene medizinische Daten in großen Paketen verkaufen. In einigen Fällen wurde viel Werbung für die Verfügbarkeit dieser Daten gemacht. In Abbildung 1 bot ein Verkäufer eine Datenbank mit persönlichen medizinischen Daten zu 397.000 Patienten an. Der Inhalt dieses Datenpakets wird in Abbildung 2 näher dargestellt.

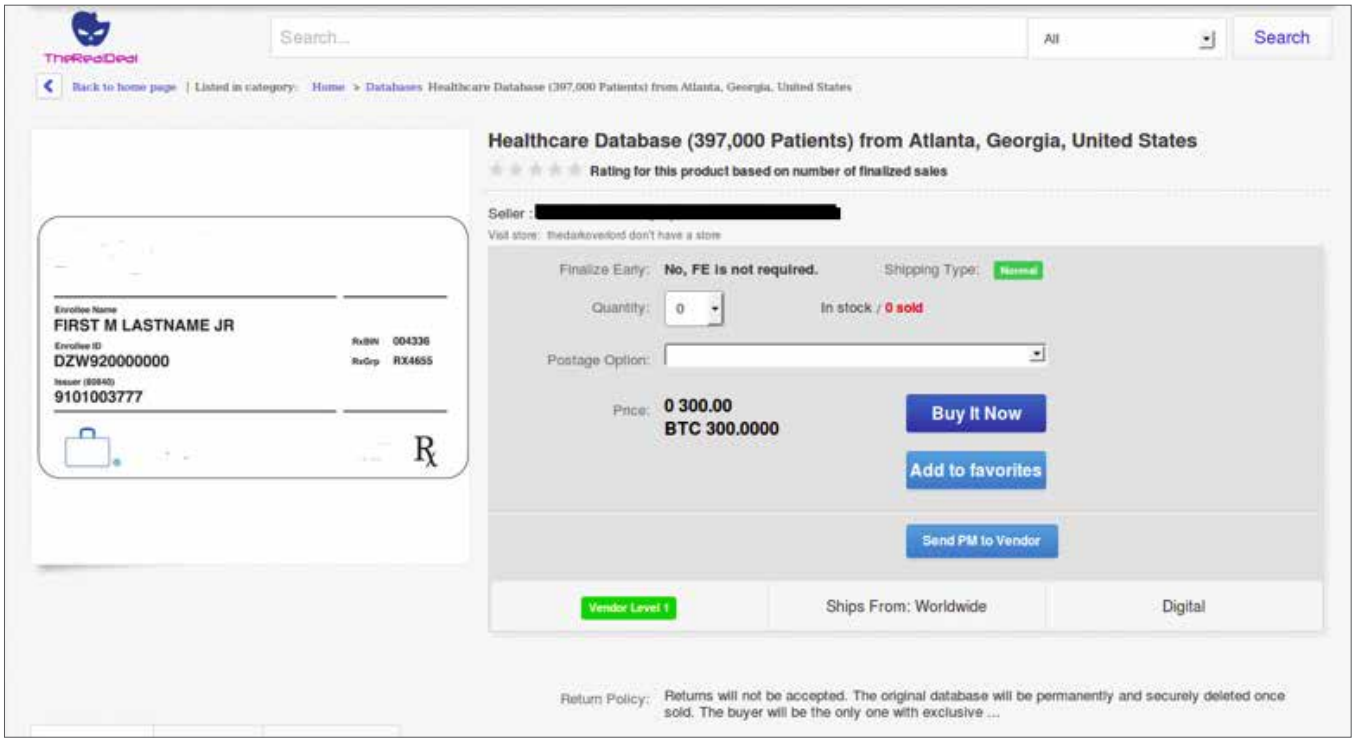


Abbildung 1: Eine zum Verkauf angebotene Datenbank aus dem Gesundheitsbereich.

Abbildung 2: Datenfelder aus einem Datenpaket aus dem Gesundheitsbereich.

Im vorherigen Beispiel umfasst das Datenpaket nicht nur die Namen und Adressen der Patienten, sondern auch Angaben zur primären und sekundären Krankenversicherung sowie weitere Informationen, die für potenzielle Käufer wertvoll sein könnten. Die Preise für diese Datensätze sind beachtlich: Im Vergleich zu anderen Datenpaketen liegen die Preise für medizinische Daten erheblich höher. Wir gehen später in diesem Bericht genauer darauf ein.

Es werden zahlreiche Datenpakete angeboten. Abbildung 3 zeigt ein Angebot für persönliche medizinische Daten, die von einer Gesundheitsorganisation in Farmington, Missouri (USA), gestohlen wurden. Dieses Angebot stammt von demselben Verkäufer wie vom obigen Beispiel (Abbildung 1 und 2).

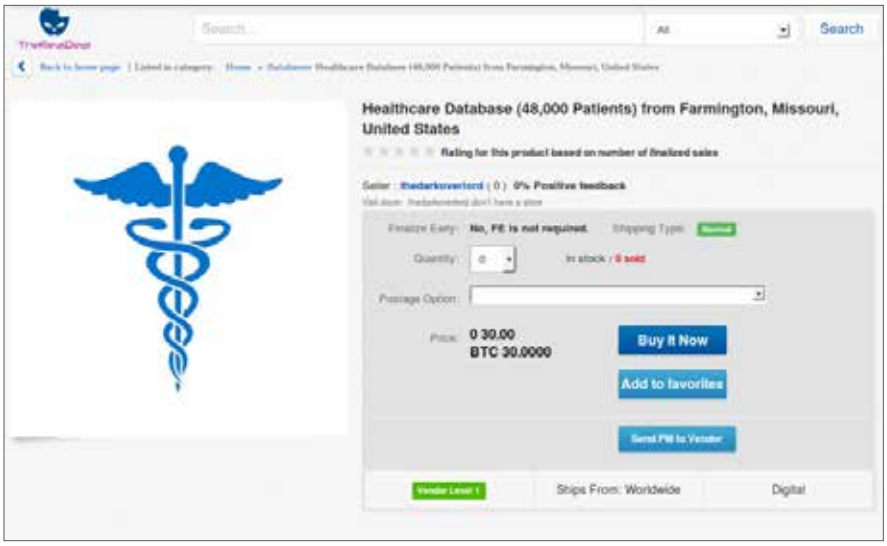


Abbildung 3: Details aus einer zweiten Kompromittierung.

Der Verkäufer geht sogar noch weiter und bietet eine dritte Datenbank mit persönlichen medizinischen Daten an, die von einer weiteren kompromittierten Gesundheitsorganisation gestohlen wurden (siehe Abbildung 4).

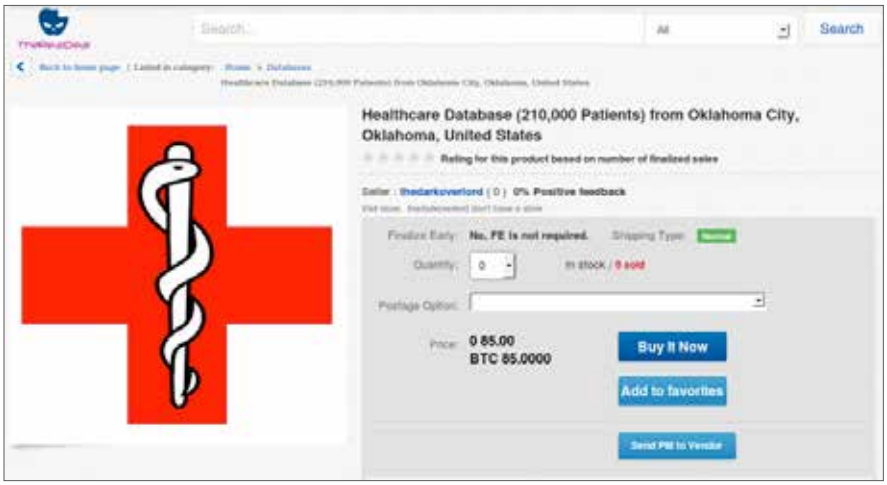


Abbildung 4: Details aus einer dritten Kompromittierung.

Vielleicht fragen Sie sich, warum wir explizit darauf hinweisen, dass der Verkäufer die Daten tatsächlich gestohlen hat: Wir stellten fest, dass der Verkäufer einen Nachweis über den Zugriff auf die kompromittierte Organisation lieferte. Für ein Interview mit Deepdotweb.com wurden mehrere Screenshots zur Verfügung gestellt. Einen der Screenshots sehen Sie in Abbildung 5.

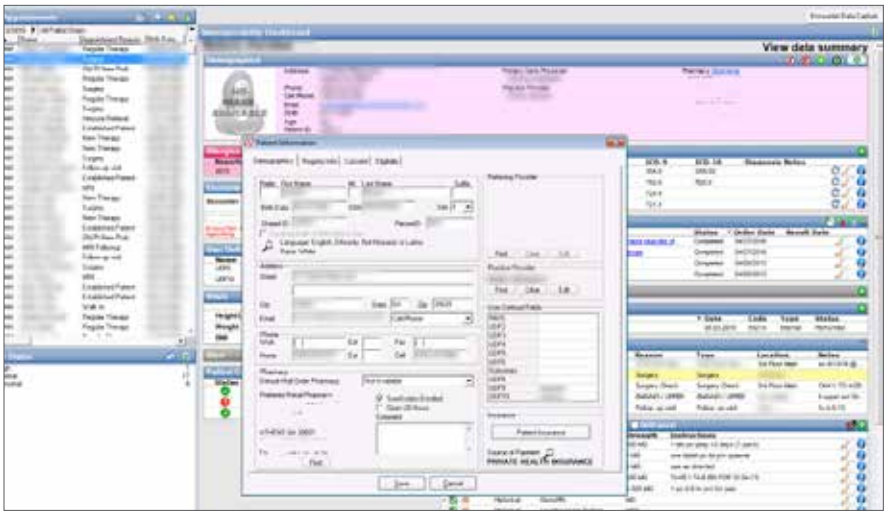


Abbildung 5: Daten aus einer kompromittierten Gesundheitsorganisation.

Dieser Verkäufer nutzt zur Kompromittierung dieser Organisationen offenbar eine Schwachstelle im Remote-Desktop-Protokoll aus.

Der einfache Diebstahl medizinischer Daten ist nur ein Teil des Problems. Auch wenn Hollywood gern behauptet, dass Kriminelle zum Hacken lediglich ein paar wahllose Zeichen in die Tastatur hämmern müssen, sind für einen erfolgreichen Angriff erheblich mehr Zeit und Aufwand erforderlich. Zudem kommt es den Cyber-Kriminellen die Rendite an. Für diesen Verkäufer ist es wahrscheinlich die größte Motivation, den Zeitaufwand (und die Investition in eventuell erforderliche Tools) in Profit zu verwandeln. Laut einem Interview mit Motherboard wurde dieser Verkäufer anscheinend für die aufgewendete Zeit sehr gut entlohnt. Der Verkäufer erklärte: „Es gab einen Käufer, der speziell an allen Datensätzen [der Krankenkasse] interessiert war.“ Er erläuterte, dass er netto bisher 100.000 US-Dollar eingenommen hat.

Dieser Vorfall zeigt zwei Dinge: Erstens werden medizinische Datensätze (wie erwartet) zum Verkauf angeboten und zweitens besteht eindeutig eine Nachfrage nach solchen Daten. Diese Schlussfolgerung basiert nicht nur auf diesem einen Verkäufer. Wir mussten nicht viel weiter suchen, um weitere Beweise zu finden.

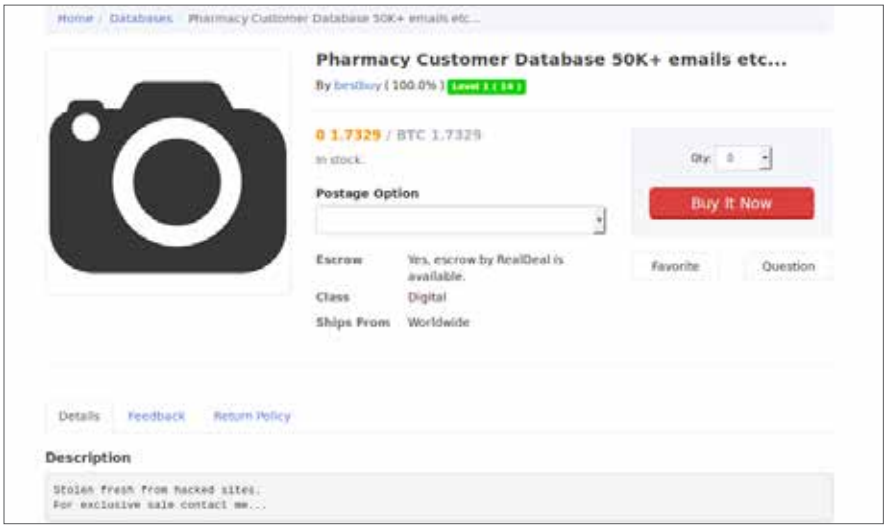


Abbildung 6: Weitere zum Verkauf angebotene Daten.

Der Verkäufer des oben genannten Datenpakets ist nicht mit den früheren Beispielen identisch – auch wenn das Angebot auf dem gleichen Markt erschien. Der Verkäufer scheint weiterhin aktiv zu sein und erhielt aus bisher 15 Interaktionen 100 % positives Feedback. Das letzte Feedback weist darauf hin, dass er diese positiven Bewertungen wahrscheinlich als Verkäufer erhielt.

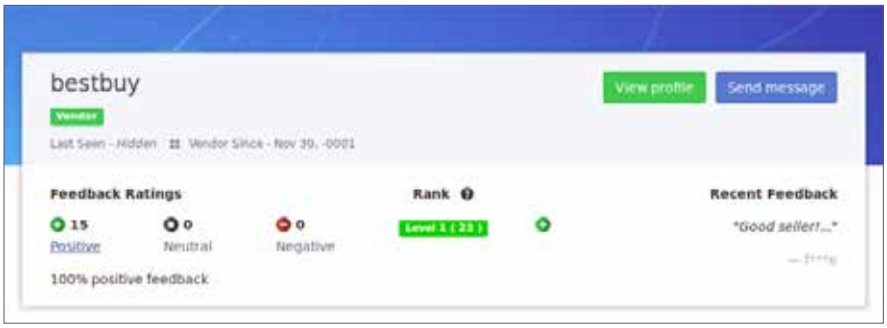


Abbildung 7: Gutes Feedback für diesen Verkäufer.

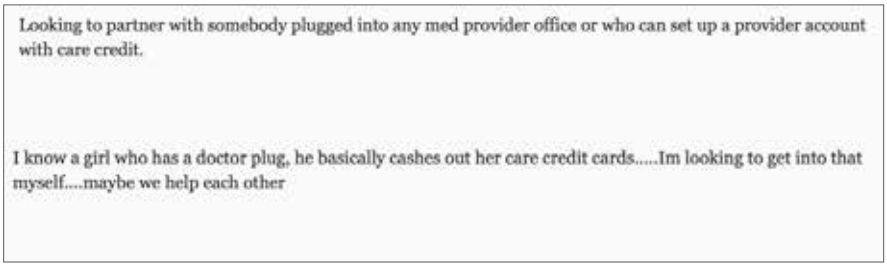
Wir können davon ausgehen, dass im gesamten Gesundheitswesen medizinische Daten gestohlen und verkauft werden. Zudem werden diese Daten nicht nur verkauft, sondern offen zum Verkauf angeboten und beworben. In einigen Fällen brüsten sich die Verkäufer sogar damit, soziale Medien für die Kompromittierung missbraucht zu haben.

Zum Zeitpunkt der Erstellung dieses Berichts funktioniert das Twitter-Konto des oben genannten Benutzers nicht mehr. Es gibt jedoch Berichte darüber, dass die Person hinter diesem Konto mit einem neuen Datenpaket wieder auftauchte, das von einer anderen Gesundheitsorganisation gestohlen wurde. Möglicherweise handelt es sich jedoch um einen Nachahmer. In den Nachrichten erschienen Mitte September Berichte darüber, dass eine Gesundheits-organisation mit der Veröffentlichung kompromittierter Daten erpresst wurde. Dieser Verkäufer kommuniziert scheinbar zuerst mit der kompromittierten Organisation und droht mit der Veröffentlichung der gestohlenen Daten, sofern nicht ein bestimmter Betrag gezahlt wird.

Wir fanden in anderen Quellen viele weitere Beispiele für gestohlene Daten von Gesundheitsorganisationen, die zum Verkauf angeboten wurden. Mit anderen Worten: Es gibt eindeutig einen Markt für gestohlene medizinische Daten.

Der Insider

Es gibt in bestimmten Dark Web-Foren Belege dafür, dass Kriminelle nach Insidern in Gesundheitsorganisationen suchen. Im folgenden Beispiel zeigen wir, dass Insider gesucht werden, um ein Konto bei CareCredit, einem Kreditkartenunternehmen im Gesundheitswesen, zu erstellen. Dabei handelt es sich nicht immer unbedingt um medizinische Daten, sondern eher um Zahlungskartenbetrug wie in unserem Bericht *Das heimliche Geschäft mit Daten*.


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

Sind medizinische Daten mehr wert?

Für Finanzdaten wie Zahlungskarteninformationen gibt es viele etablierte Märkte. Der aktuelle Preis für einen einzigen Datensatz mit „fullz"-Informationen (vollständige Pakete mit personengebundenen Angaben zur Person, einschließlich Namen, Sozialversicherungsnummern, Geburtsdatum und Kontonummer) liegt bei 14 US-Dollar bis zu mehr als 25 US-Dollar pro Datensatz. Weniger etablierte Verkäufer haben geringere Einführungspreise. Wir haben kürzlich für kleine Verkäufe Angebote von etwa 20 US-Dollar pro Datensatz gefunden. Großhandelspreise können darunter weit liegen – mit bis zu 3 US-Dollar pro Kartendatensatz bei großen Paketen. Medizinische Datensätze scheinen hingegen sehr variabel zu sein und reichen von Preisen mit weniger als einem Cent bis zu 2,42 US-Dollar pro Datensatz. Dieser Preis liegt erheblich niedriger als bei einzelnen Zahlungskarten, ist dabei aber nur etwas geringer als bei Großhandelspreisen für Kreditkartendaten.

Sind medizinische Daten also mehr wert als Finanzdaten? Das ist durchaus möglich, wobei die Unterschiede zwischen den Märkten eine Rolle spielen. Einige Verkäufer nutzen die parallelen Märkte aus, um ihre Gewinne zu erhöhen. Im Untergrundmarkt-Forum AlphaBay verkaufte der Benutzer Oldgollum 40.000 medizinische Datensätze für 500 US-Dollar, wobei er die Finanzdaten ausdrücklich entfernte und separat verkaufte. Oldgollum fährt also quasi zweigleisig, um beide Märkte maximal auszunutzen. Finanzdaten können ebenfalls einzeln oder im Paket verkauft werden. Medizinische Daten werden derzeit scheinbar nur im Paket verkauft, wodurch der Preis pro Datensatz nur wenig über dem Großmarktpreis für Kreditkartendaten liegt. Da es sich um medizinische Daten handelt, sind die Transaktionen wertvoller. Die Verkäufer versuchen, maximalen Profit aus beiden Märkten zu ziehen und rechnen auf beiden Märkten nicht mit Premium-Preisen.

Finanzdaten sind nicht der einzige Datentyp, den wir zum Vergleich der Marktdynamiken heranziehen können. Ein weiteres Beispiel sind zwei kürzlich angebotene Pakete mit Social-Media-Kontodaten, die in Paketen mit 65 bis 167 Millionen Konten verkauft wurden und pro Datensatz nur Bruchstücke eines Cents erzielten. Auch aktuellere Leaks in Bitcoin-Foren erzielen ähnliche Preise pro Datensatz. Unsere Recherchen zeigen, dass die Preise für medizinische Daten höher, aber immer noch unter den Preisen liegen, die auf etablierten Märkten wie denen für Zahlungskartendaten erreicht werden. Die gestohlenen medizinischen Daten nehmen scheinbar immer mehr Form an, doch das aktuelle Ökosystem zeigt bereits einen höheren Wert pro Datensatz als in Märkten für nicht finanzbezogene Kontendaten. Sind medizinische Daten mehr wert? Der Wert liegt scheinbar zwischen dem für herkömmliche Datenbankpakete und dem für Zahlungskartendaten. Wenn die medizinischen Daten Finanzinformationen umfassen, lässt sich der Profit steigern, wenn die Daten getrennt voneinander verkauft werden.

Cybercrime-as-a-Service im Gesundheitsbereich

Als McAfee Labs den Forschungsbericht *Cybercrime Exposed* (Die verschiedenen Gesichter der Cyber-Kriminalität) veröffentlichte, war das Konzept des Cybercrime-as-a-Service noch relativ neu. Die Tatsache, dass Teile eines Cyber-Angriffs ausgelagert werden können, war noch nicht allgemein bekannt. Heute überrascht das niemanden mehr und Cybercrime-as-a-Service ist ein sehr gut etabliertes Geschäftsmodell, das sich auch auf den Gesundheitsbereich gut anwenden lässt.

Cybercrime-as-a-Service wird jetzt im Gesundheitsbereich eingesetzt, und es gibt Belege dafür, dass Schwachstellen verkauft und Organisationen „als Service“ kompromittiert werden. Im Folgenden zeigen wir einen Online-Austausch, der scheinbar einfach ist, aber den Diebstahl einer großen Menge persönlicher medizinischer Daten von Patienten zum Thema hat, die nicht ahnen, dass ihre Daten von einem Service-Terminal gestohlen wurden.

> 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?????

Die RDP-Schwachstelle im ersten Kommentar ist der gleiche Remote-Desktop-Protokollfehler, der von unserem Verkäufer im ersten Abschnitt ausgenutzt wurde. Die Personen, die Hilfe suchten, erhielten einige Unterstützung:

> export the DB and sell it for profit obv

Das ist eine ziemlich einfache Anleitung. Die Anfrage scheint jedoch erheblich taktischerer Natur zu sein:

> 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?

Der Austausch wurde fortgesetzt, und nach einigen weiteren Support-Interaktionen konnte der ursprüngliche Poster das Problem erfolgreich beheben:


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

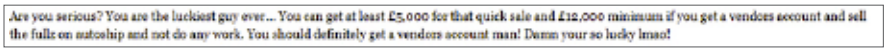
Thanks to some much needed help from [redacted] we were able to access the medical database which contains over 1000 FULLZ!!!!!!!

see pic below:

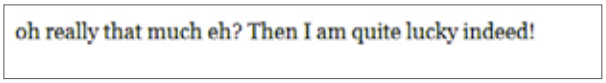
[URL]http[redacted]

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

Die Reaktion auf diese Nachricht ist ein Beleg für unsere Beobachtung aus dem ersten Abschnitt: Es besteht eine Marktnachfrage.


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!

Mit anderen Wort: Ein Cyber-Dieb mit relativ wenig technischen Kenntnissen kauft Tools, mit denen er eine gefährdete Organisation ausnutzen kann. Und mit etwas kostenlosem Technik-Support kann er 1.000 Datensätze extrahieren, die ihm netto 12.000 £ (etwa 13.475 EUR) einbringen. Wenn wir einen Beweis dafür benötigen, dass Cybercrime-as-a-Service im Gesundheitssektor intensiv eingesetzt wird, finden wir in diesem Austausch genau diesen Beleg. Nach einigen weiteren Glückwünschen schien der Cyber-Kriminelle etwas überrascht über den hohen Gewinn zu sein, der sich mit dem Verkauf der gestohlenen medizinischen Daten erzielen lässt:


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

In diesem Beispiel wäre auch eine noch einfachere Vorgehensweise möglich gewesen. So hätte der Angreifer, statt „RDP zu kaufen“, einfach ein Konto erwerben können, das zu einer Gesundheitsorganisation gehört.

Wie wir im Bericht *Cybercrime Exposed* (Die verschiedenen Gesichter der Cyber-Kriminalität) zeigten, benötigen Cyber-Kriminelle heute wenig Technikwissen und lediglich ausreichend Geld, um jemanden mit den erforderlichen Kenntnissen zu bezahlen. Tatsächlich wenden sich viele Verkäufer gestohlener Daten an Kunden, die sich dann nicht mit den direkten Angriffen auf Organisationen befassen müssen:


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.

Gleichzeitig fanden wir zahlreiche Käufer, die sich darüber beschwerten, die von Verkäufern erworbene Ware nie erhalten zu haben. In einem Post von einem glaubwürdigen Käufer auf dem vorrangig russischsprachigen Forum „Exploit“ spricht ein Verkäufer davon, Informationen von einem Krankenhausnetzwerk zu erhalten. Das Thema des Threads lautet (übersetzt aus dem Russischen): „RDP-Zugriff auf das US-Krankenhausnetzwerk“. Der Verkäufer verhökerte Patientenlisten, Dienstleisterinformationen, E-Mails, Sozialversicherungs-nummern, Geburtsdaten, medizinische Datensätze sowie andere Informationen. Zudem bot er verschiedene Datenbanken mit ähnlichen Informationen an.
Er postet seit 2011 in Foren und Marktplätzen wie Altenen, Lampeduza sowie in mehreren Kreditkartenbetrugsforen und ist dafür bekannt, personenbezogene Informationen zu verkaufen. Daher kann man zu einem bestimmten Grad darauf vertrauen, dass die zum Verkauf angebotenen medizinischen Daten echt sind.

Mit diesen Beispielen haben wir kriminelle Aktivitäten aufgezeigt, bei denen es um den finanziellen Vorteil geht und Daten erfolgreich zu Geld gemacht werden. Die Käufer gestohlener Daten können natürlich auch andere Motive haben, doch von der Kompromittierung bis zum Verkauf der gestohlenen Daten sind die Motive der Angreifer eindeutig finanzieller Natur.

Auch wenn persönliche oder sensible Daten einen gewissen Wert haben, liegt der Wert von geistigem Eigentum oder anderen Datentypen mit Medizinbezug wahrscheinlich höher. Wir könnten allein zu diesem Thema einen ganzen Bericht schreiben, möchten hier jedoch nur einen kleinen Einblick geben.

Biotechnologie/Pharmazie im Blicklicht

Die Erpressung von Gesundheitsorganisationen und der gezielte Diebstahl persönlicher Daten sind ein relativ neues Phänomen. Angriffe auf Biotechnologie- und Pharmazie-Unternehmen auf der Suche nach geistigem Eigentum treten wahrscheinlich bereits erheblich länger auf. Die ersten Beispiele erfolgten bereits im Jahr 2008, wobei damals unter anderem nach Informationen zu Arzneimittelprüfungen, chemischen Formeln sowie vertraulichen Daten zu allen Medikamenten gesucht wurde, die auf dem US-Markt verkauft werden. Der wirtschaftliche Wert dieser Informationen ist eindeutig erheblich höher als die erzielbaren Cents pro Datensatz, die in diesem und anderen Berichten thematisiert wurden.

Solche Geschäftschancen rechtfertigen die Kosten für Cyber-Diebstahlaktionen, bei denen „hunderte Personen und mindestens 1.000 Server“ zum Einsatz kommen. Diese Angriffe konzentrieren sich nicht ausschließlich auf den privaten Sektor. So gehört die US-amerikanische Food and Drug Administration (Behörde für Lebens- und Arzneimittel) „zu den auf häufigsten angegriffenen Behörden, weil sie bei der Einführung neuer Produkte auf den Markt eine so wichtige Rolle spielt“. Zum besseren Verständnis der Anzahl der Eindringungsversuche: Laut einer Anfrage in Bezug auf den Freedom of Information Act (US-Gesetz zur Informationsfreiheit) wurden „im Zeitraum zwischen 2013 und 2015 insgesamt 1.036 Vorfälle erfasst. Die Hälfte dieser Vorfälle beinhaltete illegalen, unbefugten Zugang zu FDA-Computern. Weitere 21 Prozent wurden als Tests oder Scans (ähnlich Phishing-Angriffen) eingestuft. Bei 19 Prozent handelte es sich um Malware-Eindringungen.“

Malware kommt bei Kompromittierungsversuchen auf Biotechnologie- und Pharmazie-Netzwerke scheinbar häufig zum Einsatz, doch in anderen Fällen wurden böswillige Insider angestellt, die gegen Bezahlung Daten extrahierten. In einem Fall wollte der Cyber-Dieb mit den Informationen ein eigenes Wettbewerbsunternehmen gründen.

Wir schreiben diese Aktivitäten bewusst niemandem zu, da dazu Untersuchungen erforderlich wären, die weit über die technischen Indikatoren hinausgehen. Während Drittanbieterberichte basierend auf diesen Indikatoren Behauptungen zu den Quellen der Angriffe aufstellen, möchten wir in erster Linie den Wert dieser Daten verdeutlichen und aufzeigen, dass Bedrohungsakteure mit umfangreichen Ressourcen durchaus erfolgreich sind.

Der Einsatz von Malware wurde von Community Health Systems in einer 8-K-Meldung gegenüber der US Securities and Exchange Commission (US-Börsenaufsichtsbehörde für die Kontrolle des Wertpapierhandels) angesprochen. Darin berichteten sie von einer „raffinierten Malware“, die das System des Unternehmens angegriffen hatte. In der Meldung wurde angemerkt, dass der Angreifer nach „wertvollem geistigem Eigentum wie Daten zu medizinischen Geräten und Weiterentwicklungen suchte“. Das für die Untersuchung verantwortliche Forensikteam

gab an, dass „diese Gruppe typischerweise Unternehmen in Branchen wie Luft- und Raumfahrt, Verteidigung, Bau und Ingenieurwesen, Technologie, Finanzdienstleistungen und Gesundheitswesen angreift“.

In den meisten Fällen kommt zur Infektion Spearphishing zum Einsatz, wie sich auch bei einem Angriff auf den National Research Council (kanadische Behörde für wissenschaftliche und industrielle Forschung) zeigte. Entsprechend einer Untersuchung des Canadian Cyber Incident Response Centre „begann dieser Angriff mit der Sammlung gültiger E-Mail-Adressen zu Mitarbeitern des Forschungsrats“. Sobald die Empfänger auf böswillige Links klickten, wurde Malware installiert. Trotz der einfachen Vorgehensweise kommt es auch dann immer wieder zu Spearphishing-Angriffen, wenn es um den Diebstahl von geistigem Eigentum, Geschäftsgeheimnissen und anderen sensiblen oder proprietären Informationen geht.

Wir setzen unsere Untersuchung zu Angriffen im Gesundheitswesen, die auf den Diebstahl von geistigem Eigentum abzielen, auch weiterhin fort. Auch wenn sich trefflich über die Motive und Akteure hinter diesen Angriffen diskutieren lässt, gibt es keinen Zweifel daran, dass Pharmazie- und Biotechnologie-Unternehmen aufmerksam bleiben müssen, da sich ihre wichtigsten Ressourcen im Visier entschlossener Bedrohungsakteure befinden. Ein Vice President bei Reliance Life Sciences sagte dazu: „Hacker lieben Pharmazie-Unternehmen, weil wir über so wertvolle und wichtige Ressourcen wie [Rechte an geistigem Eigentum] und Formeln verschiedener Medikamente verfügen. Zusätzlich sind wir deshalb ein so beliebtes Ziel, weil wir zu einem großen Branchenvertreter gehören.“

Fazit

Die in diesem Bericht vorgestellten Beispiele für das heimliche Geschäft mit gestohlenen medizinischen Daten stellen nur die Spitze eines Eisbergs dar. Viele weitere Kategorien und Dienste blieben unerwähnt, doch wir hoffen, dass wir mit diesen Beispielen die Größe einiger Gefahren deutlich machen konnten. In diesem Bericht ging es um gestohlene Daten aus dem Gesundheitsbereich, die zum Verkauf angeboten werden. Wir zeigten, dass Cyber-Kriminelle auch Produkte kaufen, die Angriffe ermöglichen. Dazu gehören der Kauf sowie die Anmietung von Exploits und Exploit-Kits, die die enorme Zahl der weltweiten Infektionen in die Höhe treiben.

Wenn wir über Datenkompromittierungen lesen, mögen wir das Gefühl haben, dass sich die Cyber-kriminelle Branche weitab von unserem täglichen Leben bewegt, sodass wir versucht sind, die Nachricht zu ignorieren. Cyber-Kriminalität ist jedoch lediglich eine Weiterentwicklung herkömmlicher Kriminalität. Wir müssen unsere Gleichgültigkeit überwinden und Hinweise dazu beachten, wie sich Schadsoftware und andere Bedrohungen abwehren lassen. Wenn wir dies nicht tun, könnten die Daten unseres digitalen Lebens für jeden mit einer Internetverbindung zum Verkauf angeboten werden. In Bezug auf medizinische Daten ist es jedoch erheblich schwieriger, einmal kompromittierte Daten zurückzuerlangen. Als zum Beispiel der Einzelhändler Target im Jahr 2013 kompromittiert wurde, sperrten die Opfer ihre kompromittierten Karten und erhielten neue Geldkarten. Dadurch konnte der Schaden für den Einzelnen eingeschränkt werden, obwohl die Karten den Untergrundmarkt fluteten und schnell zum Verkauf angeboten wurden. Bei medizinischen Daten und persönlichen Informationen ist die Problembehebung nicht so einfach. Daher müssen wir Präventivmaßnahmen ergreifen, um die Wahrscheinlichkeit eines Datendiebstahls zu verringern.

Ein beunruhigender Aspekt dieser Problematik ist die Tatsache, dass es keinen Hinweis auf die Motive der Käufer der gestohlenen medizinischen Daten gibt. Bei Zahlungskartendaten konnten wir nachweisen, dass die gestohlenen Kartendaten für betrügerische Aktionen gegen die Opfer genutzt wurden. Im Laufe der Untersuchungen konnten wir feststellen, wo bestimmte Daten nachgefragt wurden, um die Adressen der Opfer zu verifizieren. Derzeit konnten wir jedoch noch keine konkrete Nutzung der massenhaft gekauften medizinischen Daten ausmachen. Wir werden unsere Untersuchungen zu diesem Thema fortsetzen, da es große Aufmerksamkeit verdient. Sobald wir mehr Informationen haben, werden wir diese veröffentlichen.

Über Intel Security

McAfee gehört jetzt zu Intel Security. Durch die Security Connected-Strategie, einen innovativen Ansatz für Hardware-unterstützte Sicherheitslösungen sowie das Global Threat Intelligence-Netzwerk ist Intel Security voll und ganz darauf konzentriert, für die Sicherheit seiner Kunden zu sorgen. Dazu liefert Intel Security präventive, bewährte Lösungen und Dienste, mit denen Systeme, Netzwerke und Mobilgeräte von Privatanwendern und Unternehmen weltweit geschützt werden können. Intel Security verknüpft die Erfahrung und Fachkompetenz von McAfee mit der Innovation und bewährten Leistung von Intel, damit Sicherheit als essentieller Bestandteil jeder Architektur und Computerplattform eingebettet wird. Intel Security hat sich zum Ziel gesetzt, allen – Privatpersonen ebenso wie Unternehmen – die Möglichkeit zu geben, die digitale Welt sicher nutzen zu können.

www.intelsecurity.com

McAfee. Part of Intel Security.
Ohmstr. 1
85716 Unterschleißheim
Deutschland
+49 (0)89 37 07-0
www.intelsecurity.com

Die in diesem Dokument enthaltenen Informationen werden Intel Security-Kunden ausschließlich für Fort- und Weiterbildungszwecke bereitgestellt. Die hier enthaltenen Informationen können sich jederzeit ohne vorherige Ankündigung ändern und werden wie besehen zur Verfügung gestellt, ohne Garantie oder Gewährleistung auf die Richtigkeit oder Anwendbarkeit der Informationen zu einem bestimmten Zweck oder für eine bestimmte Situation. Intel und die Intel- und McAfee-Logos sind Marken der Intel Corporation oder von McAfee, Inc. in den USA und/oder anderen Ländern. Alle anderen Namen und Marken sind Eigentum der jeweiligen Besitzer.
Copyright © 2016 Intel Corporation. 1806_1016
OKTOBER 2016