JAHRESBERICHT DER PANDALABS 2015

panda

pandalabs

panda

pandalabs

1. EINFÜHRUNG

1 Einführung

Im vergangenen Jahr gab es einen Hauptakteur in der Welt der Cybersicherheit. Einerseits brach die Anzahl neu geschaffener Malware Rekorde mit mehr als 84 Millionen neuer Varianten, während wir andererseits erlebten, dass große Unternehmen und alle Arten von Webseiten angegriffen wurden oder deren Kundendaten gestohlen wurden. Dies führte dazu, dass Millionen von Usern weltweit von Cyberkriminalität betroffen waren.

Hotelketten seien besonders erwähnt, da sie zum Hauptziel von Kriminellen wurden, und zwar aufgrund der riesigen Datenmengen, die sie verwalten, wie zum Beispiel Kreditkartendaten.

Cryptolocker suchten die Geschäftswelt heim. Aufgrund dessen, dass viele Opfer bereit waren, für die Rückgabe ihrer Daten zu zahlen, erlebten wir einen riesigen Anstieg bei den Angriffen auf Unternehmen.

Das Internet der Dinge hat sich an die Spitze geschoben, wie Sie in diesem Bericht lesen werden. Es scheint, dass die internetfähigen Geräte ziemlich schlecht gesichert sind. 2015 konnten wir miterleben, wie es verschiedenen Spezialisten gelang, sich in die Systeme von Autos zu hacken und diese fernzusteuern.

Es gibt jedoch nicht nur schlechte Nachrichten. Private Unternehmen und Sicherheitskräfte in verschiedenen Ländern arbeiten zunehmend zusammen. Langsam aber sicher errichten sie Schranken um die Cyberkriminellen, die im Internet lauern. Obwohl es noch eine Menge zu tun gibt, ist die Tatsache, dass ihre Verbrechen nicht länger ungestraft bleiben, ein Anfang.

Adobe Flash ist wegen seiner Sicherheitslücken, die genutzt werden, um Millionen von Usern weltweit zu infizieren, ein Alptraum für die Sicherheitswelt. Doch seine Tage scheinen gezählt zu sein, denn immer mehr Systeme verbieten seine Nutzung.

Google ist ein weiteres Unternehmen, das beschlossen hat, Flash (über seinen Chrome Browser) nicht länger zu unterstützen. Und Amazon lässt keine Werbung auf seiner Webseite zu, die dieses Format nutzt.

2. DAS JAHR IN ZAHLEN

2

Das Jahr in Zahlen

Das vergangene Jahr war wieder einmal ein Rekordjahr, wenn es um die Menge an kreierter Malware geht.

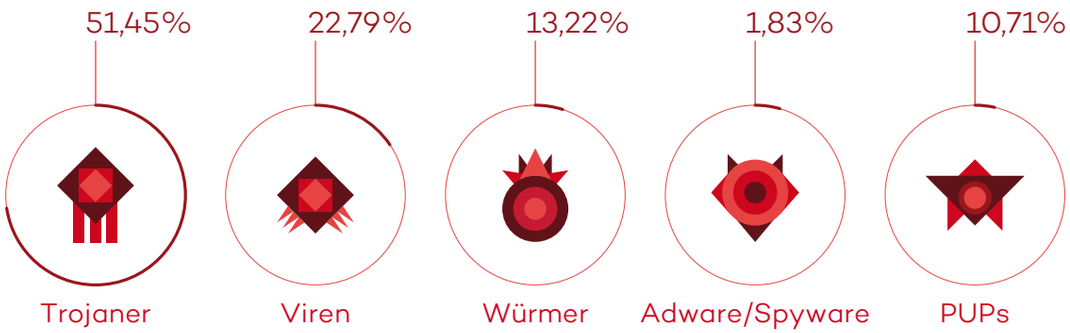
Insgesamt wurden mehr als 84 Millionen neuer Exemplare von den PandaLabs entdeckt und neutralisiert. Das sind durchschnittlich 230.000 Samples pro Tag.

Derzeit haben wir 304 Millionen registrierte Malware-Exemplare. Das bedeutet, dass mehr als jedes vierte Sample, das je entdeckt wurde, im Jahre 2015 erfasst wurde (27,36 %).

Abgesehen von Trojanern, die wie immer einen Großteil der Malware ausmachen, waren PUPs (Potenziell Unerwünschte Programme) und verschiedene Varianten von Cryptolocker (oder Ransomware) im vorigen Jahr stark vertreten. Cryptolocker haben weltweit Chaos verursacht, indem sie Informationen kidnappten und für die Rückgabe Lösegeld verlangten.

Malware-Arten, die 2015 kreiert wurden:

NEU ENTWICKELTE MALWARE
IN 2015, NACH TYP



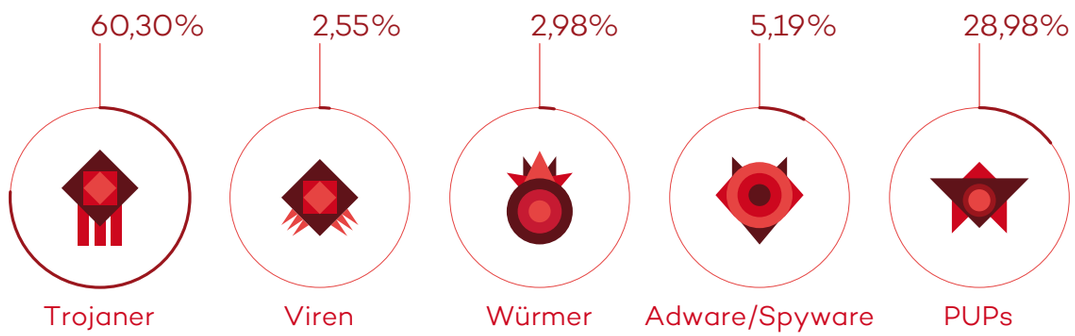
Trojaner führen wie gewöhnlich die Rangliste an, mit mehr als 50 Prozent der im Laufe des Jahres erzeugten Samples.

Jedoch ist die Anzahl der neu entwickelten Trojaner niedriger als im Vorjahr, insbesondere wenn man sie mit den anderen Kategorien — vor allem Viren (22,79 %), Würmern (13,22 %) und PUPs (10,71 %) — vergleicht, deren Prozentzahlen deutlich gestiegen sind.

Wenn wir die Infektionen analysieren, die weltweit durch Malware verursacht wurden, können wir dank der Daten von der Collective Intelligence feststellen, dass Trojaner die Ursache für die meisten Infektionen waren (60,30 %).

Hier ein Überblick darüber, wie sich die Ursachen für die Infektionen aufteilen:

INFEKTIONEN NACH MALWARE TYP
IN 2015



Wir stellen fest, dass PUPs auf dem zweiten Platz liegen und für fast ein Drittel der Infektionen verantwortlich sind. Ihnen folgen Adware/Spyware (5,19 %), Würmer (2,98 %) und Viren (2,55 %). Aggressive Verbreitungstechniken und Softwareprogramme, die von PUPs genutzt werden, bedeuten, dass sie eine hohe Installationsrate auf den Computern der User erzielen.

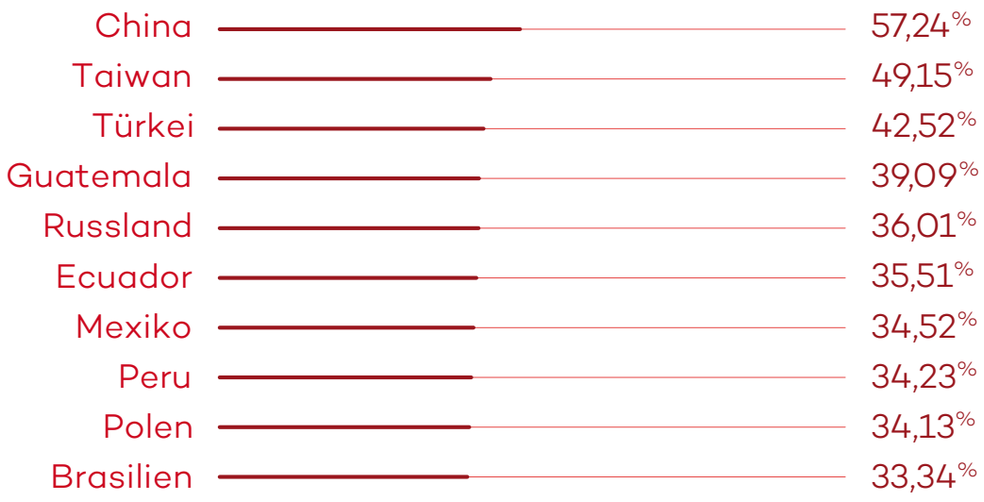
Wenn wir uns die weltweite Infektionsrate von Computern anschauen, die bei 32,13 Prozent liegt, können wir feststellen, dass sie im Vergleich zum Vorjahr gestiegen ist. Das wurde hauptsächlich durch PUPs verursacht.

Wir müssen jedoch darauf hinweisen, dass diese Zahl für Computer steht, auf denen irgend eine Art von Malware registriert wurde, was aber nicht zwangsläufig bedeutet, dass sie auch ausgeführt wurden.

Die Länder mit den höchsten Infektionsraten sind China (57,24 %), Taiwan (49,15 %) und die Türkei (42,52 %).

Es folgen die zehn Länder mit den höchsten Infektionsraten:

LÄNDER MIT DEN HÖCHSTEN INFEKTIONSRATEN IM JAHR 2015



Asien und Lateinamerika sind die Regionen mit den höchsten Infektionsraten. Andere Länder mit einer Infektionsrate über dem weltweiten Durchschnitt sind Kolumbien (33,17 %), Uruguay (32,98 %) und Spanien (32,15 %).

Wenn wir die Daten der Länder mit den niedrigsten Infektionsraten analysieren, stellen wir fest, dass neun von ihnen in Europa sind. Japan ist das einzige nichteuropäische Land in den Top Ten. Die skandinavischen Länder mit Finnland (20,32 %), Norwegen (20,51 %) und Schweden (20,88 %) führen die Rangliste an.

Es folgen die zehn Länder mit den niedrigsten Infektionsraten:

LÄNDER MIT DEN NIEDRIGSTEN INFEKTIONSRATEN IM JAHR 2015

Weitere Länder, die eine Infektionsrate unter dem weltweiten Durchschnitt verzeichneten, sind Australien (26,87 %), Frankreich (27,02 %), Portugal (27,74 %), Österreich (28,96 %), Kanada (29,03 %), die USA (29,48 %), Venezuela (30,11 %), Ungarn (30,23 %), Italien (31,84 %) und Costa Rica (32,10 %).

3. DAS JAHR AUF EINEN BLICK

3

Das Jahr auf einen Blick

Cyberkriminalität

Wenn wir die gefährlichste Cyberattacke des ersten Quartals 2015 auswählen müssten, wäre es Ransomware, und Cryptolocker im Besonderen.

Dieser Angriffstyp betrifft alle Arten von Usern, obwohl Unternehmen das bevorzugte Ziel zu sein scheinen, da sie wertvolle Informationen speichern und bereit sind, ein Lösegeld für die Rückgabe zu zahlen.

Es ist eine bekannte Tatsache, dass einige Unternehmen dieser Form der Erpressung letztendlich nicht standhalten konnten, insbesondere jene, die kein Backup-System hatten, um ihre Daten zu sichern. Im Februar wurde öffentlich bekannt gemacht, dass eine Polizeibehörde in Illinois 500 Dollar Lösegeld gezahlt hatte, um einen Computer zu entsperren, der mit Ransomware infiziert war.

Cyberkriminelle nutzen unterschiedliche Techniken, um Systeme zu infizieren und Benutzerdaten zu stehlen. Eine der gebräuchlichsten Infektionstechniken ist die Nutzung von Exploits. Das sind Programme, die Schwachstellen von Software auf dem Rechner des Opfers ausnutzen.

Im Januar wurde enthüllt, dass Internetbetrüger dabei waren, eine Schwachstelle im Flash Player aktiv auszunutzen. In diesem Fall war die Sicherheitslücke eine Zero-Day-Schwachstelle, die bis dahin unbekannt war und für die es deshalb kein Patch gab.

Flash ist ein Hauptziel für Cyberkriminelle, genauso wie Java, eine weitere Software, die oft von diesen angegriffen wird.

Wenn wir über Phishing reden, denken wir oft an E-Mails, die vorgeben von Banken oder Finanzinstituten zu kommen.

Obwohl es zutrifft, dass Phishing-Attacken auf diese Weise gestartet werden können und diese Technik in vielen Fällen noch genutzt wird, konzentrieren sich Phisher nicht länger nur auf Kunden von Banken und Online-Bezahldiensten.

Eine der „neuen" Techniken, die von Cyberkriminellen genutzt wird, ist die Verwendung von Makros in Office-Dokumenten (insbesondere Word), um die User auszutricksen und ihre PCs mit Ransomware zu infizieren. (Eigentlich handelt es sich um eine alte Technik, denn die ersten solcher Angriffe gab es bereits vor fast 20 Jahren.)

Die meisten User haben das falsche Sicherheitsgefühl, dass ein Textdokument keine Bedrohung enthält. Mit diesem Wissen und in dem Bewusstsein, dass Perimeter-Filter nichts gegen solche Dateien unternehmen, hat es einen drastischen Anstieg von Angriffen mit dieser Methode gegeben.

Der Schwachpunkt bei dieser Attacke ist, dass der User Makros aktivieren muss. Doch die Cyberkriminellen sind sich dessen sehr wohl bewusst und haben erfolgreich ein paar geniale Social Engineering Techniken entwickelt.

Ein von den PandaLabs entdecktes Beispiel war ein Word-Dokument, das ein verschwommenes Bild enthielt.

Ganz oben auf dem Dokument stand in fettgedruckten Großbuchstaben, dass das Bild aus Sicherheitsgründen verschwommen sei. Wenn die User das Bild anschauen wollten, mussten sie Makros aktivieren. Ein Pfeil zeigte auf die Schaltfläche, die angeklickt werden sollte. Nach der Aktivierung konnten sie ein klares Bild sehen, doch gleichzeitig wurde der Rechner mit einer Art des Cryptolockers infiziert.

Eine andere Ransomware, die sich als sehr beliebt erwiesen hat, ist eine, die Bilder von der beliebten Fernsehserie „Breaking Bad" nutzte. Besonders populär war sie in Australien, obwohl man sie zuvor auch schon in anderen Ländern gesehen hatte.

Im Januar startete eine Hackergruppe eine Phishing-Attacke, bei der Apple imitiert wurde. Die schädliche Nachricht kam vom „Apple-Support" und nutzte eine wiederkehrende Taktik: Es wurde auf ein angebliches Sicherheitsproblem hingewiesen, um das Opfer zu verängstigen. „Ihre Apple-ID wurde gesperrt." In der Nachricht wurde der User darüber informiert, dass eine unbefugte Person versucht hätte, auf seinen Account zuzugreifen, und dass infolgedessen das Konto deaktiviert worden sei. Die E-Mail enthielt einen Link, der den Benutzer zu einer Seite führte, die das Erscheinungsbild der Apple-Seite hatte und auf der viele Informationen abgefragt wurden: vollständiger Name, Adresse, Telefonnummer, Kreditkartendaten usw.

Das US-amerikanische Unternehmen Anthem bestätigte im Februar, Opfer eines Angriffs geworden zu sein, bei dem die Daten von 80 Millionen Kunden gestohlen wurden. In diesem Fall gelang es den Angreifern mithilfe eines gestohlenen Namens und Passwortes, auf eine der Datenbanken des Unternehmens zuzugreifen. Man schätzt, dass die Attacke Anthem mehr als 100 Millionen Dollar kosten könnte.

Im März schickte das US-Unternehmen Slack all seinen Usern eine Nachricht, um ihnen mitzuteilen, dass man einen nicht autorisierten Zugriff auf eine Datenbank entdeckt hätte, in der Informationen über Benutzerprofile gespeichert werden. Obwohl

keine sensiblen Daten gestohlen wurden (Slack hat seinen Usern tatsächlich mitgeteilt, dass es nicht nötig sei, die Zugangsdaten zu ändern.), aktivierte das Unternehmen sofort ein Zwei-Faktor-Authentifizierungssystem und forderte die Nutzer auf, diese Sicherheitsfunktion zu nutzen, um den Schutz zu erhöhen.

Der Billigflieger Ryanair wurde Opfer einer Attacke, bei der das Unternehmen 5 Millionen Dollar verlor. Obwohl keine Einzelheiten darüber preisgegeben wurden, wie die Täter den Angriff ausgeführt haben, ist bekannt, dass er die Folge einer Überweisung an eine chinesische Bank war. Das Unternehmen meldete das Verbrechen und gab bekannt, dass es das gestohlene Geld einfrieren konnte und zuversichtlich sei, es bald zurückzuerhalten.

CareFirst BlueCross BlueShield, eine Krankenversicherung, wurde das Opfer einer Cyberattacke, bei der die Daten von 1,1 Millionen Kunden gestohlen wurden.

Mit jedem Tag nimmt die Bedrohung zu, von diesen Kriminellen angegriffen zu werden. Und dieses sind nur einige Beispiele für Hunderte von Datendiebstählen, die sich weltweit ereignen.

Bei einem Angriff wurden der Internet-Kontaktbörse Adult FriendFinder private Nutzerdaten gestohlen. Die Angreifer boten die gestohlenen Informationen demjenigen an, der als Erster bereit war, 70 Bitcoins zu zahlen. Das entsprach zu der Zeit etwa 17.000 Dollar. Kurz darauf wurde die vollständige Datenbank im Internet veröffentlicht.

LastPass, ein führendes Unternehmen für Passwortverwaltung, war ebenfalls Opfer eines Datendiebstahls. Glücklicherweise sieht es so aus, als hätten die Angreifer keine sensiblen Passwortinformationen in die Hände bekommen, sondern nur die Hash-Codes für die Master-Passwörter der User. Die Komplexität dieser Hashes (durcheinandergewürfelt und schwer zu verstehen) erschwert es den Cyberkriminellen erheblich, das echte Passwort zu bekommen. Trotzdem sollten Sie das Kennwort ändern, wenn Sie ein schwaches nutzen.

Das Hard Rock Hotel und Casino in Las Vegas gab bekannt, dass die Sicherheit in einem Zeitraum von acht Monaten verletzt worden sei. Die Angreifer waren in der Lage, Kundendaten wie Namen, Kredit- und Debitkartennummern sowie die Kartenprüfwerte zu stehlen. Davon betroffen waren die Kunden, die ihre Karten in den Restaurants, Bars und Geschäften des Hotelkomplexes nutzten. Diejenigen, die im Hotel oder Casino Einkäufe getätigt haben, waren hingegen nicht betroffen. Dieser Angriff erinnert an andere, die wir in der Vergangenheit erlebt haben (Target, Home Depot, UPS, Neiman Marcus) und bei denen Kassenterminals das Ziel waren, um die Kreditkarteninformationen der Kunden zu stehlen.

Es gab Gerüchte, dass Uber das Opfer einer Attacke gewesen sei, nachdem man festgestellt hatte, dass Nutzer des Services ungewöhnliche Aktivitäten in ihren Accounts beobachtet hatten. Allerdings sieht es so aus, als sei dies ein Fall von Phishing gewesen, bei dem die User ihre IDs preisgegeben haben, nachdem sie von den Angreifern überlistet worden waren.

Ende Juni strandeten 1.400 Passagiere der polnischen Fluggesellschaft LOT am Chopin-Flughafen Warschau, nachdem das Bodensystem, das zur Erstellung der Flugpläne dient, gehackt worden war.

Einer der größten Angriffe, die im dritten Quartal stattfanden, war zweifellos der auf Ashley Madison. Die als Impact Team bekannten Angreifer veröffentlichten eine Mitteilung auf ihrer Webseite, in der sie die Schließung der Dating-Agentur forderten oder sie würden alle Informationen veröffentlichen, die sie gestohlen haben.

Kurz darauf veröffentlichten sie eine Flut von Informationen (10 GB), da das amerikanische Unternehmen ihren Forderungen nicht nachgekommen war.

Zu den preisgegebenen Informationen gehörten die privaten Daten von 37 Millionen Kunden, abgeschlossene Geschäfte, E-Mail-Adressen, sexuelle Vorlieben usw. Darüber hinaus wurden sogar interne Dokumente veröffentlicht, die das Unternehmen betreffen.

In diesem Quartal gab es auch eine Menge neuer Schwachstellen, die von Cyberkriminellen ausgenutzt wurden, um Zugang zu ihren Opfern zu erlangen. Abgesehen von den typischen Flash- oder Java-Angriffen, erlebte auch das Betriebssystem Apple Mac OS X einige Störfälle. Die erste Schwachstelle, die von Stefan Esser entdeckt wurde, ermöglichte den Zugriff auf das Stammverzeichnis und die Nutzung von Adware, um Macs anzugreifen.

Die zweite Sicherheitslücke wurde von Forschern bei MyK entdeckt. Sie bestand aus einer Schwachstelle im Passwort-Verwaltungssystem, die dem Angreifer ermöglichte, alle gespeicherten Informationen zu erhalten.

Eine der Angriffsmethoden, die sich zunehmender Beliebtheit erfreut, besteht darin, Router-Verbindungen zu unterbrechen, sowohl in Haushalten als auch in Unternehmen. Dadurch erhalten die Angreifer Kontrolle über die Router.

Man hat entdeckt, dass Router in Unternehmen, wie zum Beispiel ASUS, DIGICOM, Observa Telecom, PLDT und ZTE, vordefinierte Informationen in ihren Zugangscodes enthielten. Dies ermöglichte den Angreifern, die Kontrolle über die Router zu übernehmen, ohne das Grundstück betreten zu müssen. Beispiele dafür gab es zu Weihnachten, als Cyberkriminelle DDoS-Attacken gegen Xbox Live und PSN einsetzten.

Die Tage von Adobe Flash, bekannt für seine zahlreichen Sicherheitsprobleme, sind gezählt. Sowohl iOS als auch Android erlauben nicht mehr, dass es auf ihren Betriebssystemen läuft. Nun ist es an Google, sein Schicksal zu besiegeln, indem es Adobe Flash aus seinem Chrome Browser verbannt. Amazon hat ebenfalls angekündigt, dass es keine Werbeanzeigen mehr auf seinen Webseiten zulässt, die auf diesem Format basieren.

Das FBI hat fünf Personen festgenommen, die in das Hacking von JPMorgan im Jahre 2014 verwickelt waren. Bei diesem Angriff gelang es den Hackern, die Anmeldedaten eines Angestellten zu nutzen, um Zugriff auf 90 Firmenserver zu erhalten und Informationen von 76 Millionen Personen sowie 7 Millionen Unternehmen zu stehlen, die alle Kunden der Firma waren.

Microsoft hat beschlossen, die Sicherheit seiner Produkte und Lösungen zu verbessern, indem es die Belohnung verdoppelt hat, die es für User gibt, denen es gelingt, neue kritische Fehler in seinen Lösungen ausfindig zu machen. Der Betrag wurde von 50.000 Dollar auf 100.000 Dollar erhöht.

Obwohl solche Belohnungen bei IT-Firmen zunehmend beliebter werden, sind sie noch nicht bis in alle Bereiche vorgedrungen. Dennoch bieten immer mehr Unternehmen ihren Ermittlern solche Anreize, in der Hoffnung, dass man sie zuerst informiert, statt die Daten an eine externe Quelle zu verkaufen.

United Airlines, die Flugmeilen als Belohnung anbieten, haben beschlossen, den Ermittlern bis zu 1 Million Flugmeilen anzubieten, die Fehler entdecken und diese melden.

Auch das FBI bietet Anreize, allerdings für diejenigen, die Informationen über mutmaßliche Kriminelle liefern können. Die höchste gebotene Belohnung sind 3 Millionen Dollar für jeden, der dabei helfen kann Evgeniy Mikhailovich Bogachev festzunehmen, den führenden Kopf hinter dem Netzwerk von Gameover ZeuS Bots.

Hotelketten sind ebenfalls zum Ziel von Cyberkriminellen geworden. Abgesehen von dem Angriff auf das Hard Rock Hotel & Casino in Las Vegas waren auch andere betroffen: die Hotelketten Hilton und Starwood (Westin, Sheraton usw.), das Las Vegas Sands Casino, die Trump Hotels, das Mandarin Oriental, das FireKeepers Casino und Hotel usw. Das ist eine lange Liste, die zweifelsohne noch länger werden wird, da Hotels Informationen über Millionen von Kreditkarten besitzen. Es gibt kaum ein Hotel, das seine Gäste nicht um Zahlung per Kreditkarte bittet, deshalb nehmen die Angriffe auf Kassenterminals (POS) zu. (Wir wissen, dass dies in der Vergangenheit für Kriminelle gut funktioniert hat. Ein Beispiel dafür ist der Fall von Target, wo sie mithilfe von Malware auf dem Terminal die Informationen von 46 Millionen Kreditkarten gestohlen hatten.)

Der Spielzeuganbieter VTech erlitt eine Sicherheitsverletzung, von der die Daten von 4,98 Millionen Eltern und 6,37 Millionen Kindern betroffen waren. Einige Wochen nach diesem Angriff verhaftete jedoch die Polizei in Großbritannien einen Verdächtigen, der mit der Attacke in Verbindung stehen soll.

Viele Unternehmen und Webseiten hatten unter ähnlichen Angriffen zu leiden, wie beispielsweise T-Mobile. Dort wurden die Daten von 15 Millionen Kunden gestohlen und bei sanriotown.com die von weiteren 3,3 Millionen Kunden.

Soziale Medien

Als US-Präsident Barack Obama im Januar eine Reihe von Maßnahmen zur Bekämpfung von Cyberkriminalität ankündigte, hackte zur selben Zeit eine Gruppe, die behauptete ISIS zu sein, die Social Media Accounts des Pentagons.

Außerdem möchten wir die Aufmerksamkeit auf den derzeit gängigsten Facebook-Betrug lenken: gefälschte Posts, die Gutscheine als Werbegeschenke von beliebten Firmen ankündigen. Im Januar erfanden Betrüger ein Facebook-Event und versprachen 430 Gutscheine von Zara im Wert von 500 Dollar. Um daran teilzunehmen, sollten die User einfach „Danke Zara“ auf ihrer Facebook-Pinnwand posten und 50 ihrer Kontakte einladen, dasselbe zu tun. In nur wenigen Stunden hatten sich über 5.000 Personen an dieser Aktion beteiligt und mehr als 124.000 Einladungen versendet.

Alle User-Verbindungen zu den Servern von Facebook, einschließlich der gesendeten und empfangenen Nachrichten, werden über das sichere HTTPS-Protokoll übertragen. Da dies noch nicht genug war, richtete der Social Media Gigant einen Service im Tor-Netzwerk ein, damit der Online-Datenschutz der User noch besser gewährleistet werden kann. Neben den Verbindungen, die von den Usern über den eigenen Service hergestellt werden, gibt es jedoch andere indirekte Arten der Kommunikation, die auf Facebook per Mail ausgeführt werden. Das sind Benachrichtigungen, die Sie erhalten, wenn Ihnen ein Freund eine private Nachricht gesendet hat. (Es sei denn, Sie haben diese Funktion deaktiviert.)

Da die Sicherheit dieser Mitteilungen gefährdet war, hat Facebook angekündigt, dass von nun an alle User – wenn sie wollen – diese geschützt durch die beliebte Verschlüsselungssoftware Pretty Good Privacy (PGP) erhalten.

PGP versteckt die Mails vor potenziellen Eindringlingen mit einem System, das auf einem Public Key (den der Absender der Nachricht haben muss) und einem Private Key (den nur der Empfänger haben muss) basiert.

Der Konfigurationsprozess ist einfach – greifen Sie auf Ihr Profil zu, gehen Sie in den Bereich „Informationen“ und dann zu „Kontakt und Basisinformationen“. Dort können Sie Ihren Public PGP Key eingeben. (Wenn Sie nicht wissen, was das ist oder wie Sie ihn bekommen, können Sie die Anleitung lesen.) Er wird dann in Ihrem Profil sichtbar und für jeden verfügbar, der Ihnen eine verschlüsselte Mail schicken möchte.

Unterhalb der Grafik gibt es ein Kästchen, in das Sie ein Häkchen setzen müssen, wenn Sie wollen, dass alle Mails, die Facebook Ihnen sendet, in diese neue Sicherheitsmaßnahme integriert werden. Es ist wichtig, sich den Key zu merken, den Sie nutzen, um Ihre Mails mit GPG zu schützen. Wenn Sie ihn vergessen, können Sie Ihre Benachrichtigungen nicht lesen und Sie könnten sogar den Zugriff auf Ihren Account im sozialen Netzwerk verlieren.

WhatsApp ist eine beliebte Art, um User anzulocken und zu versuchen, sie zu infizieren. Wir haben einen Schwindel entdeckt, bei dem sie versuchen, die User mit einer Instant Messaging Applikation, namens WhatsApp Trendy Blue, hereinzulegen. Sie gibt sich als „neue Version“ der Anwendung mit zusätzlichen Features aus. In Wirklichkeit ist das einzige, was sie tut, den User bei einem teuren Abrechnungsservice anzumelden.

Dieses betrügerische Programm fordert Sie außerdem dazu auf, mindestens 10 Ihrer Kontakte einzuladen, sich für seine Services anzumelden.

Facebook kündigte an, dass sie einen „Unlike“-Button entwickeln wollen, und wie erwartet waren Cyberkriminelle die ersten, die uns diese Option anboten. In nur wenigen Stunden gab es eine Vielzahl von verschiedenen Betrügereien, die den angeblich neuen Button anboten. Jede einzelne zielte darauf ab, vertrauliche Informationen von den Opfern zu stehlen.

Mobiles

Das Jahr begann mit einer Bedrohung, die uns an alte E-Mail- und Instant-Messaging-Würmer erinnerte, praktischerweise modifiziert, um SMS-Nachrichten nutzen zu können.

Der Angriff beginnt, wenn das Opfer eine SMS mit einem Link zu einem angeblichen Foto von sich erhält. Das Problem mit dem Link ist, dass er tatsächlich eine APK-Datei (Android Application Package) herunterlädt. Wenn das Opfer diese installiert, sendet die schädliche App eine SMS, genau wie die empfangene, an alle Kontakte des Betroffenen.

Fujitsu hat in Zusammenarbeit mit dem japanischen Betreiber NTT Docomo Arrows NX F-04G herausgebracht, das auf Android basiert und das erste Android Mobilgerät ist, das einen Iris-Scanner als Teil seiner Sicherheitsfunktionen enthält. Diese Methode ist viel sicherer als die mit Fingerabdruck, die bei seinen Konkurrenten wie Apples iPhone 6 oder Samsungs Galaxy S6 beliebt ist.

Im Juni entdeckten wir eine Phishing-Aktion, die gegen Android-Entwickler gerichtet war, die ihre Kreationen in Google Play veröffentlichten, dem offiziellen App Store des Betriebssystems. Die Nachricht wurde von einer Instanz mit dem Namen „Play Developer Support“ verschickt und trug den Titel „Update Your Account Information“. Wenn man den Link anklickte, wurde man zu einer Webseite geleitet, die wie Google aussah. Dort wurde man nach seinen Daten gefragt.

Phishing-Attacken dienen dazu, die Identität des Users und seine persönlichen Informationen zu stehlen. Deshalb sind solche Angriffe auf Finanzinstitute und jede Art von Bezahlplattform so beliebt.

Dieser Fall unterscheidet sich jedoch von anderen, da die Kriminellen nicht die Bankkonten der Opfer plündern wollten, sondern deren Daten nutzten, um Malware über den Google Play Store zu verteilen.

Der besorgniserregendste Aspekt von all dem ist, wie einfach es für Kriminelle sein könnte, den gesamten Prozess zu automatisieren.

Alles, was sie tun müssen, ist Folgendes:

- Einen Spider oder Crawler erstellen (Es gibt zahlreiche Open Source Projekte, die ihnen dabei helfen), um Informationen von allen Apps herunterzuladen, die auf Google Play veröffentlicht werden.
- Die Informationen analysieren, um die E-Mail-Adressen der verschiedenen Entwickler zu bekommen.
- Eine maßgeschneiderte Phishing-Aktion senden, bei der sogar die Webseite auf den Entwickler zugeschnitten ist. Dies lässt den Trick sogar noch plausibler erscheinen und hilft dabei, eine höhere „Konversionsrate“ zu erzielen.
- Weil der Angreifer Informationen über alle Apps hat, die jeder Entwickler veröffentlicht hat, kann er ein System entwickeln, das ihn jedes Mal informiert, wenn ein Herausgeber einer beliebten App (Millionen von Downloads) in die Falle getappt ist.

Angesichts dessen wäre die einfachste und am wenigsten aufwändige Attacke die Veröffentlichung von Apps über diesen Account. Stellen Sie sich vor, dass es jemandem gelingt, die Daten eines der Entwickler von Candy Crush zu stehlen und Candy Crush 2 über denselben Account zu veröffentlichen. Wenn die Angreifer clever sind und eine Möglichkeit finden, die App zu modifizieren, ohne den Private Key (den man nicht mit den gestohlenen ID-Informationen erhalten kann) zu nutzen, dann könnten sie jede beliebige Applikation veröffentlichen und aktualisieren.

Stellen Sie sich beim genannten Beispiel vor, dass die Angreifer eine aktualisierte Version von Candy Crush entwickeln, die einen Trojaner enthält. – Millionen Menschen würden sie herunterladen und installieren, ohne zu bemerken, dass sie in Gefahr sind.

Google hat ein neues Programm mit dem Namen Android Security Awards entwickelt, dass diejenigen entlohnt, die neue Schwachstellen bei Androids Sicherheit suchen und finden.

Die gezahlte Summe hängt vom Ausmaß der Sicherheitslücke ab: 2000 Dollar für eine kritische, 1000 Dollar für eine große und 500 Dollar für eine mittelschwere Schwachstelle. Je nach der Schwere des Problems und den gefundenen Einzelheiten könnte sich der Betrag auf bis zu 38.000 Dollar summieren.

Im Juli entdeckte Zimperium eine große Schwachstelle bei Android, die 950 Millionen Geräte mit diesem Betriebssystem betraf. Das Problem war nicht nur die Menge an Mobiltelefonen, Tablets oder anderen Geräten, die betroffen waren, sondern viel mehr, wie einfach es war, sie aus der Ferne zu gefährden.

Durch das einfache Senden einer schädlichen MMS ist es möglich, die Kontrolle über jedes Telefon zu übernehmen, wenn man die Nummer des Opfers kennt. Es ist nicht einmal erforderlich, die MMS zu öffnen, da Android Bilder automatisch verarbeitet, d. h., dass das Empfangen der MMS ausreichte, um den Schaden zu verursachen.

Obwohl das Problem behoben wurde, bedeutet die große Anzahl von Herstellern und Versionen des Betriebssystems, dass es immer noch Varianten geben könnte, die noch nicht mit den neuesten Sicherheitsmaßnahmen aktualisiert worden sind.

Google hat seitdem eine große Anzahl von Herstellern (Sony, LG, Motorola usw.) dazu gebracht, die neuesten Updates einzubeziehen. Samsung kündigte an, dass sie ihren Kunden monatliche Updates anbieten würden, um den ständig auftauchenden neuen Schwachstellen voraus zu sein.

Tatsächlich veröffentlichten kurz darauf zwei Forscher von IBMs XForce ein weiteres Sicherheitsproblem, das es einem Angreifer ermöglichte, eine vertrauenswürdige App durch eine schädliche zu ersetzen. Diese wiederum erlaubte es dem Angreifer, auf die Berechtigungssteuerung der ersetzten App zuzugreifen. Google aktualisierte daraufhin seine Software, um dieses Sicherheitsproblem zu beseitigen.

Inzwischen sind wir an Angriffe auf PCs mittels Ransomware gewöhnt. Doch nun richten sie sich zunehmend auch gegen Android. In den vergangenen drei Monaten haben sich diese Attacken durch ihre Originalität und Einfachheit ausgezeichnet. Eine schädliche App ändert die PIN des Gerätes und verlangt ein Lösegeld von 500 Dollar.

Die Nutzer unseres Antivirus für Android können beispielsweise den PIN-Code ihres Handys über ihre Webkonsole ändern und so diese Angriffsart unwirksam machen und 500 Dollar sparen. Apples Betriebssystem hatte in diesen Monaten ebenfalls unter verschiedenen Angriffen zu leiden.

Das Unternehmen Appthority hat eine Schwachstelle mit dem Namen Quicksand entdeckt, die Firmen betrifft, die MDM-Services (Mobile Device Management) nutzen, und vertrauliche Unternehmensdaten gefährden könnte. Apple hat diese Sicherheitslücke mit seiner neuen Version von iOS 8.4.1 behoben.

Eine weitere Schwachstelle, die beseitigt wurde, ist ImsOmnia. Sie ermöglichte es einer schädlichen App, die Beschränkungen von Apple zu umgehen und die Aktivierung des Mikrofons oder der Kamera zu erlauben, und so den Benutzer auszuspionieren.

Apple musste aufgrund einer Attacke, bekannt als XcodeGhost, eine Reihe von Applikationen aus seinem Apple Store entfernen. Die Angreifer veröffentlichten eine modifizierte Version der Software, die Urheber für die Entwicklung von Apps für iOS nutzen. So brachten sie die Entwickler dazu, unwissentlich schädliche Features in ihre Apps zu integrieren.

Mit einem anderen Angriff, der sich gegen Apple-User richtete, gelang es Cyberkriminellen, die iCloud-Anmeldedaten von mehr als 225.000 Nutzern zu stehlen. Die Attacke betraf User, die zuvor ihre Geräte per Jailbreak freigeschaltet hatten, damit sie Apps installieren können, ohne den offiziellen App Store nutzen zu müssen. Doch dies führte dazu, dass die in iOS installierten Sicherheitskontrollen gelöscht wurden.

Internet der Dinge

Im Juli veröffentlichte HP Fortify die Ergebnisse einer Studie über Smartwatches, die feststellte, dass 100 Prozent der analysierten Geräte anfällig für Angriffe waren, und Aufschluss über die Hauptprobleme von Smartwatches gab.

Beispielsweise bot keine der Smartwatches eine Zwei-Faktor-Authentifizierung an, wenn sie mit einem Mobilgerät verbunden wurde, und falsche Passwörter konnten mehrfach eingegeben werden.

Die Sicherheitsforscher Charlie Miller und Chris Valasek demonstrierten im Juli etwas, das die Welt in einen Schock versetzte.

WIRED

Sie überredeten Andy Greenberg, einen Journalisten von Wired, einen Jeep Cherokee zu fahren, während die beiden sich von zu Hause aus in das Auto hackten.

Anfangs übernahmen sie die Kontrolle über Dinge wie die Klimaanlage im Auto. Sie aktivierten die Scheibenwischer, wechselten den Radiosender und spielten mit der Lautstärke herum... Schließlich übernahmen sie die volle Kontrolle über das Auto, einschließlich seines Bremssystems.

Sie hatten Monate mit der Arbeit an diesem Angriff verbracht und sogar den Hersteller vor dem Test informiert, in der Hoffnung dieser würde neue Sicherheitsupdates installieren, um die Schwachstelle zu beheben. Das Paar gab weitere Informationen darüber bekannt, wie sie die Tests durchgeführt haben, und zwar in einem Interview auf der BlackHat-Konferenz im August.

Land Rover wurde im Juli über einen Fehler in der Software informiert, der 65.000 Fahrzeuge betraf, die seit 2013 verkauft wurden. Aufgrund der Schwachstelle konnte man die Türen über externe Quellen öffnen. Kevin Mahaffey und Marc Rogers, zwei Forscher, zeigten auf der BlackHat-Konferenz, wie man einen Tesla Modell S hackt. Obwohl sie physischen Zugriff auf das Auto benötigten, entdeckten sie 6 neue Schwachstellen, mit denen sie den Motor bei geringen Geschwindigkeiten abschalten konnten. Der Hersteller hat daraufhin Maßnahmen ergriffen, um dieses Problem zu beheben.

Hiroyuki Inoue, ein außerordentlicher Professor an der Graduate School of Information Sciences in Hiroshima, führte ein Experiment durch, bei dem er einen Toyota Corolla mit dem Internet verband und ihn hacken konnte. Er war in der Lage, unter anderem aus der Ferne die Fenster des Autos zu bedienen, den Geschwindigkeitsbegrenzer zu manipulieren und das Gaspedal zu blockieren.

Obwohl dieses Experiment mit einem Auto, das mit dem Internet verbunden war, durchgeführt wurde – etwas, mit dem das Modell nicht ausgestattet ist – ließ es doch die Alarmglocken bei den Herstellern schrillen.

Cyberkrieg

Zum ersten Mal verhängten die Vereinigten Staaten Sanktionen gegen ein Land als Reaktion auf eine Cyberattacke.

Bei dem Land handelt es sich um Nordkorea und die Sanktionen waren eine Reaktion auf das Hacken von Sony im Dezember 2014. Dabei ging es um die Komödie „The Interview“, in dem ein paar Journalisten von der CIA angewiesen werden, das nordkoreanische Staatsoberhaupt zu ermorden.

Außerdem kamen neue Enthüllungen aus den von Edward Snowden an die Presse geleakten Dokumenten ans Licht. Im Januar veröffentlichte das deutsche Magazin „Der Spiegel“, dass China viele Terabytes an Daten über den Kampf-Jet F-35 gestohlen hätte, einschließlich der Informationen über das Radar-Design, Motor-Schaltpläne usw.

Ben Rhodes, stellvertretender Berater für nationale Sicherheit und strategische Kommunikation des US-Präsidenten Barack Obama, gab bekannt, dass das Weiße Haus Opfer einer IT-Attacke geworden sei. In einem Interview mit CNN bestätigte Rhodes, dass die Angreifer unerlaubten Zugriff auf ein nicht geheimes Computersystem erlangt und äußerst wichtige Informationen gestohlen hätten, obgleich das geheime System nicht gehackt worden sei. Obwohl Rhodes weder enthüllen wollte, ob der Angriff von russischen Hackern ausgeführt worden sei, noch wann er sich ereignet hätte, vermittelte er den Eindruck, dass er nicht erst vor wenigen Tagen stattgefunden habe. Ohne weitere Informationen preiszugeben, erklärte Rhodes, dass man bereits „eine Reihe von Sicherheitsmaßnahmen“ unternommen hätte, „um den verursachten Schaden zu beurteilen und zu minimieren.“

Im Juni fanden wir heraus, dass das Office of Personnel Management (OPM), das Amt für Personalverwaltung der Vereinigten Staaten, angegriffen wurde und vertrauliche Daten über mindestens vier Millionen Mitarbeiter im öffentlichen Dienst gestohlen wurden. Diese Attacke fand in etwa zur gleichen Zeit statt wie der Angriff auf das Weiße Haus. Die Angriffe scheinen jedoch nicht zusammenzuhängen, wenn man berücksichtigt, dass letzterer mit chinesischen Hackern in Verbindung gebracht wird, obwohl die US-Regierung dies nicht offiziell bestätigt hat.

ISIS-Sympathisanten griffen den französischen Fernsehsender TV5MONDE an und konnten seine Übertragung sabotieren. Darüber hinaus übernahmen sie auch die Facebook-Seite sowie die Webseite des Senders.

Der Deutsche Bundestag war Opfer eines Angriffs, bei dem es Cyberkriminellen gelang, mehrere Computer zu infiltrieren und Informationen zu stehlen. Man glaubt, dass der Angriff aus Russland kam, aber es ist schwierig zu beweisen, wer

genau dahintersteckte. Wir wissen bereits, dass die NSA eine modifizierte Version von Stuxnet benutzt hat, um zu versuchen, ein Atomprogramm der Nordkoreaner zu sabotieren. Obwohl sie bei diesem Versuch nicht erfolgreich waren, ist anzumerken, dass es ihnen mit Stuxnet gelungen ist, vor einigen Jahren zumindest 1.000 Zentrifugen für Uran in einem Werk in Natanz, Iran, zu zerstören.

Hacking Team ist ein Unternehmen, das dafür bekannt ist, Tools für Cyberspionage und Cyberattacken an eine Vielzahl von Regierungen weltweit zu liefern.

Im Juli war es Opfer einer massiven Attacke, bei der alle Arten von Daten gestohlen wurden. Der Angriff wurde über den Twitter-Account von Hacking Team bekannt gemacht, der ebenfalls von den Angreifern übernommen worden war. Sie änderten den Namen des Accounts in „Hacked Team“ und hängten einen Link zum Download der gesamten gestohlenen Informationen an:

Sie veröffentlichten Kundenlisten (Polizei und Geheimdienste verschiedener Länder, von den USA bis Usbekistan). Außerdem machten sie ein Unternehmenszertifikat öffentlich, das von Hacking Team genutzt wurde sowie Passwörter für ihre am meisten geschützten Systeme, Listen von Produkten, die sie verkauft hatten, Quellcodes für ihre Applikationen, Finanzdaten usw. Sie veröffentlichten sogar eine Webseite mit einer Suchfunktion, mit der man die von Hacking Team gespeicherten E-Mail-Adressen durchsuchen konnte.

Einige Tage später wurde dank der von Hacking Team gestohlenen Informationen ein Zero-Day-Exploit bei Adobe Flash entdeckt.

James Comey, Direktor des FBI, sprach auf einem Sicherheitsforum und berichtete, wie sie entdeckt hatten, dass Terroristen ein wachsendes Interesse an Strategien zum Starten von cyberterroristischen Angriffen auf die Vereinigten Staaten haben.

Er präzisierte die Angriffsarten nicht und sagte, dass die Terroristen noch in der Planungsphase seien und herausfinden wollten, wie effektiv sie sein könnten.

Am 25. Juli gelang es russischen Hackern, auf ein nicht geheimes E-Mail-System des Pentagons zuzugreifen. Offizielle Quellen gaben bekannt, dass es eine ausgereifte Attacke gewesen sei und dass sie sich sicher seien, dass eine Regierung dahinterstecke.

Im September veröffentlichten Forscher des DGI eine Studie über die Einheit 78020 der chinesischen Armee, in der sie zeigten, dass diese hinter der als Naikon bekannten Gruppe steckte. Naikon war für verschiedene militärische, wirtschaftliche und diplomatische Spionageangriffe in ihrer Region verantwortlich. Zu den Opfern gehörten Kambodscha, Indonesien, Laos, Malaysia, Myanmar, Nepal, die Philippinen, Singapur, Thailand, Vietnam, das Entwicklungsprogramm der Vereinten Nationen sowie der Verband Südostasiatischer Nationen.

Anonymous startete eine Kampagne gegen ISIS, bei der Webseiten und Social Media Accounts von Tausenden seiner Mitglieder gehackt und veröffentlicht wurden.

4. TRENDS FÜR 2016

4 Trends für 2016

Im Folgenden werfen wir einen Blick auf Dinge, von denen wir denken, dass sie die wichtigsten IT-Sicherheitstrends für 2016 sind.

1.- Exploit Kits

Sie werden weiterhin das bevorzugte Tool von Cyberkriminellen sein, da diese danach trachten, massive Infektionen zu verursachen. Exploit Kits können auf dem Schwarzmarkt gekauft werden und erhalten Updates, die es den Angreifern ermöglichen, mithilfe neuer Angriffsmethoden neue Opfer zu finden. Viele Sicherheitslösungen sind immer noch nicht in der Lage, diese Art von Angriffen effektiv zu bekämpfen. Das bedeutet, dass die Erfolgsrate für die Kriminellen hoch ist.

2.- Malware

Die Anzahl neuer Malware-Exemplare wächst stetig. Obwohl die Mehrheit der Samples weiterhin PE-Dateien (Portable Executable) sein werden, denken wir, dass es ein Wachstum von Nicht-PE-Malware, hauptsächlich von Scripts, geben wird. Es wird nicht einfach nur das bekannte Javascript sein, sondern vielmehr wird es einen Anstieg bei der Nutzung und dem Missbrauch von Powershell geben, einem Tool, das standardmäßig mit Windows 10 geliefert wird und das Starten aller Arten von Scripts ermöglicht. Es wird sich selbst mit bekannten Angriffen wie Fileless Attacks verbinden. Der schädliche Code befindet sich hierbei nicht in einer physikalischen Datei auf dem Computer, sondern ist ein Parameter bei der Ausführung eines Befehls oder ein Eintrag im Register, das das auszuführende Script enthält.

3.- Direkte Angriffe

Es wird eine Zunahme von direkten Angriffen geben. Die Verwendung von Rootkit-Techniken wird sich verschärfen. Mit diesen Techniken kann sich der Angriff den Blicken des Betriebssystems und der Sicherheitslösungen entziehen. Unternehmen müssen unbedingt Sicherheitsmaßnahmen ergreifen, um vor diesen Attacken geschützt zu sein, da sie erheblichen Schaden anrichten können, sowohl finanziell als auch in Bezug auf den Ruf der Firma. Vergessen Sie nicht, dass diese Angriffe den Zweck haben, nicht nur vertrauliche Firmendaten zu stehlen (Finanzdaten, strategische Pläne usw.), sondern auch Kundendaten.

4.- Malware für Android

Malware für Mobilgeräte wird zunehmen, insbesondere für Android, da es das beliebteste Betriebssystem auf dem Markt ist. Wir werden erleben, dass mehr Bedrohungen das Gerät rooten werden. Das bedeutet, dass es für Antiviren nahezu unmöglich ist, diese Malware zu eliminieren, es sei denn, sie wurden bereits vom Werk installiert.

5.- Mobile Bezahlsysteme

Es ist noch nicht klar, ob 2016 das Jahr sein wird, in dem diese Plattformen wirklich populär werden. Was wir jedoch wissen, ist, dass ihre Verwendung zunehmen wird und dass sie zum Ziel für Cyberkriminelle werden, da sie eine direkte Möglichkeit zum Stehlen von Geld bieten. Wenn eine der Plattformen den Durchbruch schafft und Beliebtheit erlangt, wird sie der Spitzenkandidat für Angreifer werden, die nach Schwachstellen suchen, die sie in diesem System missbrauchen können.

6.- Internet der Dinge

Wir wissen, dass 2016 nicht das Jahr des Internets der Dinge sein wird. Doch es werden immer mehr Geräte an das Internet angeschlossen und so werden wir viele Tests erleben, die zeigen, wie verschiedene Angriffe ausgeführt werden können. 2015 haben wir bereits viele dieser Tests gesehen, wie die bei automobiler Software, mit der Autos während der Fahrt ferngesteuert werden können.

7.- Wichtige Infrastruktur

Es wird kein Ziel für normale Cyberkriminelle sein, aber auf dem Gebiet des Cyberkrieges wird die Macht, wichtige Infrastrukturen eines anderen Landes aus der Ferne zu sabotieren, so sehr geschätzt, dass die Geheimdienste der mächtigsten Staaten der Welt versuchen werden, sie zu erlangen. Um diese Art von Angriff auszuführen, benötigt man viel Geld und eine umfangreiche Planung, wie das Beispiel von Stuxnet gezeigt hat.

8.- Threat Intelligence für Unternehmen

Die zunehmende Anzahl und Komplexität von Angriffen verändert die Nutzung von Informationen und ebenso die Art und Weise, wie diese geteilt werden. Obwohl Firmen, die Sicherheitslösungen und -services anbieten, gewöhnlich Informationen teilen, um ihre Kunden besser zu schützen, wird sich das System drastisch verändern. Wir werden große Unternehmen haben, die ihren Sicherheitsanbieter auffordern werden, ihnen alle Informationen zu geben, während sie gleichzeitig alle Daten sammeln werden, die sich in ihren Netzwerken befinden, und diese mit anderen Firmen teilen.

5. FAZIT

5 Fazit

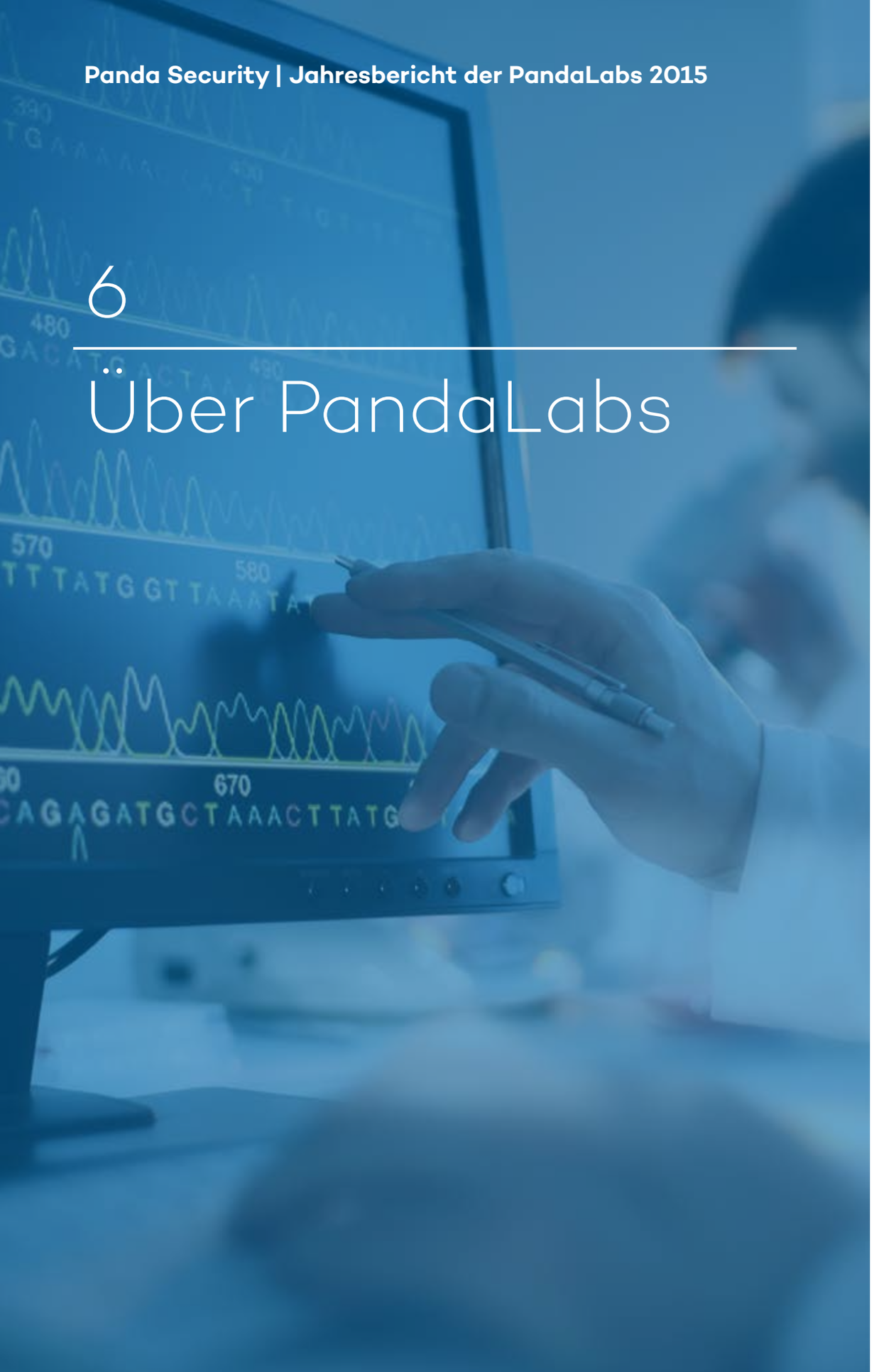
2015 war ein schwieriges Jahr, in dem Angriffe in einem nie zuvor gesehenen Maße zugenommen haben. Die Wahrheit ist, dass 2016 noch schwieriger werden wird. Viele dieser Attacken, die wir im vergangenen Jahr erlebt haben, wird es auch in den kommenden 12 Monaten geben, wie Cryptolocker, die cyberkriminellen Banden so viel Geld eingebracht haben.

Besondere Aufmerksamkeit müssen wir dem Internet der Dinge widmen, da wir immer mehr Geräte mit dem Internet verbinden, die zu einem Tool für Cyberkriminelle werden könnten, mit dem sie alle möglichen privaten und geschäftlichen Informationen über uns in die Hände bekommen. Obwohl diese Geräte normalerweise nicht sehr viele Daten speichern, können sie als Eintrittspunkt für Kriminelle dienen, um in unser Netzwerk zu gelangen, zu Hause oder bei der Arbeit.

Anhand der stattgefundenen Datendiebstähle wird deutlich, dass Unternehmen ein Schutzdefizit haben, das sie umgehend beseitigen müssen. Niemand sollte denken, dass er geschützt und sicher ist. Es ist besser, sich so zu verhalten, als sei man bereits angegriffen worden, statt es erst Monate oder Jahre später herauszufinden. Alles, was in Ihrem Netzwerk passiert, zu verfolgen, ist unerlässlich.

Wir hoffen, dass Sie diesen Bericht nützlich und informativ finden und wir werden Sie über unsere Aktivitäten auf dem Laufenden halten, mit unseren nächsten Reports und in unserem Blog: http://www.pandanews.de

6. ÜBER PANDALABS



6 Über PandaLabs

PandaLabs ist Panda Securitys Anti-Malware-Labor und stellt das Nervenzentrum des Unternehmens für Malware-Behandlung dar:

PandaLabs entwickelt ständig und in Echtzeit die notwendigen Gegenmaßnahmen, um weltweit Panda-Security-Kunden vor allen Arten von schädlichem Code zu schützen.

PandaLabs ist somit verantwortlich für die Durchführung detaillierter Scans von allen Arten von Malware, mit dem Ziel, den Schutz für Panda-Security-Kunden zu verbessern und die allgemeine Öffentlichkeit zu informieren.

Bei PandaLabs ist man ständig wachsam und beobachtet genau die verschiedenen Trends und Entwicklungen, die im Bereich Malware und Sicherheit stattfinden.

Ziel ist es, sowohl vor drohenden Gefahren und Bedrohungen zu warnen, als auch zukünftige Ereignisse vorherzusagen.

pandalabs

panda

pandalabs