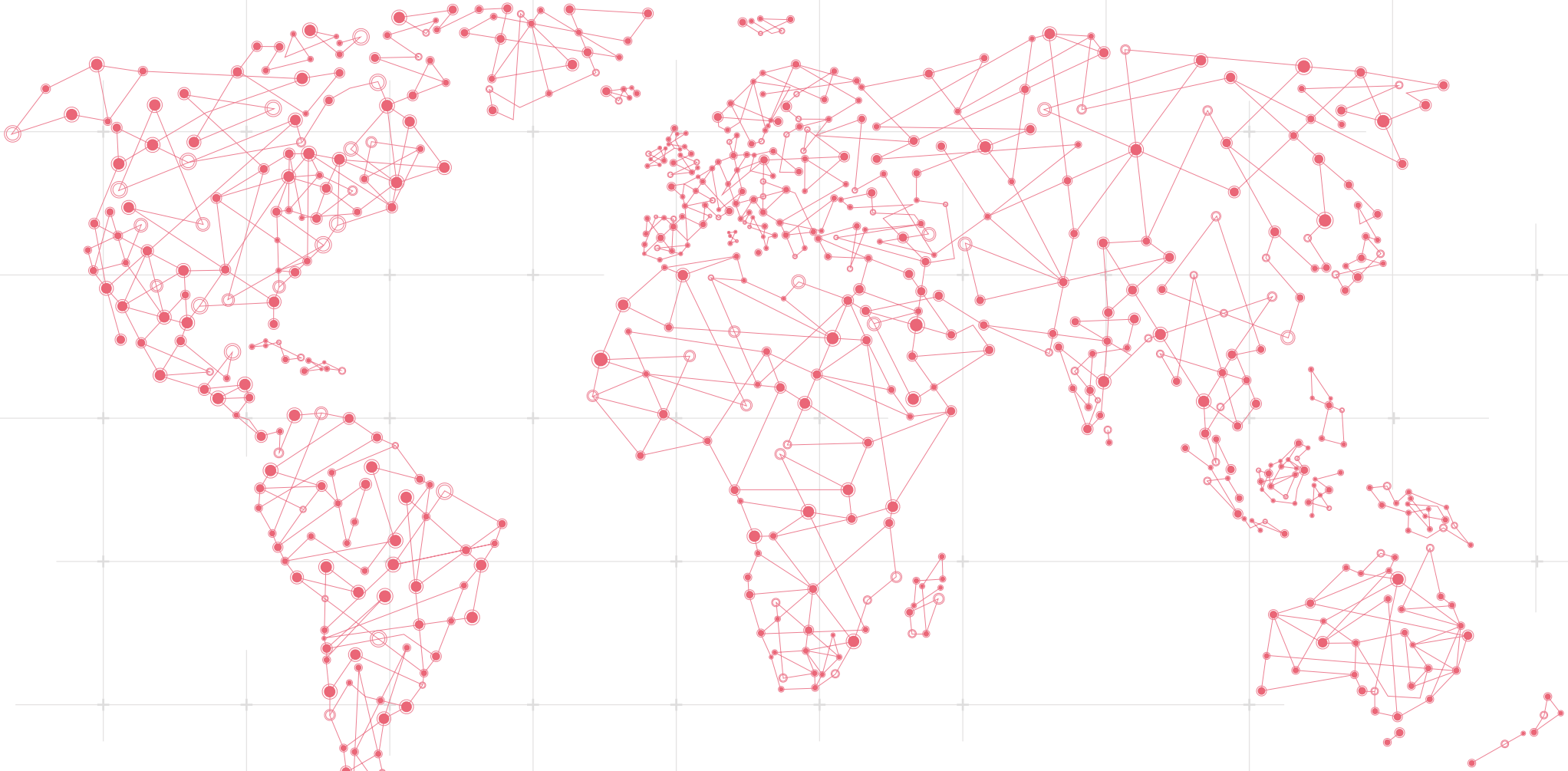
PANDALABS

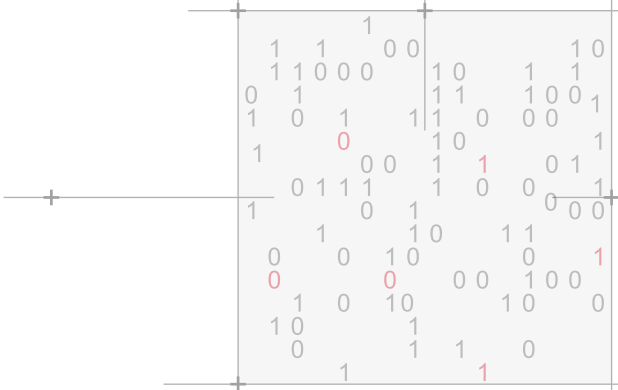
THE EYE OF SECURITY



QUARTALSBERICHT

Q3 2014

PANDA SECURITY | *The Cloud Security Company*



EINLEITUNG

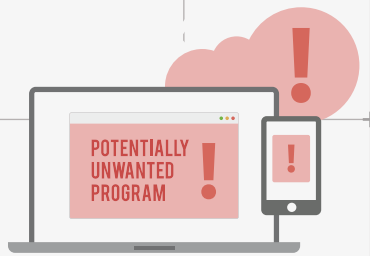
Die Sommerferienzeit fällt in das dritte Quartal und so wird es oft als die Zeit zum Ausruhen und Entspannen angesehen… Nun, das gilt nicht für den Kampf gegen Cyberkriminalität. Wir hatten ganz und gar keine ruhige Zeit, denn die Anzahl der Cyberangriffe auf der ganzen Welt hat exponentiell zugenommen.

__ Die Anzahl der brandneuen Malwarefamilien erreichte mit mehr als 20 Millionen neuer Exemplare, die im 3. Quartal identifiziert wurden, ein neues Rekordhoch. __

Auch im Bereich der Malware für Mobilgeräte steigen die Zahlen. Auf der einen Seite verkünden leitende Android-Sicherheitsingenieure bei Google, dass sich die User überhaupt keine Sorgen machen müssen und Antivirenprogramme für Android nicht unbedingt nötig seien. Auf der anderen Seite tauchen neue Sicherheitslücken auf, die es Angreifern ermöglichen, die Geräte von Usern zu infizieren und die Kontrolle zu übernehmen.

Wir werden uns den #celebgate-Hack näher anschauen, aufgrund dessen private Fotos von mehr als 100 Schauspielerinnen und Models ins Internet gelangten, und inwiefern Apple dafür verantwortlich ist. Außerdem werden wir einige der großen Datenschutzverletzungen behandeln, die Firmen auf der ganzen Welt erlitten haben, z.B. UPS, JP Morgan Chase, Home Depot usw.

Abschließend werden wir unsere Aufmerksamkeit auf die jüngsten Cyberspionage-Skandale lenken, die durch den ehemaligen NSA-Angestellten Edward Snowden aufgedeckt wurden.



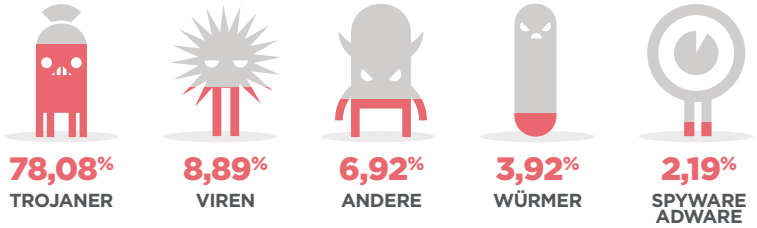
MALWARE-ZAHLEN IM 3. QUARTAL

Die Anzahl der neuen im Umlauf befindlichen Malware ist im ersten Halbjahr beträchtlich gestiegen. Die Zahlen des letzten Jahres wurden verdoppelt und erreichten durchschnittlich 160.000 neue Exemplare pro Tag. Im 3. Quartal verschärften sich die Dinge. In den PandaLabs verzeichneten wir mehr als 20 Millionen neue Malware-Exemplare allein in den vergangenen drei Monaten. Im Durchschnitt erschienen 227.747 neue Schädlinge an einem einzigen Tag.

Die Mehrheit dieser Malware-Bedrohungen gehört nicht zu neu entwickelten Familien. Vielmehr sind es Varianten von wohlbekannten Malware-Exemplaren, die von ihren Autoren in geeigneter Weise abgewandelt wurden, um Erkennungssysteme zu umgehen.

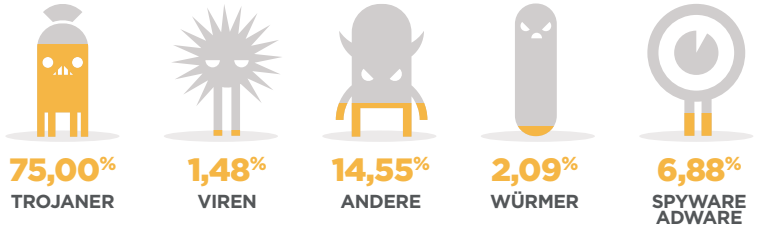
Trojaner sind weiterhin die häufigste Art von Malware. Sie machen 78,08 Prozent der in Umlauf gebrachten neuen Malware-Exemplare aus. Computerviren sind mit nur 8,89 Prozent weit abgeschlagen. Hier ein Überblick über neue Malware, die im dritten Quartal erschienen ist:

NEU ENTWICKELTE MALWARE IM DRITTEN QUARTAL 2014, NACH TYP



Wenn man das weltweite Auftreten von Infektionen analysiert, gleichen sich die Zahlen. Jedoch muss festgestellt werden, dass die Prozentzahlen in der Kategorie „Andere" deutlich voneinander abweichen. Hier ist die Anzahl der Infektionen, die durch „andere" Malware verursacht wurden, mehr als doppelt so hoch wie die Anzahl an neu entwickelter „anderer" Malware.

INFEKTIONEN DURCH MALWARE NACH TYP IM 3. QUARTAL 2014

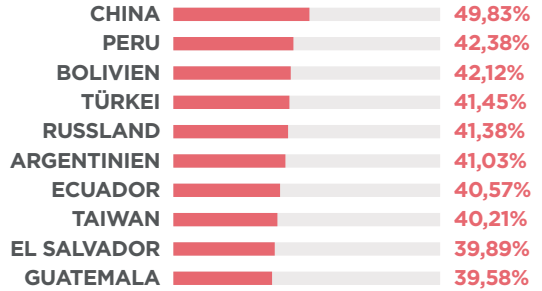


Die in den Kategorien „Andere" (die ‚Potentiell Unerwünschte Programme' (PUPs) einschließt) und „Adware/Spyware" enthaltene Malware scheint also besonders effizient zu sein. Diese Programme können mit weniger Exemplaren verhältnismäßig mehr Computer infizieren. Es handelt sich meist um vertrauenswürdige Software, die sehr aggressive Mittel nutzt, um Computer zu erreichen. So werden beispielsweise kostenfreie Installationsprogrammen, die legale Software verteilen, mit Anwendungen gebündelt, die ohne das Wissen der User andere Programme auf deren Computern installieren.

Die weltweite Infektionsrate lag mit 37,93 Prozent leicht über denen der vorangegangenen Quartale. Im Ländervergleich lag China wieder auf Platz 1 mit einer Infektionsrate von 49,83 Prozent. Das ist nach langer Zeit das erste Mal, dass das größte asiatische Land eine Rate von unter 50 Prozent aufweist. China wird gefolgt von Bolivien (42,12 %) und Peru (42,38 %).

Nachstehend listen wir die 10 Länder mit den höchsten Infektionsraten auf:

LÄNDER MIT DEN HÖCHSTEN INFEKTIONSRATEN



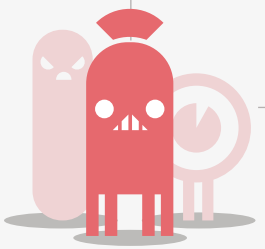
Es ist klar ersichtlich, dass die höchsten Positionen in der Rangliste von asiatischen und lateinamerikanischen Ländern gehalten werden. Zu weiteren Ländern mit Raten über dem weltweiten Durchschnitt gehören: Polen (39,48 %), Brasilien (39,21 %), Slowenien (39,05 %), Kolumbien (38,86 %), Spanien (38,37 %), Costa Rica (38,19 %), Chile (38,05 %) und Italien (37,97 %).

Im Gegensatz dazu folgt jetzt eine Liste der Länder mit den geringsten Infektionen:

LÄNDER MIT DEN NIEDRIGSTEN INFEKTIONSRATEN

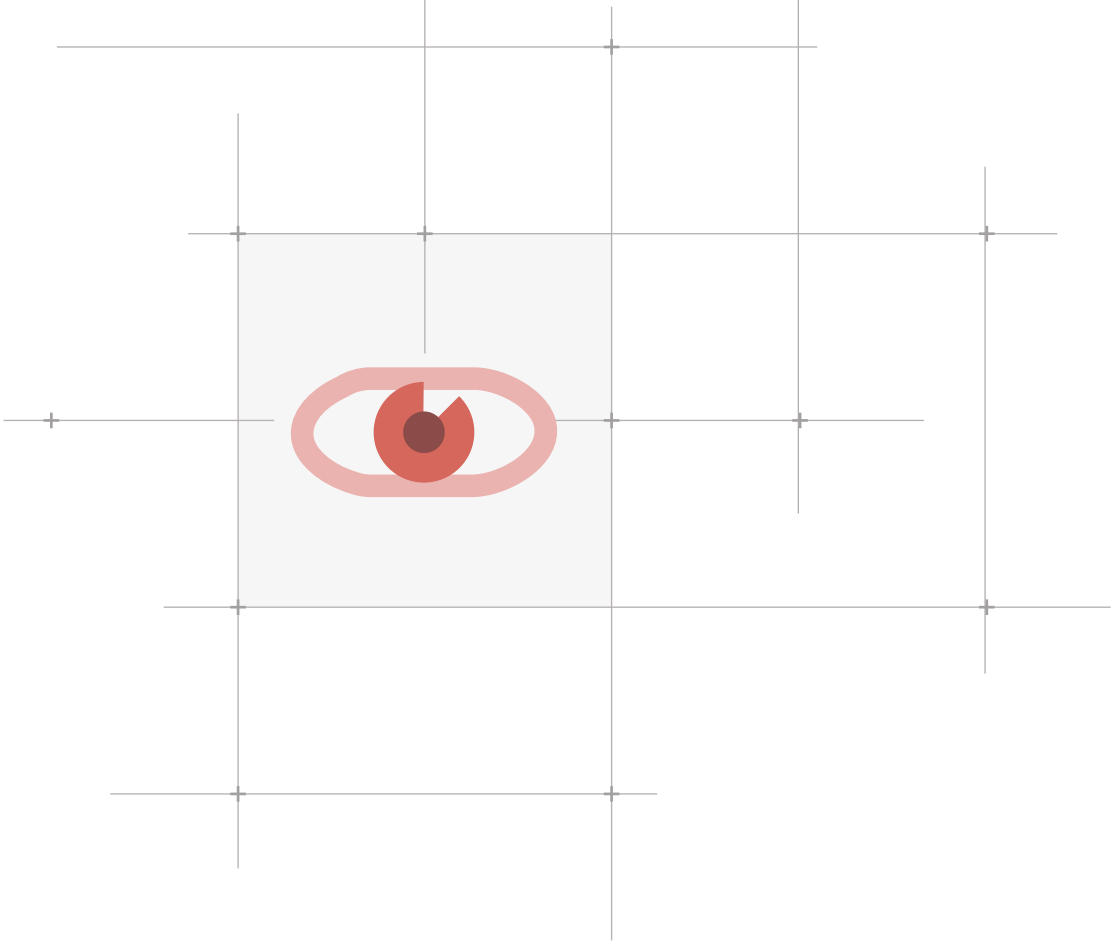
PORTUGAL	27,83%
BELGIEN	27,39%
NIEDERLANDE	26,96%
DEUTSCHLAND	26,52%
FRANKREICH	25,87%
GROSSBRITANNIEN	25,11%
SCHWEIZ	24,61%
JAPAN	24,02%
SCHWEDEN	23,44%
NORWEGEN	23,07%

Europa ist allgemein das Gebiet mit den niedrigsten Infektionsraten. Neun europäische Länder sind in diesem Ranking vertreten. Norwegen (23,07 %), Schweden (23,44 %) und Japan (24,02 %) sind weltweit die Länder mit den wenigsten Infektionen. Andere Länder, die es zwar nicht in die Liste der Top 10 geschafft haben, aber trotzdem unter dem Durchschnitt liegen, sind: Dänemark (28,18 %), Finnland (28,59 %), Panama (29,77 %), Kanada (30,03 %), Österreich (30,55 %), Uruguay (31,15 %), Venezuela (32,35 %), Australien (32,54 %), USA (33,03 %), Tschechische Republik (34,46 %), Mexiko (36,31 %) und Ungarn (36,99 %).



DAS QUARTAL IM ÜBERBLICK

Obwohl das dritte Quartal in die Sommerferienzeit fiel, gab es so viel zu tun wie immer. Nachstehend fassen wir einige der wichtigsten Ereignisse zusammen, die sich in diesem Zeitraum in der Welt der Computersicherheit ereignet haben.



CYBER-KRIMINALITÄT

__ iCloud befand sich im Mittelpunkt des viel diskutierten #celebgate Skandals. Durch diesen Hackerangriff gelangten private Fotos von mehr als 100 Schauspielerinnen und Models ins Internet. __

Eine der besten Möglichkeiten zum Entschärfen des Risikos von Hackerangriffen ist die Zwei-Faktor-Authentifizierung. Die meisten Online-Service-Unternehmen (Facebook, Google, Microsoft usw.) nutzen diese bereits. In diesem Quartal hat Apple, das die Zwei-Faktor-Authentifizierung schon für seinen iCloud Service nutzt, die Features für seine iCloud.com Web-App-Suite erweitert. Damit bietet es Usern, die über ihre iPhones oder iPads auf ihre iCloud-Accounts zugreifen, eine zusätzliche Sicherheitsebene.

iCloud stand im Mittelpunkt des viel diskutierten #celebgate Skandals. Durch diesen Hackerangriff gelangten private Fotos von mehr als 100 Schauspielerinnen und Models ins Internet. Schauspielerinnen wie Jennifer Lawrence, Kirsten Dunst oder Kate Upton waren unter den Opfern dieses massiven Fotohacks. Die Bilder wurden aus dem Online-Speicher, der von Apples iCloud-Plattform angeboten wird, gestohlen.

Anfangs dachte man, dass es die Lecks aufgrund einer potentiellen Sicherheitslücke gegeben haben könnte. Aber dann kündigte Apple nach einer 40-stündigen Untersuchung an, dass sie herausgefunden hätten, dass die Konten dieser Promis „durch einen Angriff auf diese speziellen Benutzernamen, Passwörter und Sicherheitsabfragen gefährdet wurden".

Apple ergänzte, dass diese Angriffe „im Internet allzu üblich geworden seien". Die Opfer solcher Hackerangriffe sollten daraus einige Lehren ziehen:

- Laden Sie nie Bilder hoch, die Sie nicht teilen wollen.
- Aktivieren Sie die Zwei-Faktor-Authentifizierung für Ihre Online-Accounts.

Eine russische Hackergruppe, die unter dem Namen w0rm bekannt ist, griff die Technologie-Newsletter-Webseite CNET an und stahl Benutzernamen, E-Mails und verschlüsselte Passwörter von mehr als einer Million Usern. Es handelt sich um dieselbe Bande, die sich in der Vergangenheit dazu bekannt hatte, die Webseiten von BBC, Adobe und der Bank of America gehackt zu haben.

Im dritten Quartal dieses Jahres gab es massive Datendiebstähle bei großen Unternehmen und Institutionen auf der ganzen Welt. Community Health Systems, eine der größten Krankenhausgruppen der USA, gab bekannt, dass ihr Computernetzwerk das Ziel eines Cyberangriffs gewesen sei, bei dem Identifikationsdaten für 4,5 Millionen Patienten gefährdet wurden. Im August meldete die Supermarktkette Supervalue, dass es Hackern gelungen sei, Kundendaten in 180 ihrer Supermärkte im ganzen Land zu stehlen. Außerdem bestätigte UPS, dass Kredit- und Debitkarten-Informationen von Kunden, die ihre Geschäfte in 51 der Zweigstellen erledigten, als Folge eines Eindringens in das Unternehmensnetzwerk gefährdet wurden.

Die US-Bank JP Morgan Chase wurde Opfer einer ähnlichen Datenschutzverletzung. Hacker starteten einen gezielten Angriff auf bestimmte Mitarbeiter von JP Morgan Chase, um Zugriff auf deren Computer zu erhalten und damit auf die Datenbanken des Kreditinstitutes. Die Hacker veränderten und löschten einige der Bankdaten. Das Motiv für diese Aktionen ist immer noch unklar. Sowohl das FBI als auch der Geheimdienst ermitteln in diesem Fall.

Home Depot war das Opfer eines der größten Angriffe in diesem Quartal. Der Baumarktbetreiber bestätigte, dass seine Server angegriffen wurden, und dass 56 Millionen Kredit- und Debitkarten-Informationen gestohlen wurden. Laut dem Wall Street Journal gestand das Unternehmen auch ein, dass in einigen Fällen die zu den Karten gehörigen Konten leergeräumt wurden.

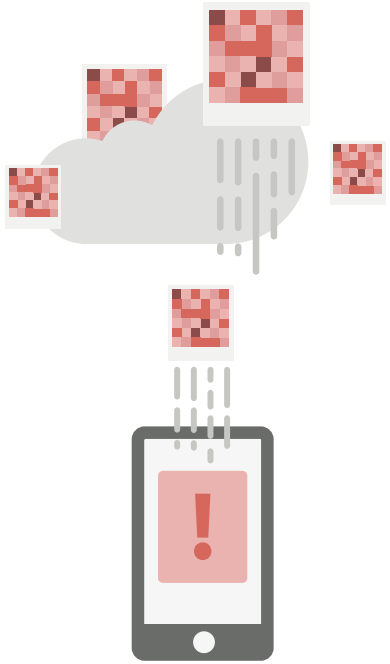
Außerdem gab es betrügerische Transaktionen in den USA, weil die Kriminellen die gestohlenen Kreditkartendaten nutzten, um Prepaidkarten, Elektrogeräte und sogar Lebensmittel zu kaufen.

Dieser Angriff ereignete sich nur einige Monate nach einer ähnlichen Attacke auf Target Corp. und könnte damit in Verbindung stehen, da für den Hack dasselbe Tool – BlackPOS – benutzt wurde. Es sieht so aus, als seien von dieser Sicherheitsverletzung Kunden betroffen, die im Zeitraum April bis September in irgendeinem der fast 4.000 Geschäfte, die das Unternehmen in den USA und Kanada besitzt, eingekauft haben.

Die Nachricht von einem potentiellen Hackerangriff auf Google machte Schlagzeilen. Eine Liste von fast fünf Millionen Gmail Benutzernamen und Passwörter gelangte ins Internet. In einer Erklärung für die Medien sagte Google, es gäbe keine Beweise dafür, dass seine Systeme gefährdet gewesen seien. Außerdem fügten sie hinzu, dass Schritte unternommen werden, um Usern zu helfen, ihre Benutzerkonten zu schützen, wann immer sie eine Gefährdung von Accounts wahrnehmen. Google behauptet, dass 98 Prozent der Passwörter nicht funktioniert hätten und dass es so aussähe, als sei man an die Daten durch Phishing und andere Hackerangriffe auf User gelangt.

Eine Sicherheitslücke, welche die Sicherheit von Linux- und Mac-Usern gefährdete, wurde in Bash entdeckt. Diese Schwachstelle namens „Shellshock" beeinträchtigte den Kommandozeileninterpreter in diesen Betriebssystemen. Diese Lücke könnte den Cyberkriminellen den Fernzugriff auf ein System, das Bash nutzt, ermöglichen und somit das Einschleusen von Spyware. Mit dieser könnten sie vertrauliche Informationen stehlen oder gar die Kontrolle über das System übernehmen.

Zu den betroffenen Systemen gehörten Mac OS X Computer, viele Webserver und einige Geräte für Heimnetzwerke wie zum Beispiel Router.



SOZIALE NETZWERKE

__ Twitter tritt der Unternehmensgruppe bei, die solche User belohnt, die sich der Entdeckung von Sicherheitslücken in ihren Programmen oder Plattformen widmen. __

In der Technologiewelt ist es mittlerweile üblich, dass Unternehmen die Bemühungen von fortgeschrittenen Usern belohnen, die ihre Zeit dem Entdecken von Sicherheitslücken in ihren Programmen oder Plattformen widmen.

Obwohl es immer noch Firmen gibt, die von der Wirksamkeit solcher Prämienprogramme überzeugt werden müssen, sehen viele sie als äußerst sinnvoll an. Einerseits können so neue, bislang unentdeckte Bugs gefunden werden. Andererseits ziehen die Unternehmen diese Anwenderexperten damit auf ihre Seite. Twitter gehörte noch zu denjenigen, die diese Idee bislang nicht aufgegriffen hatten. Das soziale 140 Zeichen-Netzwerk wollte anscheinend nur widerwillig in seine Taschen greifen, um Experten finanziell zu ermutigen, Bugs in seinem Dienst zu finden.

Nichtsdestotrotz hat das Unternehmen jetzt bekanntgegeben, dass es diejenigen, die Sicherheitslücken in Twitter.com, ads.twitter, mobile Twitter, TweetDeck, apps.twitter sowie in den Apps für iOS und Android finden, mit mindestens 140 $ belohnt. Diese Summe ist noch weit entfernt von dem, was andere Firmen bieten. Prämienprogramme bei Unternehmen wie Facebook oder Google belohnen User, die Schwachstellen entdecken, mit Beträgen von jeweils über 500 $ bzw. 1000 $.

MOBILE MALWARE

__ Malware für Android hat weiterhin exponentiell zugenommen. 2014 ist jetzt schon das Jahr, in dem die meisten Exemplare mobiler Malware in Umlauf gebracht wurden. __

Android war wieder einmal das Hauptziel für die Entwickler von Malware für Mobilgeräte. Adrian Ludwig, führender Sicherheitsingenieur für Android bei Google, sagte, dass es „eine gewisse falsche Wahrnehmung" gegeben hätte, was das Überprüfen der Apps für seinen Google Play Store im Vergleich mit anderen Stores angeht (eine nicht besonders subtile bissige Bemerkung in Richtung von Apples iOS App Store, der den Ruf hat, in dieser Hinsicht anspruchsvoller zu sein). In diesem Zusammenhang verkündete er sogar, dass ein mobiler Antivirus für Android nicht notwendig sei.

Inzwischen hat Malware für Android weiter exponentiell zugenommen. 2014 ist jetzt schon das Jahr, in dem die meisten Exemplare mobiler Malware in Umlauf gebracht wurden.

Außerdem sind neue Schwachstellen aufgetreten, die von Cyberkriminellen für schädliche Zwecke ausgenutzt werden könnten:

- CVE-2013-6272: Existiert in allen Android-Versionen ab 4.4.2 (KitKat). Damit können Apps nicht genehmigte Anrufe zu teuren Sonderrufnummern machen.

- CVE-2014-N/A: Existiert in Android 2.3.3 und 2.3.6 und hat dieselben Auswirkungen wie die vorherige Schwachstelle.

CYBERKRIEG

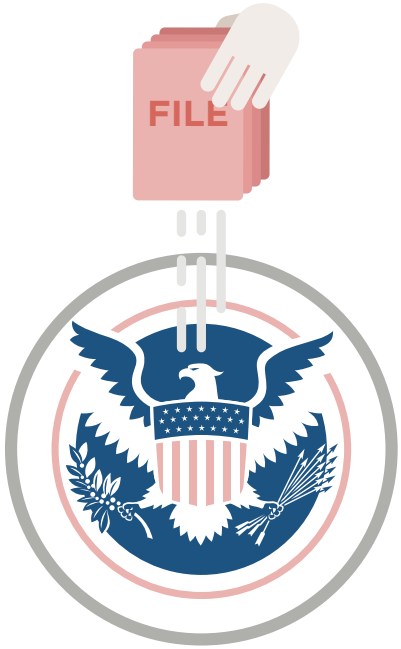
Im Juli enthüllte die US-amerikanische Zeitung The New York Times, dass mutmaßliche chinesische Hacker Zugriff auf einige der Datenbanken erhalten hätten, die vom Office of Personnel Management verwaltet werden und persönliche Informationen von Bundesbediensteten enthalten, die sich um höchste Sicherheitsfreigaben bewerben. Die US-Regierung bestätigte den Angriff, aber bestritt den möglichen Diebstahl von geheimen Informationen. Obwohl die Hacker nach China zurückverfolgt wurden, gibt es keinen endgültigen Beweis dafür, dass sie im Auftrag der chinesischen Regierung gearbeitet haben.

Im dritten Quartal des Jahres gab es massive Datendiebstähle bei großen Firmen und Institutionen auf der ganzen Welt.

Streng geheime Dokumente der NSA und des britischen Geheimdienstes GHCQ enthüllten die Existenz von „Treasure Map", einer geheimen Operation mit dem Ziel, das gesamte Internet aufzuzeichnen, einschließlich der Geräte der Endanwender. Die vom ehemaligen NSA-Angestellten Edward Snowden veröffentlichten Dokumente zeigten, wie die NSA und ihre Geheimdienstpartner illegal in interne Netzwerke verschiedener Unternehmen eindrangen, um ihr Ziel zu erreichen. Eine dieser Firmen ist die Deutsche Telekom. Nachdem diese durch das deutsche Magazin „Der Spiegel" über einen möglichen Angriff informiert wurden, scannte sie ihr Netzwerk. Ein Beweis für ein Eindringen konnte allerdings nicht gefunden werden.

Andere von Snowden enthüllte Geheimdokumente zeigten, wie der britische Geheimdienst GHCQ aktiv Skype-User in Echtzeit und ohne deren Wissen überwachen konnte.

Im August behauptete ein Hacker, 40 GB an internen Dokumenten von Gamma International (http://en.wikipedia.org/wiki/FinFisher), einem deutsch-britischen Technologieunternehmen, gestohlen zu haben. Gamma International entwickelt Spionagesoftware für Regierungen und Polizeibehörden auf der ganzen Welt. Der Cyberkriminelle erstellte einen Twitter-Account (@GammaGroupPR), über den er anfing, Links zu der gestohlenen Dokumentation zu posten.

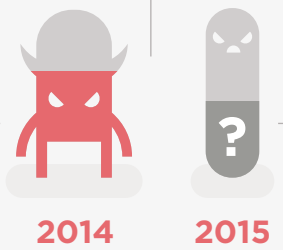


FAZIT

Das dritte Quartal des Jahres 2014 war so aufregend wie erwartet. Wir haben in der Tat die höchste Anzahl neuer Malware-Exemplare in der Geschichte aufgezeichnet. Außerdem gab es die bislang größten Fälle von Datenschutzverletzungen, bei denen Millionen von Kreditkarten- und persönlichen Informationen gestohlen wurden.

Ausgehend von den hektischen Aktivitäten, die bisher für dieses Jahr kennzeichnend waren, gibt es keinen Zweifel daran, dass auch das letzte Quartal ebenso spannend sein wird. Wird die Programmierung von Malware weiterhin zunehmen oder schließlich nachlassen? Welche neuen Taktiken können wir im Bereich der Mobilgeräte erwarten? Welche neuen Firmen werden Opfer von Cyberattacken werden? Welche neuen Dokumente wird Edward Snowden offenlegen und wie wird dies den bereits angeschlagenen Ruf der NSA beeinflussen?

Sie werden die Antworten auf diese Fragen und vieles mehr in unseren nächsten Bericht finden. Der Report wird eine Zusammenfassung der bedeutendsten Ereignisse des vergangenen Jahres enthalten sowie eine Vorhersage für die Internetgefahren des kommenden Jahres.



ÜBER PANDALABS

PandaLabs ist das Anti-Malware-Labor des weltweit agierenden IT-Spezialisten Panda Security und fungiert als dessen zentrale Stelle für Malware-Behandlung.

- PandaLabs entwickelt kontinuierlich und in Echtzeit die notwendigen Gegenmaßnahmen, um Panda Security Kunden vor allen Arten von schädlicher Software auf globalem Level zu schützen.
- PandaLabs ist somit verantwortlich für die Durchführung detaillierter Scans aller Malware-Arten. Ziel ist es, sowohl den Schutz für die Panda Security Kunden zu verbessern als auch die Öffentlichkeit aktuell und zeitnah zu informieren.

Ebenso bleiben die PandaLabs ständig wachsam und beobachten genau die verschiedenen Trends und Entwicklungen, die in den Bereichen Malware und Sicherheit stattfinden. Aufgabe der PandaLabs ist es, sowohl vor drohenden Gefahren zu warnen als auch zukünftige Ereignisse vorherzusagen.

https://www.facebook.com/PandaSecurityDE

https://twitter.com/pandanewsde

https://plus.google.com

https://www.youtube.com/PandaTV1

http://www.pandasecurity.com/mediacenter