
PANDALABS QUARTALSBERICHT Q2 2016



1. Einleitung

2. Das Quartal auf
einen Blick

Ransomware

Cyberkriminalität

Social Media

Mobilgeräte

Internet der Dinge

Cyberkrieg

3. Fazit

4. Über PandaLabs

1. EINLEITUNG

1

Einleitung

Das Internet ist ein wichtiger Bestandteil unseres täglichen Lebens geworden. Die digitale Entwicklung beeinflusst sowohl das berufliche als auch das private Umfeld, da die Anzahl der internetfähigen Geräte weiterhin zunimmt. Konzepte wie "Digital Home" und "BYOD" (Bring Your Own Device) bilden bereits einen Teil unseres hyper-verbundenen Universums; immer mehr Internetnutzer arbeiten von zu Hause aus oder verwenden ihre eigenen Geräte sowohl für private als auch für berufliche Zwecke. Das bedeutet, dass es zunehmend Sicherheitslücken gibt.

Beweis dafür sind die 18 Millionen neuen Malware-Exemplare, die PandaLabs im 2. Quartal 2016 entdeckt hat.

Diese neuen Bedrohungen bringen neue Ziele und Chancen für die Welt der Cybersicherheit mit sich. In dem Quartal behaupten die Trojaner ihre Spitzenposition in der Liste der erfassten Malware und unterstreichen so die Zunahme von Ransomware-Angriffen in dieser Kategorie. Die durchschnittliche Anzahl neuer Bedrohungen, die täglich entdeckt werden, beträgt 200.000. Diese Zahl ist deutlich niedriger als im vorherigen Quartal, als täglich rund 227.000 neue Schädlinge identifiziert wurden.

Neben den Ransomware-Angriffen hat die Mehrzahl der anderen Attacken in diesem Quartal zum Diebstahl von persönlichen Informationen und Anmeldedaten geführt.

Unternehmen sehen einen riesigen Boom (und eine kurzfristige Gefahr) im Internet der Dinge. Es wird zu einer Geburtsstätte für Angriffe und hat das Potenzial, unser privates Leben zu beeinflussen. Beispielsweise könnten Kriminelle mittels Cyberattacken unsere Autos stehlen, indem Sie per Fernzugriff den Diebstahlalarm deaktivieren und das Fahrzeug starten.

Jeden Tag entdecken wir neue Schwachstellen im Bereich der Mobiltelefone. Nur zur Erinnerung: Die meisten Probleme, die aufgrund dieser Sicherheitslücken entstehen, sind größtenteils auf das Fehlen von Updates oder deren späte Veröffentlichung durch die verschiedenen Hardware-Hersteller zurückzuführen.

2. DAS QUARTAL AUF EINEN BLICK

2

Das Quartal auf einen Blick

Ransomware

Wir wissen, dass Ransomware ein großes Geschäft für Cyberkriminelle ist. Einen genauen Wert anzugeben, ist jedoch schwierig. Im Jahr 2015 gab das amerikanische Justizministerium bekannt, dass die Beschwerdestelle für Internetkriminalität (IC3) 2.500 Beschwerden über Ransomware-Attacken erhalten habe. Die Opfer dieser Erpressungen zahlten Lösegelder in Höhe von insgesamt 24 Millionen Dollar. Erpressungssoftware ist ein weltweites Phänomen. Wenn wir den Gesamtbetrag des in diesem Beispiel gezahlten Lösegeldes und die großflächige Zunahme von Malware berücksichtigen, können wir schlussfolgern, dass Ransomware jedes Jahr Kosten in Milliardenhöhe verursacht.

Es gab bereits eine Reihe von Ransomware-Angriffen im Gesundheitswesen. Zu Beginn dieses Quartals wurde MedStar Health zu einem neuen Opfer. Diese gemeinnützige Gesundheitsorganisation mit Sitz in Columbia, Maryland (USA), erlitt eine so schwerwiegende Ransomware-Attacke, dass sie ihre Systeme für mehrere Tage vom Netz nehmen musste.

Im Fall von MedStar Health scheint es sich um einen gezielten Angriff gehandelt zu haben, bei dem eine bestehende Schwachstelle in ihren Systemen ausgenutzt wurde. Die meisten dieser Attacken werden jedoch über schädliche E-Mail-Anhänge oder gefährdete Internetseiten ausgeführt. So geschehen im April dieses Jahres. Maisto International, ein Unternehmen, das für die Herstellung ferngesteuerter Spielzeuge bekannt ist, setzte die Besucher seiner Webseite unwissentlich Ransomware aus. Ihre kompromittierte Website infizierte Besucher mit dem bekannten Exploit Kit Angler. Ziel von Angler ist es, beliebte Softwareprogramme ausfindig zu machen (Flash, Java usw.), und dann die verschiedenen Schwachstellen dieser installierten Applikationen auszunutzen, um den Computer zu infizieren.

Allerdings sind nicht alle Angriffe über Webseiten die Folgen desselben Hacking-Typs. Cyberkriminelle bedienen sich einer weiteren beliebten Taktik, die als Malvertising bekannt ist. Dabei nutzen sie öffentliche Räume auf stark besuchten Webseiten, um die Besucher zu infizieren.



Der bekannte Blog perezhilton.com fiel kürzlich zwei Malvertising-Attacken zum Opfer. Hacker benutzten das Exploit Kit Angler, um mehr als 500.000 der täglichen Besucher zu infizieren.

Gezielte Angriffe nutzen Systemschwachstellen aus. Das Hacken von Webseiten und Malvertising sind die häufigsten Bedrohungen.

Einer der interessantesten Erpressungsfälle im zweiten Quartal 2016 ereignete sich in einem Unternehmen in Slowenien. Die IT-Abteilung der Firma erhielt eine E-Mail aus Russland, in der mitgeteilt wurde, dass ihr

Netzwerk gehackt worden sei. Die russischen Cyberkriminellen drangen in das Netzwerk ein und bereiteten die Ausführung von Ransomware auf allen Firmencomputern vor. Sollte sich das slowenische Unternehmen weigern, das geforderte Lösegeld von 9.000 Euro (in Bitcoins) innerhalb von drei Tagen zu zahlen, würde die Ransomware ausgeführt werden. Um zu beweisen, dass sie Zugriff auf das Firmennetzwerk haben, schickten die Verbrecher eine Liste aller mit dem internen Netzwerk des Unternehmens verbundenen Geräte.

Es gibt viele Opfer von Erpressungssoftware, die sich dazu entschlossen haben, das Lösegeld zu zahlen. Jedoch ist dies keine Garantie dafür, dass die gestohlenen Daten tatsächlich zurückgegeben werden. Im Mai wurde das Kansas Heart Hospital von Ransomware angegriffen und die Verantwortlichen entschieden, das Lösegeld zu zahlen, um die gestohlenen Daten zurückzuerhalten. Sie waren schockiert, als sie feststellen mussten, dass sie mit dem Passwort, das man ihnen gegeben hatte, nur einen Teil der gekidnappten Informationen entsperren konnten. Für die Rückgabe der gesamten gestohlenen Daten forderten die Angreifer eine zweite Zahlung. Das Krankenhaus lehnte dies ab.

Das CSLFR, ein professionelles NASCAR-Rennsport-Team, bestätigte Angriffe auf drei ihrer Computer. Die Ransomware Teslacrypt verschlüsselte Informationen, die mehr als 2 Millionen Dollar wert waren. In diesem Fall zahlte CSLFR das Lösegeld (vermutlich rund 500 \$) und erhielt alle Daten zurück.

Ist es ratsam, die geforderten Lösegelder zu zahlen?

Jedes Mal, wenn die Opfer die Erpresser bezahlen, steigert das deren Gewinne. Wenn ein Angriff erfolgreich ist und die Ergebnisse lukrativ sind, werden die Kriminellen ermutigt, weitere Anwender oder Gruppen anzugreifen. Auf lange Sicht werden diese Attacken uns alle treffen.

Die Zahlung von Lösegeld, um gestohlene Daten zurückzuerhalten, fördert kriminelle Aktivitäten.

Zahlen oder nicht zahlen? Dies wird weiterhin eine umstrittene Frage bleiben. Nachteilig dabei ist, dass ausgerechnet das FBI vergangenes Jahr in einer Stellungnahme bestätigte, dass es in den meisten Fällen dazu rät, das Lösegeld zu zahlen. Im April dieses Jahres machte James Trainor, Assistent des Leiters der Cyber-Division des FBI, die (geänderte) Haltung des FBI in einer öffentlichen Stellungnahme deutlich:

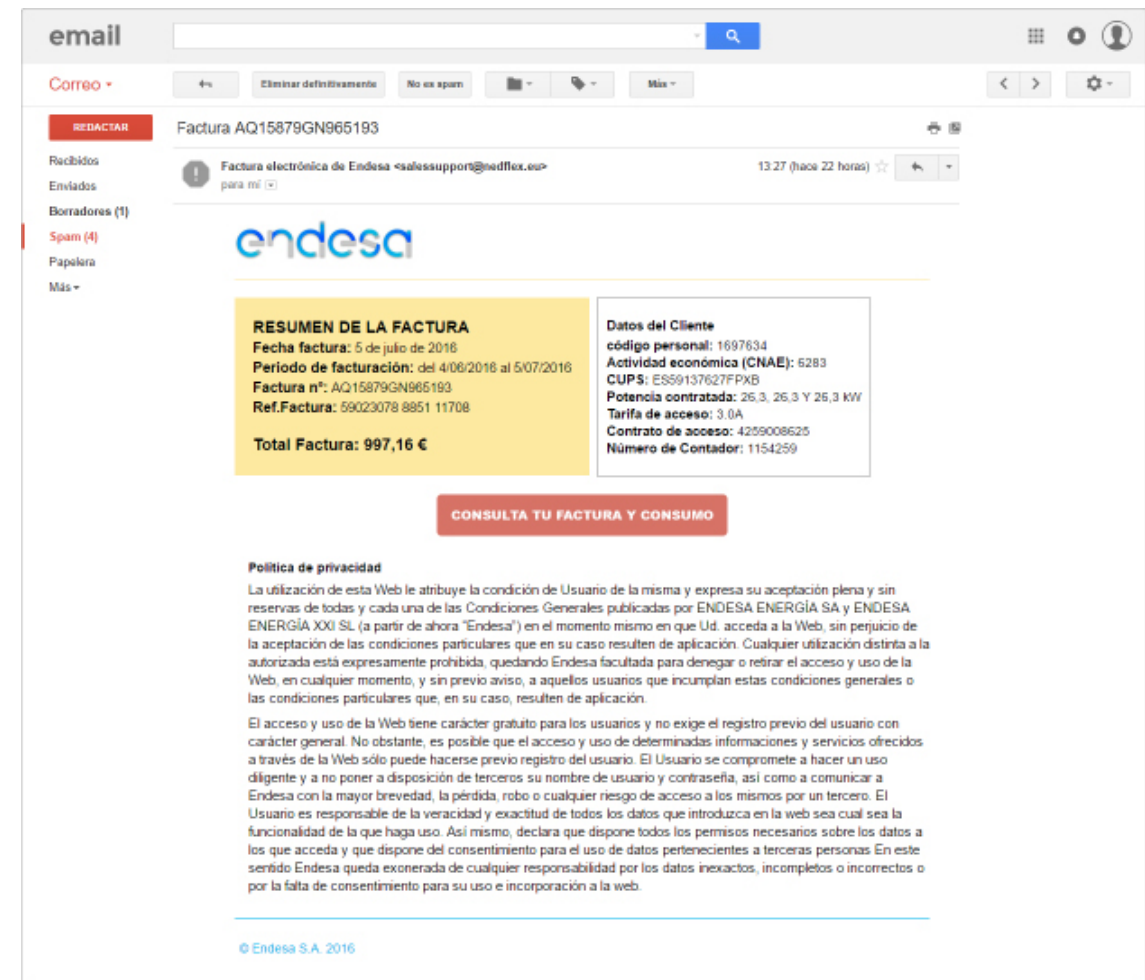
“Die Zahlung eines Lösegeldes garantiert nicht, dass ein Unternehmen seine Daten zurückbekommt. Wir haben Fälle erlebt, bei denen Organisationen nie einen Entschlüsselungscodes erhalten haben, nachdem sie das Lösegeld gezahlt hatten. Lösegeldzahlungen ermutigen die Cyberkriminellen nicht nur dazu, weitere Unternehmen anzugreifen, sie dienen auch als Anreiz für andere Verbrecher, ebenfalls bei dieser Art von illegalen Aktivitäten mitzumischen. Und schließlich könnte ein Unternehmen durch die Zahlung von Lösegeld ungewollt andere rechtswidrige Handlungen der Kriminellen finanzieren.”

Die Entwicklung von schädlichen E-Mails

Ransomware-Attacken erfolgen nicht nur über Malvertising oder kompromittierte Webseiten. Viele von ihnen haben ihren Ursprung in E-Mails, die als Rechnungen oder Mitteilungen getarnt sind.

Eine dieser E-Mail-Attacken ereignete sich sowohl in Polen als auch in Spanien. Dabei tarnten sich die Cyberkriminellen als Elektrizitätsunternehmen im jeweiligen Land. Die Verbrecher schickten infizierte E-Mails an ihre Opfer. Die E-Mails enthielten keine Anhänge, sondern einfach eine Rechnung und schriftliche Informationen sowie einen Link, um „ausführlichen Einblick in die Rechnung erhalten“ zu

können. Durch das Anklicken dieses Links wurde der Anwender zu einer gefälschten Webseite geleitet, die eine genaue Nachbildung der echten Webseite des Elektrizitätsunternehmens war.



Hier konnte der User die “Rechnung” herunterladen. Wenn er die “Rechnung” nach dem Download öffnete, wurde er mit der Ransomware infiziert.

Was würden Sie einem Cyberkriminellen sagen, der Sie angegriffen hat, wenn Sie die Chance dazu hätten?

Wir haben die Entwicklung von Ransomware erlebt. Gewöhnlich werden den Opfern ausführliche Anweisungen gegeben, wie die Zahlungen auszuführen sind. Bei einigen Arten von Erpressungssoftware, wie der neuen Variante der Jigsaw-Familie, gehen die Angreifer so weit, dass sie einen Chat Service integrieren, über den die Anwender in Echtzeit mit den Erpressern reden und die Bedingungen für die Lösegeldzahlung aushandeln können.

Jetzt ist es möglich, mit Internetverbrechern zu chatten, um die Lösegeldzahlungen für die entwendeten Informationen auszuhandeln.

Eine der originellsten – und gefährlichsten – Ransomware-Attacken der vergangenen Monate ereignete sich in Russland. Sie ist einzigartig in der Art, wie sie sich verbreitet, da die Malware zwar per E-Mail versandt wird, aber eigentlich nicht ausgeführt wird. Stattdessen ist sie in ihrer eigenen Sprache programmiert, die von einem Software-Hersteller in Russland kopiert wurde (mit mehr als einer Million Firmen in Russland und der ehemaligen Sowjetunion), und sie funktioniert nur, wenn Sie besagte Software auf Ihrem Computer installiert haben. Sie bringt Sie dazu, Ihr System zu aktualisieren. Wenn die Software ausgeführt wird, verbindet sie sich mit einer Software-Datenbank, sucht nach sich selbst und schickt sich die E-Mails der Anwender. Gleichzeitig infiziert sie den Computer mit Ransomware, verschlüsselt Dateien und verlangt das Standardlösegeld.

Cyberkriminalität

Geld ist fast immer die Hauptmotivation für Cyberkriminalität. Wir haben erlebt, wie die Kriminellen auf verschiedene Arten Gewinne machen: durch Ransomware, das Stehlen von Firmen- und Anwenderdaten und manchmal durch gezielte Angriffe auf Banken. Diese Vorfälle sind in den zurückliegenden Monaten äußerst schwerwiegend geworden. Wenn wir sie genauer betrachten, können wir feststellen, dass sie alle Organisationen betreffen, von Wohlfahrtsverbänden über Finanzinstitute bis hin zu pornografischen Webseiten und Wählerdaten. Sogar die Polizei war betroffen. Jeder ist gefährdet.

Datendiebstahl

Team Skeet, eine Webseite, die pornografische Videos vertreibt und zum US-amerikanischen Paper Street Media Netzwerk gehört, erlitt kürzlich einen Angriff, bei dem die Daten von 237.000 Nutzern gestohlen wurden. Es wurden nicht nur die Anmeldedaten und E-Mail-Adressen der Nutzer gestohlen, sondern außerdem deren Postanschriften. Diese Daten wurden online für 400 Dollar pro Datensatz verkauft. Für alle Log-in-Daten würde sich der Wert auf fast 95 Millionen Dollar belaufen.

Ransomware und das Stehlen von Unternehmens- und Anwenderdaten sind beliebte Taktiken der Cyberkriminellen.

Der National Childbirth Trust (NCT), ein Wohlfahrtsverband mit Sitz in London, hatte am 7. April eine Sicherheitsverletzung zu verzeichnen. Bei diesem Angriff wurden die Daten von 15.085 Nutzern gestohlen, einschließlich der Benutzernamen, der verschlüsselten Passwörter und der E-Mail-Adressen.

Die US-amerikanischen Onlineshops des bekannten Hardware-Herstellers Acer wurden ebenfalls Opfer einer Attacke, bei der die Daten von insgesamt 34.500 Nutzern entwendet wurden. Was besonders erschreckend an diesem Fall ist: Die Seite war über ein Jahr lang (von Mai 2015 bis April 2016) kompromittiert, ohne dass das Unternehmen davon wusste. Nach Bekanntwerden der Sicherheitslücke wurden die User der betreffenden Acer-Onlineshops umgehend von dem Unternehmen informiert und das Problem behoben. Wie das Unternehmen mitteilte, waren die europäischen Onlineshops jedoch nicht von der potentiellen Sicherheitslücke betroffen.

Im Juni bot ein Hacker mit dem Decknamen "The Dark Overlord" Patientendaten von drei verschiedenen US-Unternehmen im Dark Web zum Verkauf an. Insgesamt wurden die Daten von mehr als 650.000 Patienten gestohlen und The Dark Overlord verlangte eine Zahlung von 700.000 Dollar. Kurz darauf versuchte derselbe Hacker die Daten von 9,3 Millionen Kunden einer Krankenversicherung zu verkaufen. Diese Informationen wurden für 750 Bitcoins angeboten. Das entspricht etwa einer halben Million Dollar.

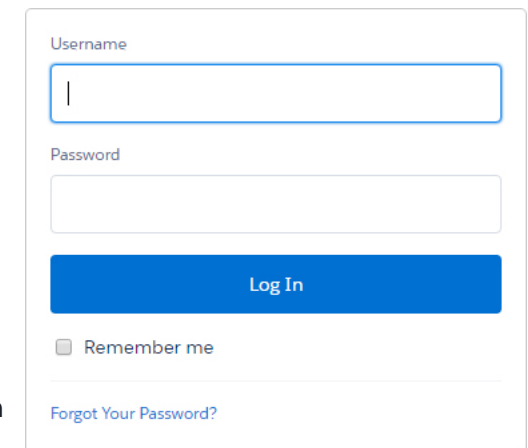
In Spanien veröffentlichte die Gruppe Anonymous eine Liste mit den persönlichen Daten von 5.000 Angehörigen der Nationalpolizei. Die Daten wurden nicht von den Servern der Polizei entwendet, sondern mittels einer Attacke auf die Webseite mupol.es der Police Social Welfare Mutuality.

Wenn wir über Ermittlungen im Kampf gegen Cyberkriminalität sprechen, sollte Ihnen der Name Chris Vickery etwas sagen. Dieser Sicherheitsermittler fand einen Server in der Amazon-Cloud, auf dem jemand eine Datenbank mit den Datensätzen von 93,4 Millionen mexikanischen Wählern hinterlassen hatte. Die Informationen enthielten Postanschriften, offizielle Identifikationen usw. Vickery meldete dies umgehend den mexikanischen Behörden und es dauerte nicht lange, bis die Datenbank entfernt wurde. Was wir immer noch nicht wissen, ist, wie diese Informationen auf den Server gelangt sind. Es ist zu vermuten, dass jemand die Daten gestohlen und den Amazon Server für eine Zwischenspeicherung genutzt hat.

Chris Vickery entdeckte noch einen weiteren Datendiebstahl. In diesem Fall wurden die Kontaktinformationen von 1,1 Millionen Nutzern der Dating-Webseite beautifulpeople.com gestohlen. Obwohl Vickery den Betreibern der Webseite diesen Vorfall meldete, hatten sich die Verbrecher bereits mit der Datenbank aus dem Staub gemacht und sie auf dem Schwarzmarkt verkauft.

Neben den Kriminellen und den Unternehmen, deren Hauptziel es ist, Schaden im gesamten Internet anzurichten, gibt es auch legale Tools, die man gegen uns arbeiten lassen kann. Mithilfe des beliebten Fernzugriff-Tools TeamViewer wurde eine große Anzahl von Nutzern ausgeraubt, da ihre Computer für den Fernzugriff offen waren. Aufgrund der hohen Opferzahl dachte man anfangs, dass jemand TeamViewer gehackt und die Datenbanken für einen späteren unberechtigten Zugriff gestohlen hätte. Später stellte sich heraus, dass die für diesen Raub durchgesickerten Daten von den Nutzern selbst kamen, und zwar von denen, die dieselben Anmeldedaten für verschiedene Dienste nutzten.

Das ist eine bei Hackern weit verbreitete Taktik: Wenn sie die Anmeldedaten von einer Seite stehlen konnten, versuchen sie mit derselben Benutzernamen-Passwort-Kombination, auch auf andere Dienste zuzugreifen. Sie wissen, dass viele Menschen dieselben Anmeldedaten auf verschiedenen Webseiten nutzen. In diesem Fall griffen die Hacker, nachdem sie Zugang zu den Computern der Opfer erlangt hatten, auf deren PayPal-Konten zu und raubten alles Geld, das sie finden konnten.



The image shows a login form with the following elements:

- A text input field labeled "Username" containing a vertical cursor.
- A text input field labeled "Password" which is currently empty.
- A blue button labeled "Log In".
- A checkbox labeled "Remember me".
- A link labeled "Forgot Your Password?".

Die zunehmende Nutzung von POS-Terminals

Eine andere weit verbreitete und beliebte Hackertaktik ist die Nutzung von Point of Sale (POS)-Terminals. POS-Terminals sind anfällig für Malware-Infektionen, die speziell entwickelt wurden, um Kreditkarteninformationen zu stehlen. Gewöhnlich sind Hotels die Opfer, wie wir es bei der Attacke auf das Hard Rock Hotel & Casino in Las Vegas erlebt haben. Es ist bekannt, dass die POS-Terminals von Oktober 2015 bis März 2016 infiziert und Daten von Kreditkarten gestohlen wurden, die in dieser Einrichtung verwendet wurden.

Solche Fälle ereignen sich auf der ganzen Welt. Kürzlich wurde eine kleine Kette von Luxushotels in Spanien angegriffen. Glücklicherweise wurde der Angriff rechtzeitig gestoppt und konnte die POS-Terminals nicht erreichen, was den Raub verhinderte. Diese Attacke wurde speziell für diese Hotelkette entwickelt. Um die Kommunikation nach außen zu ermöglichen und unentdeckt passieren zu lassen, registrierten die Angreifer die Domain unter dem Namen eines der Opfer aus einem afrikanischen Land.

POS-Terminals in Hotels, Restaurants und Unternehmen werden für Hacker immer attraktiver.

Doch nicht nur POS-Terminals und Hotels stehen in der Schusslinie. Cyberkriminelle konzentrieren sich auf Restaurants, um Kreditkartendaten zu stehlen. Mehr als 1.000 Filialen der beliebten amerikanischen Fast-Food-Kette Wendy's waren Opfer von POS-Malware. Die Verbrecher konnten Kreditkarteninformationen von Wendy's Kunden gewinnen. PandaLabs entdeckte eine Attacke, die eine bekannte Malware (in diesem Fall PunkeyPOS) nutzte und mehr als 200 Restaurants in den Vereinigten Staaten infizierte.

Bild: Exemplarische Abbildung einer Wendy's Filiale. Das bedeutet nicht, dass genau dieses Restaurant betroffen war.



Direkte Angriffe auf Finanzinstitute

Wir haben bereits von vielen gewinnbringenden Datendiebstählen berichtet. Lukrativer ist da nur noch das direkte Hacking von Banken.

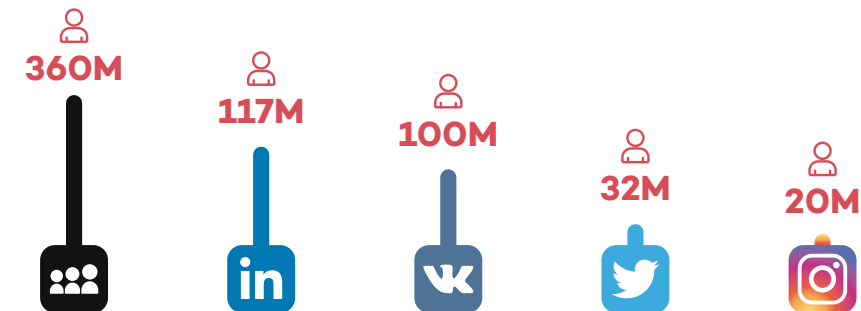


Das passierte der Zentralbank von Bangladesch. Durch einen Angriff konnten Hacker rund 1 Milliarde Dollar überweisen. Glücklicherweise konnte die Bank, als sie dies bemerkte, eine große Anzahl von Überweisungen stoppen. Trotzdem konnten die Diebe mit 81 Millionen Dollar entkommen. In der Folge ereigneten sich zwei ähnliche Fälle: Ein Angriff richtete sich gegen eine Bank in Vietnam und ein weiterer gegen eine Bank in Ecuador.

Auch wenn die Verfolgung von Cyberkriminellen sehr kompliziert und zeitaufwändig sein kann, bringt sie Ergebnisse. Im April wurde Dmitry Fedotov, alias „Paunch“ und Autor des Exploit Kits Blackhold, zu sieben Jahren Haft in einem russischen Gefängnis verurteilt. Aleksandr Panin, ein 27 Jahre alter Russe, wurde ebenfalls verurteilt, diesmal in den Vereinigten Staaten. Er muss neuneinhalb Jahre im Gefängnis verbringen. Panin steckte hinter SpyEye, einem bekannten Banking-Trojaner.

Soziale Medien

Wenn es etwas gibt, das in diesem Quartal in den sozialen Medien besonders auffiel, so sind es die riesigen Mengen an gestohlenen Anmeldedaten, die fast immer in den falschen Händen landen. Schauen wir uns die beliebtesten an:



LinkedIn:

Die Sicherheit von 117 Millionen LinkedIn-Nutzern war gefährdet, nachdem eine Liste mit E-Mail-Adressen und Passwörtern veröffentlicht worden war. Obwohl sich die Sicherheitsverletzung bereits im Jahre 2012 ereignete, wurde die vollständige Liste erst vor kurzem publiziert. Die beste Möglichkeit, sich vor dieser Art von Angriffen zu schützen, ist die Aktivierung der Zwei-Faktor-Authentifizierung. Auf diese Weise können Ihre Anmeldedaten nicht für den Zugriff auf Ihren Account genutzt werden, sollten sie in die falschen Hände geraten.

Twitter:

32 Millionen Twitter-Benutzernamen und Passwörter wurden für 10 Bitcoins bzw. rund 6.000 Dollar zum Kauf angeboten. Die Social-Media-Seite bestritt, dass die Accounts von ihrem Server gestohlen wurden. Die Passwörter waren im Klartext gespeichert und die meisten von ihnen gehörten russischen Usern. Das lässt darauf schließen, dass sie über Phishing-Attacken gestohlen worden sein könnten oder möglicherweise mithilfe von Trojanern.

vk.com:

Das "russische Facebook" musste den Verkauf von Daten von 100 Millionen seiner Nutzer miterleben. Zu den Informationen gehörten E-Mail-Adressen, Namen, Postanschriften, Telefonnummern und Passwörter. Dies ähnelt dem LinkedIn-Fall, mit der Ausnahme, dass in hier die Daten, die vor Jahren gestohlen wurden, gegenwärtig zum Verkauf stehen.

Instagram:

Sicherheitsberater Arne Swinnen fand eine Sicherheitslücke bei Instagram, die es möglich machte, dass 20 Millionen der Accounts kompromittiert wurden. Nachdem er dies gemeldet hatte, erhielt der Ermittler von Facebook (dem Besitzer von Instagram) eine Belohnung in Höhe von 5.000 Dollar im Rahmen des Bonusprogramms. Das ist nicht die höchste Belohnung, die es in diesem Quartal gab. Facebook zahlte einem Zehnjährigen aus Finnland 10.000 Dollar. Das finnische Wunderkind fand eine Sicherheitslücke, die es möglich machte, Kommentare in allen Instagram-Accounts zu löschen.

MySpace:

Erinnern wir uns an die Social-Media-Seite MySpace. Heutzutage gehört sie nicht mehr zu den meistverwendeten, aber sie war dennoch anfällig für eine Attacke, die Millionen Nutzer betraf. Der Vorfall ereignete sich bereits 2013, doch er wurde erst im Mai dieses Jahres entdeckt. Bei diesem Angriff wurden Benutzernamen, Passwörter und E-Mail-Adressen gestohlen. Es heißt, dass mehr als 360 Millionen Konten kompromittiert wurden. Vielleicht haben Sie sich schon seit Jahren nicht mehr bei MySpace eingeloggt. Doch wenn Sie zu denjenigen gehören, die Ihre Benutzernamen und Passwörter wiederverwenden, ist es jetzt Zeit, diese zu ändern und die Vorteile der Zwei-Faktor-Authentifizierung zu nutzen.

Wenn Sie uns nicht glauben, fragen Sie einfach Mark Zuckerberg, den Gründer von Facebook. Zuckerberg stellte fest, dass Konten auf Twitter, Pinterest und Instagram von ein paar Witzbolden gehackt wurden, die sich selbst OurMine nannten. Offensichtlich wurde das Passwort für LinkedIn auch für alle anderen Accounts genutzt, was es für OurMine einfach machte, Zugriff auf alle Konten zu erhalten.

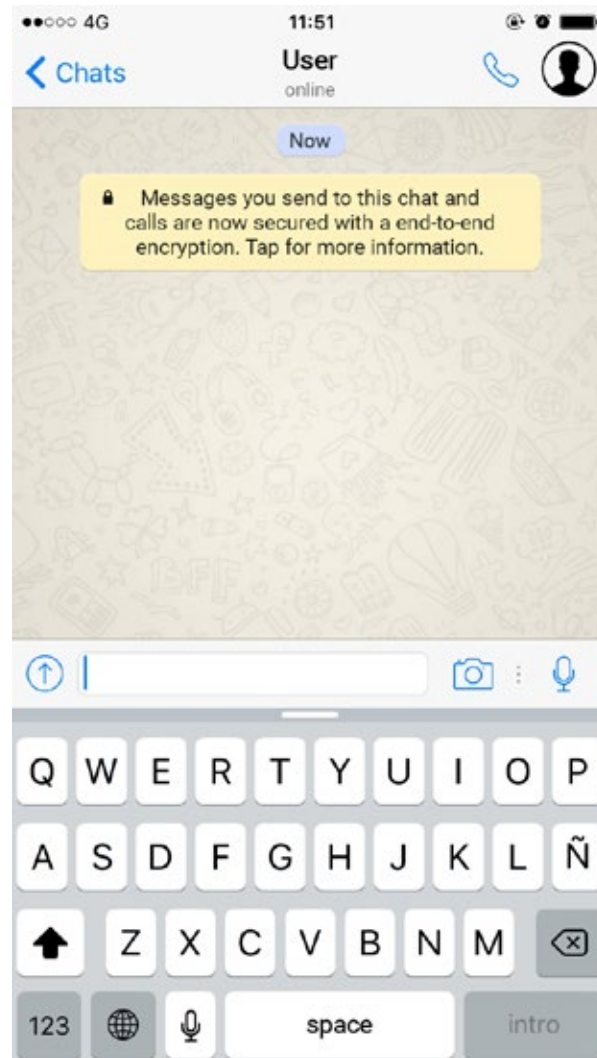
Die Aktivierung der Zwei-Faktor-Authentifizierung und die Nutzung von verschiedenen Passwörtern für unterschiedliche Webseiten sind zwei wichtige Ratschläge, die man befolgen sollte.

Außerdem ist es wichtig, komplexe Passwörter zu verwenden. Eine Studie von Kore Logic, bei der 117 Millionen Passwörter überprüft wurden, zeigte, dass sich die Mehrheit der Nutzer für äußerst einfache Kennwörter entscheidet. Die zehn am häufigsten genutzten Passwörter finden Sie in der folgenden Tabelle:

# ANZAHL DER NUTZER	PASSWORT
1.135.936	123456
207.488	linkedin
188.380	password
149.916	123456789
95.854	12345678
85.515	111111
75.780	1234567
51.969	654321
51.870	qwerty
51.535	sunshine

In dieser Hinsicht müssen wir der Initiative von Microsoft Beifall zollen, denn diese verbietet die Verwendung von häufig genutzten Passwörtern, die in solchen Listen zu finden sind. Wir hoffen, dass viele andere diesem Beispiel folgen werden.

Der Eigentümer der beliebtesten Messaging-App der Welt, Facebook, beschloss, die Sicherheit der Nutzer zu erhöhen, und zwar durch das Verschlüsseln aller über diese App versandten Nachrichten. Diese Pläne werden in den kommenden Monaten auch den Facebook Messenger einschließen.



Mobilgeräte

Es scheint, dass Google große Anstrengungen unternimmt, wenn es um das Patchen aller Sicherheitslücken in seinen Betriebssystemen geht. Mit monatlichen Updates zum Beheben neu entdeckter Schwachstellen gelang es ihnen, allein im Mai 25 Sicherheitslücken zu korrigieren. Obwohl es so aussieht, als sei keine dieser Schwachstellen von Angreifern ausgenutzt worden, ist dies eine der größten Update-Aktionen von Google bisher.

Trotz aller Verbesserungen ist das Android-System noch immer stark gefährdet.

Zweifelsohne ist eines der größten Probleme von Android, dass Updates zu lange auf sich warten lassen, was zum Großteil an den Hardware-Herstellern der verschiedenen Android-Geräte liegt. Während Produkte, die direkt von Google produziert werden, diese Updates nahezu sofort erhalten, (zum Beispiel Nexus Mobiltelefone und Tablets), müssen andere Android-Nutzer Monate warten, bis sie die Patches erhalten. In einigen Fällen kommen diese Patches nie an.

Die fehlenden Updates machen die Geräte anfälliger für bekannte Sicherheitsprobleme und da die Angriffe zunehmen, ist dies für das Android-System wirklich gefährlich.

Internet der Dinge

Neuerdings gibt es in diesem Bereich fast immer Neuigkeiten über gehackte Autos. Diesmal war der Mitsubishi Outlander an der Reihe. Dieses Hybridfahrzeug hat sein eigenes Wi-Fi-Netzwerk, das sich mit einer App verbindet, über die man die Temperatur und andere Einstellungen ändern kann. Der Security-Ermittler Ken Munro entdeckte das Passwort für das Wi-Fi-Netzwerk mittels eines Brute-Force-Angriffs. Nachdem er in das Netzwerk gelangt war, konnte Munro das Auto sabotieren (zum Beispiel indem er die Batterie des Elektromotors vollständig entlud). Noch schwerwiegender ist, dass er den Alarm aus der Ferne deaktivieren konnte. Das ist etwas, das von Verbrechern ausgenutzt werden könnte.

Das Beratungsunternehmen Gartner hat einen interessanten Bericht über die Sicherheit im Internet der Dinge veröffentlicht. In diesem wird vorhergesagt, dass 25 Prozent der Angriffe auf Unternehmen bis zum Jahre 2020 unter Einbeziehung von internetfähigen Geräten erfolgen werden. Es wird erwartet, dass 2016 bereits 6,4 Milliarden dieser Geräte mit dem Internet verbunden sein werden (30 % mehr als 2015), und für 2018 hat man eine Gesamtzahl von 11,4 Milliarden prognostiziert.

Die Ausgaben für die Sicherheit des Internets der Dinge werden sich schrittweise erhöhen. Wenn man jedoch die Vorhersagen in der folgenden Tabelle in Betracht zieht, wird es wahrscheinlich nicht genug sein:

Geschätzte weltweite Ausgaben für die Sicherheit des Internet der Dinge
(in Millionen Dollar)

2014	2015	2016	2017	2018
231.86	281.54	348.32	433.95	547.20

Quelle: Gartner (April 2016)

Cyberkrieg

Im vergangenen Jahr berichteten wir darüber, wie das Unternehmen Hacking Team kompromittiert wurde. Diese Firma ist bekannt, weil sie Tracking Software (Malware) an Regierungen und Sicherheitskräfte auf der ganzen Welt verkauft. Sie kamen in die Schlagzeilen, als die italienische Zeitung "Il Fatto Quotidiano" berichtete, dass das "Hacking Team" seine Exportlizenz verloren hätte, was es ihnen fast unmöglich mache, ihre Programme außerhalb der Europäischen Union zu verkaufen, zumindest ohne langwierige bürokratische Verfahren durchlaufen zu müssen.



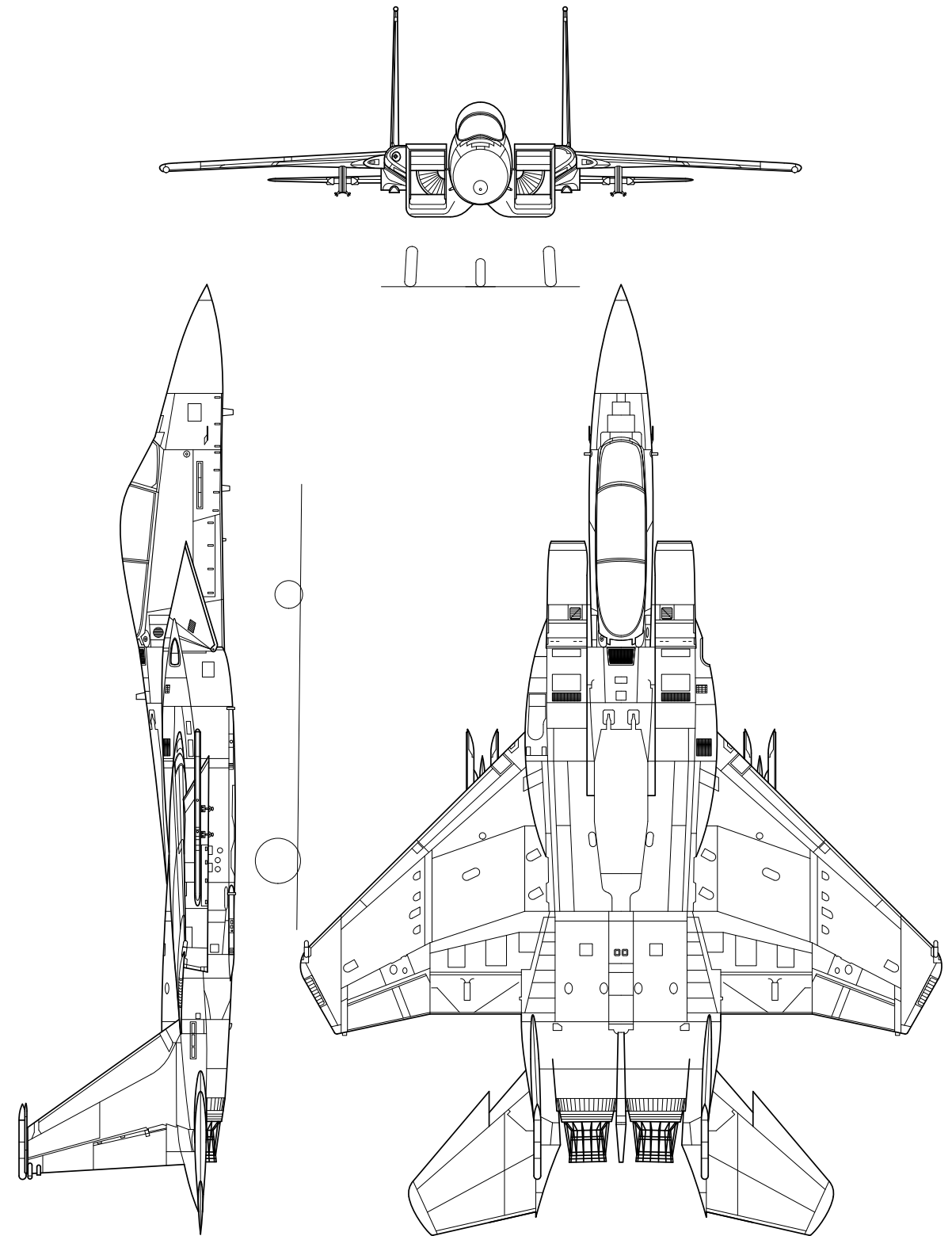
Wenn wir in der Mehrheit dieser Fälle von Cyberkrieg sprechen, reden wir über Attacken, die wahrscheinlich von verschiedenen Ländern gesponsert werden, auch wenn kaum Beweise dafür zu finden sind, wer für den jeweiligen Angriff verantwortlich ist.

Jedoch sind die USA in die Offensive gegangen und haben zugegeben, dass sie Cyberattacken gegen die Organisation Der Islamische Staat (ISIS) starten. Robert Work, stellvertretender Verteidigungsminister der USA, sagte:

“Wir werfen Cyberbomben ab. Das haben wir noch nie zuvor getan. Genauso wie wir Luftwaffeneinsätze haben, will ich, dass wir Cyberangriffe führen. Ich will dafür alle Kapazitäten einsetzen, die ich habe.”

Im Juni machte die Polizeibehörde von Südkorea einen Angriff von Nordkorea öffentlich. Es scheint, dass die Attacke vor über einem Jahr begann und sich auf 140.000 Computer von Regierungsorganisationen und Rüstungskonzernen konzentrierte. Dieser Angriff wurde erst im Februar entdeckt. Laut Polizeiberichten wurden mehr als 42.000 Dokumente gestohlen, von denen 95 Prozent verteidigungsbezogen waren, wie zum Beispiel die Pläne und Spezifikationen der Flügel des amerikanischen F 15 Fighters.

Das US Democratic National Committee bestätigte, dass seine Systeme ein Jahr lang (vielleicht auch länger) kompromittiert waren. Man glaubt, dass die Angreifer zum russischen Geheimdienst gehören. Die Hacker hatten Zugriff auf E-Mails, Chats und alle Arten von Forschungsarbeiten. Es wurde auf alle Computer der Untersuchungsabteilung zugegriffen und einige Dateien wurden gestohlen.



3. FAZIT

3

Fazit

Die Anzahl der Angriffe, mit denen Daten und Geld gestohlen werden, steigt weiter an. User erleben den Diebstahl ihrer Identitäten oder Accounts. Häufig werden sie nicht direkt angegriffen. Stattdessen werden ihre Informationen in Datenbanken kompromittierter Firmen entdeckt.

Zudem verwenden einige Nutzer ihre Passwörter mehrfach, was den Diebstahl ihrer Daten vereinfacht. Dieses Problem könnte recht einfach gelöst werden, indem man die Zwei-Faktor-Authentifizierung aktiviert, die bereits von den meisten Webseiten angeboten wird. Eine weitere Möglichkeit wäre, dass Service Provider von ihren Usern verlangen, diese Sicherheitsmaßnahmen zu aktivieren. Doch momentan ist das eher unwahrscheinlich, da der Benutzerfreundlichkeit immer noch eine höhere Priorität eingeräumt wird als der Sicherheit.

Ransomware-Attacken sind oftmals auf einem hohen Stand der Technik. Hacker machen große Profite damit. In den kommenden Monaten werden wir sehen, wie diese Angriffe weiterhin zunehmen.



Ein anderer besorgniserregender Trend ist der Diebstahl von Kreditkarteninformationen über POS-Terminals. Davon sind hauptsächlich kleine Unternehmen wie Restaurants, Bars usw. betroffen, die häufig kein engagiertes IT-Sicherheitsteam haben, auf das sie sich verlassen können. Wenn man in Betracht zieht, wie einfach es ist, diese Informationen auf dem „Schwarzmarkt“ gewinnbringend zu verkaufen, erscheint es logisch, dass diese Methode von Cyberkriminellen weiterhin genutzt werden wird.

4. ÜBER PANDALABS

4

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.



Dieser Bericht darf ohne die vorherige schriftliche Genehmigung von Panda Security weder im Ganzen noch in Teilen vervielfältigt, reproduziert, in einem Datenabrufsystem gespeichert oder neu übertragen werden.

© Panda Security 2016 Alle Rechte vorbehalten.

