Globaler Bedrohungsbericht

JAHRESMITTE 2018

MobileIron

401 East Middlefield Road
Mountain View, CA 94043, USA
globalsales@mobileiron.com
www.mobileiron.com
Tel.: +1.877.819.3451
Fax: +1.650.919.8006

MKT DE-A4 v1

Globale Bedrohungsdaten

1. Januar – 30. Juni 2018

In der ersten Jaheshälfte 2018 wurden verschiedene Arten von Risiken und Bedrohungen für Mobilgeräte in aller Welt erkannt. Die Risiken und Bedrohungen sind wie folgt kategorisiert (und werden oft als mobile „DNA"-Bedrohung bezeichnet):

GERÄTEBEDROHUNGEN UND RISIKEN

Bedrohungen für das Gerät oder Betriebssystem, beispielsweise durch Sicherheitslücken, für die keine Patches installiert wurden.

NETZWERK-BEDROHUNGEN

Bedrohungen gelangen über das Funknetz oder das WLAN auf das Gerät

APP-BEDROHUNGEN

Mobile Malware, Spyware, Adware oder „undichte Apps" auf Geräten

Haupterkenntnisse:

- Jeder Kunde stellt Bedrohungen für mobile Betriebssysteme fest.
- MITM-Angriffe sind im Vergleich zur letzten Jahreshälfte angestiegen.
- Jedes dritte Gerät erkannte eine mobile Bedrohung.

Mobile Bedrohungen existieren überall

Offengelegte Sicherheitslücken

Immer wenn Sicherheitslücken für Mobilgeräte und Apps mit Schadsoftware bekannt werden, kommt die Frage, ob wir Schutz gegen BankBot, BroadPwn, KRACK, Meldown, Spectre und andere Angriffe bieten, die gerade Gesprächsstoff sind. Die Antwort lautet „ja“, weil unser auf künstlicher Intelligenz basierendes Modul Angriffe sowohl auf Geräte als auch Netzwerke und Apps erkennt. Die meisten Angriffe auf Mobilgeräte nutzen Sicherheitslücken in Geräten, Netzwerken und Apps sowie bestimmte Verfahren, sogenannte „kill chains“; diese Angriffe können in allen drei Phasen unabhängig davon erkannt werden, auf welchen kreativen Wegen sie auf das Gerät gelangen. Wenn eine Störung in Ihrem Betriebssystem auftritt, wird sie sofort über unser Modul zur Erkennung von Bedrohungen diagnostiziert.

Im letzten Quartal wurden mehrere Sicherheitslücken auf dem Markt bekannt. Bei jeder konnte sich ein cleverer Angreifer auf sehr komplizierte Weise Zugang zu Ihrem Gerät verschaffen, eine App übernehmen oder den WLAN-Traffic abhören.

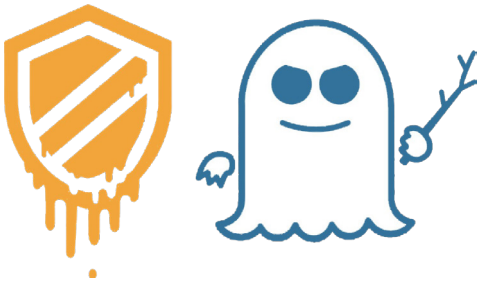
Meltdown und Spectre

Nach Angaben des Teams an der Technischen Universität Graz, das verantwortungsbewusst die neuen Sicherheitsprobleme veröffentlichte, nutzen Meltdown und Spectre kritische Sicherheitslücken moderner Prozessoren. Aufgrund dieser Hardwarefehler können Programme Daten stehlen, die gerade im Computer verarbeitet werden. Zwar wird es Programmen in der Regel nicht erlaubt, Daten anderer Programme zu lesen, doch eine Schadsoftware kann mit Meltdown und Spectre die im Speicher anderer laufender Programme abgelegten geheimen Informationen lesen. Dies können beispielsweise in einem Passwortmanager oder Browser gespeicherte Passwörter sein, private Fotos, E-Mails, Sofortnachrichten, aber auch wichtige geschäftliche Dokumente.

Meltdown (CVE-2017-5754)

Meltdown wird so bezeichnet, weil diese Sicherheitslücke die Grenzen, die normalerweise durch die Hardware durchgesetzt werden, faktisch wegschmelzen lässt. Meltdown durchbricht die fundamentale Trennung zwischen den Benutzeranwendungen und dem Betriebssystem. Da der Angreifer hierbei Zugriff auf den Speicher und seine Daten hat, kann er auch auf Daten anderer Programme und das Betriebssystem zugreifen.

Nach den Berichten sind möglicherweise alle Intel-Prozessoren seit 1995 (mit Ausnahme von Intel Itanium und Intel Atom vor dem Jahr 2013) von Meltdown betroffen. ARM-Prozessoren sind ebenfalls betroffen, nicht jedoch AMD-Prozessoren, da nach Angaben von AMD deren Architektur anders ist.



Spectre (CVE-2017-5753 und CVE-2017-5715)

Spectre erhielt seinen Namen aufgrund seines Verhaltens, der spekulativen Ausführung. Spectre lässt sich nicht so einfach beseitigen. Wie der Name schon vermuten lässt, ist Spectre nicht leicht zu fassen und wird die Forscher noch geraume Zeit beschäftigen. Spectre durchbricht die Trennung zwischen verschiedenen Anwendungen und ermöglicht es dem Angreifer, Daten auch aus fehlerfreien Programmen auszulesen.

Fast jedes System ist von Spectre betroffen.
Eine Sicherheitslücke für Spectre wurde insbesondere bei Prozessoren von Intel, AMD und ARM festgestellt. Außerdem ist bekannt, dass weitere Sicherheitsprobleme für andere Architekturen existieren. Dies betrifft das IBM-System Z, POWER8 (Big Endian und Little Endian) sowie POWER9 (Little Endian).

Schutz von Mobilgeräten vor Sicherheitslücken für Meltdown und Spectre

Patches des Betriebssystems

Sowohl Apple als auch Google betonen, dass derzeit keine Kunden bekannt sind, die Sicherheitsprobleme haben. Um solche Sicherheitsprobleme zu vermeiden, haben sowohl Apple als auch Google Patches bereitgestellt. Apple-Benutzer sollten mindestens auf iOS-Version 11.2 wechseln, um sich gegen Meltdown zu schützen. Nach Angaben von Apple lässt sich Spectre zwar nur extrem schwierig als Schadprogramm einsetzen, selbst wenn eine App lokal auf Mac- oder iOS-Geräten läuft. Spectre kann jedoch möglicherweise über Javascript in einem Web-Browser genutzt werden. Infolgedessen plant Apple Einschränkungen für den Safari-Webbrowser, die in Kürze vor Spectre schützen sollen.

Android-Benutzer sollten mit dem Sicherheits-Patch 2018-01-05 oder höher arbeiten, das am 5. Januar als Teil des Sicherheits-Patch-Updates vom Januar 2018 von Android veröffentlicht wurde.

Bluetoothd daemon

Sicherheitsprobleme im bluetoothd daemon von Apple

Wir analysierten iOS Mach message IPC, insbesondere die Dienste, die aus der iOS Sandbox heraus zugänglich um zu klären, ob es potenziell Möglichkeiten gibt, Berechtigungen hochzusetzen und aus der Sandbox auszubrechen, die ein wesentlicher Bestandteil der vollständigen iOS-Sicherheitskette ist.

Wir fanden zwei wesentliche Sicherheitslücken im bluetoothd daemon bei iOS, webOS und tvOS, die mit CoreBluetooth zusammenhängen. Die erste Sicherheitslücke ist ein Speicherfehler in bluetoothd, die zweite die Ausführung von willkürlichem Code auf verschiedenen wichtigen daemons.

Die erste Sicherheitslücke (CVE-2018-4095) betrifft eine vollständige relative Steuerung (ASLR-Bypass) im Stack von CoreBluetooth, die zu einem Speicherfehler über bluetoothd führt.

Die zweite wesentliche Sicherheitslücke (CVE-2018-4087) führt zur Ausführung von beliebigem Code auf verschiedenen wichtigen daemons in iOS, indem die Sitzung zwischen dem daemon und bluetoothd gekapert wird. Einige der betroffenen daemons sind: SpringBoard, mDNSResponder, aggregated, wifid, Preferences, CommCenter, iaptransportd, findmydeviced, routined, UserEventAgent, carkitd, mediaserverd, bluetoothd, coreduetd usw.

MobileIron

ZipperDown

Sicherheitslücke ZipperDown: 100 Mio. iOS-Benutzer gefährdet

Sicherheitsanalysten der iOS Jailbreak-Firma Pangu Lab informierten über eine Sicherheitslücke, die ihrer Meinung nach etwa 10 % aller iOS-Apps betrifft. In einem Blogartikel der neu erstellten Informationswebsite https://zipperdown.org informierte Pangu, dass seine Analysten einen allgemeinen Programmierfehler festgestellt hätten, der im Zusammenhang mit betroffenen Apps schwerwiegende Konsequenzen hat, beispielsweise Daten überschreibt und sogar Programmcode ausführt. Pangu berechnete, dass die infizierten Apps mindestens 100 Mio. Benutzer gefährden könnten. Damit keine Details des Programmfehlers bekannt werden, bezeichnete Pangu ihn als „ZipperDown".

Vorläufige ZipperDown-Analyse

Nach Angaben von Pangu sind zum Schutz der Endbenutzer Details von ZipperDown bisher für die Öffentlichkeit nicht zugänglich. Unserer Ansicht nach liegt das Problem in der Bibliothek eines Drittanbieters, die viele Apps nutzen. Bei ZipperDown geht es nicht um Malware, sondern um eine Sicherheitslücke, die bei verschiedenen Apps für einen MITM-Angriff im Netzwerk genutzt werden könnte.

So bekämpft MobileIron ZipperDown

MobileIron Threat Defense erkennt MITM-Attacken und die Sicherheitsprobleme, die ZipperDown nutzen kann, und kann die Ausführung durch Durchsetzung einer kundendefinierten Richtlinie verhindern.

Die auf dem Gerät laufende Erkennungssoftware MobileIron Threat Defense arbeitet mit künstlicher Intelligenz und hat zahlreiche Vorteile. Einer der Hauptvorteile ist die Erkennung der „kill chain", wobei unsere Lösung die verschiedenen Phasen der Angriffe auch ohne Aktualisierung oder Signaturen erkennt. In diesem Fall erkennt unsere Lösung MITM-Attacken und Sicherheitsprobleme, mit denen versucht wird, Benutzerrechte zu erhöhen, um das Gerät zu kapern.

Cryptojacking

Das illegale Mining von Crypto-Währungen, das sogenannte Cryptojacking, ist in diesem Jahr geradezu explodiert. Cryptojacking wird nicht nur genutzt, um digitale Währungen und Wallets von Mobilgeräten zu stehlen; am häufigsten ist die unkontrollierte Nutzung von Rechenleistung der CPU, GPU, DRAM und ASIC infizierter Geräte, um Crypto-Währungen zu schürfen. Dadurch ist der Akku der Mobilgeräte schneller erschöpft und die Stromrechnung steigt, weil häufiger aufgeladen werden muss. In einem Fall kam es bei einem Android-Gerät zu einer Überhitzung und Verformung, weil der Prozessor längere Zeit mit Höchstgeschwindigkeit betrieben wurde. Die häufigste JavaScript-Schadsoftware, die sich Geräte beim Surfen im Web einfangen können, ist das CoinHive-Mining-Skript, das auf fast 94 % aller infizierten Websites zu finden ist. Coinhive wird vor allem zum Mining der Crypto-Währung Monero eingesetzt, BitCoin dagegen erfordert mehr Rechenleistung. Nach dem aktuellen Stand gibt es über 50.000 infizierte Websites, darunter auch einige beliebte und öffentliche Webseites, die infiziert sind.

MobileIron Threat Defense erkennt Malware, die Cryptojacking-Skripte enthält. Außerdem können Internetbenutzer die Erweiterungen zur Erkennung von Cryptojacking für ihren Webbrowser (beispielsweise Google Chrome) installieren.

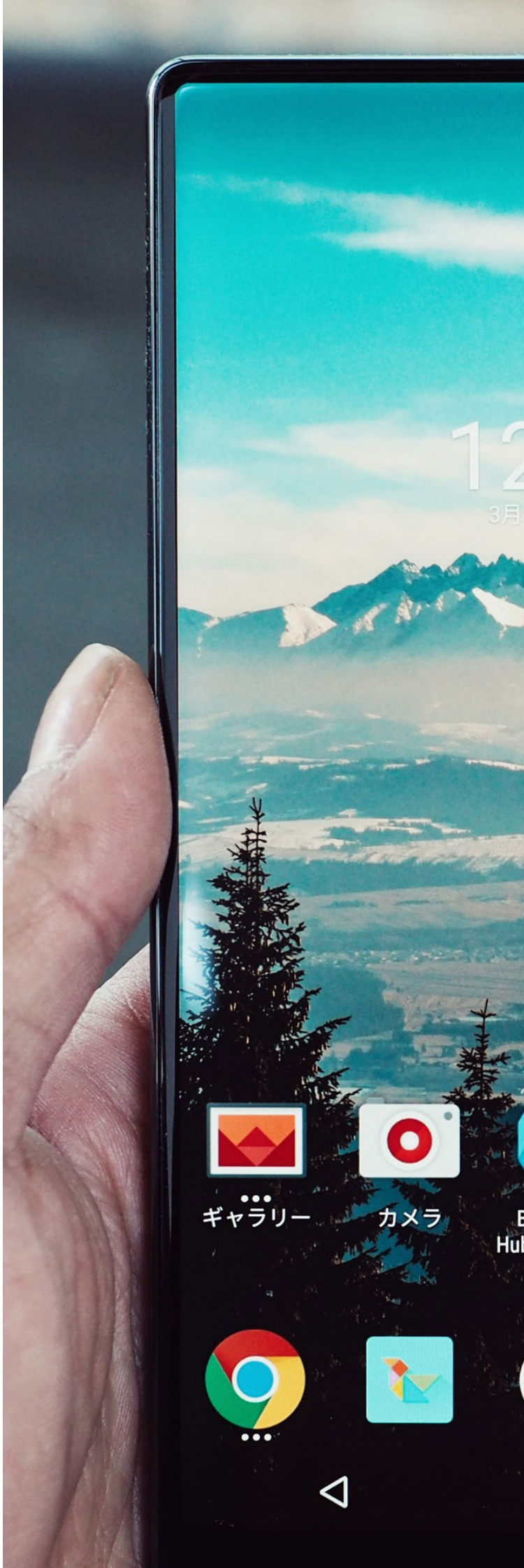
Neues zu den Updates von Apple und Google

Sicherheits-Updates und Patches

In der ersten Jahreshälfte 2018 gab Apple sechsmal kleinere und größere Updates für iOS frei. Insgesamt wurden mit diesen Sicherheitsupdates 110 CVEs beseitigt, von kleineren Grafikupdates bis zu wichtigen Browser- und Kernel-Updates. 2017 wurden 387 CVEs festgestellt. Dies sind genauso viele wie für iOS im ganzen Jahr 2015 ermittelt wurden. Apple erzwingt Sicherheitsupdates auf Telefonen sehr effektiv und stellt schnell die neuesten Patches zur Verfügung. Die Benutzer müssen jedoch ein Update auf die aktuelle Version des Betriebssystems durchführen.

Google veröffentlichte für die Zeit zwischen Januar 2018 und Juni 2018 insgesamt sechs Android-Sicherheitsmitteilungen. Insgesamt gab es Updates für 495 CVEs, von denen 48 als kritisch eingestuft wurden. Google informierte die Benutzer in dem Update vom Januar 2018 über Sicherheitspatches für Meltdown und Spectre. Dies war ein hochkritisches Update, mit dem Sicherheitslücken in der CPU und auf Hardware-Ebene beseitigt werden sollten.

Das Update vom April 2018 betraf 311 CVEs, darunter viele, die mit Sicherheitsproblemen für Qualcomm-Firmware aus dem Jahr 2014 zusammenhängen. Die Updates zu den Sicherheitslücken in Qualcomm-Komponenten teilte Qualcomm mit seinen Partnern über die Qualcomm AMSS Sicherheitsmitteilungen bzw. Sicherheitswarnungen zwischen 2014 und 2016. Sie waren Bestandteil der Android-Sicherheitsmitteilung vom April mit dem betreffenden Sicherheits-Patchlevel.



MobileIron

Welche Geräte wurden angegriffen? Wie und wann?

Geräterisiken und Bedrohungen

Die Analyse der Mobilgeräte zeigte, dass Unternehmen ihre Geräte weiter mit verfügbaren Sicherheits-Patches aktualisieren. Ältere Versionen jedes Betriebssystems gab es bei weniger Geräten, die Geräte waren damit weniger anfällig für bekannte Sicherheitslücken als in den vorherigen Quartalen. Auch wenn viele Kunden über UEM-Pakete zur Überwachung der Betriebssystemversionen verfügen, werden die Geräte nicht unbedingt sofort aktualisiert, sobald Sicherheitspatches verfügbar sind.

Wir betrachten jedes Betriebssystem separat, da jedes sein eigenes Ökosystem und seinen eigenen Updatezeitplan hat. iOS-Geräte werden von unseren Kunden bevorzugt eingesetzt. Wir haben festgestellt, dass die Updates auf diesen Geräten schnell installiert werden. Das letzte wesentliche Update für iOS ist das Release 11.4 vom 29. Mai 2018. Bei über der Hälfte der iOS-Geräte (51,9 %) ist das aktuelle Update installiert. Auf den übrigen Geräten ist die Vorversion bzw. die Vorvorversion installiert. 26,5 % der iOS-Geräte arbeiten noch mit Version 11.3, die übrigen 21,5 % mit Version 11.2 oder noch älteren Versionen.

Auf den meisten Android-Geräten läuft Android 6, 65 % der Geräte arbeiten mit der Version Marshmallow und 16 % mit Android-Version 7 (Nougat). Viele Analysten weisen darauf hin, dass Marshmallow die Mindestversion ist, die in Unternehmen im Netzwerk verwendet werden sollte. Dreizehn Prozent (13,8 %) der Android-Geräte arbeitet mit der neuesten Version Android 8 (Oreo). Die übrigen 4 % der Android-Geräte arbeitet mit Lollipop oder noch älteren Versionen des Betriebssystems.

Wir analysierten, wie sicher diese Geräte sind und wie sie konfiguriert sind. Wir halten Geräte dann für hochriskant, wenn bestimmte Einstellungen zum Datenschutz und zur Sicherheit deaktiviert sind. Zu den hochriskanten Einstellungen, die wir analysierten, gehörten die Aktivierung der Entwickleroptionen, Jailbreaks oder Roots auf dem Gerät und die Datenschutzeinstellungen, beispielsweise die Verschlüsselung und Absicherung mit PIN-Codes.

Bei 38 % der Geräte existieren unnötige Risiken

Extrem gefährdet waren Geräte mit deaktivierter Code-Signatur, welche die Installation von Apps aus unbekannten Quellen erlaubten oder deren Profile manipuliert waren. Bei nur 1 % dieser Geräte waren die iOS-Konfigurationsprofile manipuliert, sodass mit dem Gerät Daten gestohlen werden konnten. Weiter stellen wir fest, dass diese Profile mit Apps verknüpft sind, die die Benutzer bei der Installation täuschen, um das Gerät zu gefährden oder RATs (Trojaner für den Fernzugriff) zu installieren.

Wir maßen das statische Konfigurationsrisiko und die aktiven Bedrohungen unabhängig voneinander, da die Mobilitätteams oft getrennte Richtlinien je nach Geräterisiko, Benutzerprofilen oder Benutzerrollen verwalten. Diese Teams möchten wissen, welche Geräte am stärksten gefährdet sind, damit sie diese in Sondergruppen eingliedern oder anders bezeichnen können. Die Kunden möchten natürlich wissen, welche Geräte wie und wann angegriffen wurden.

In der ersten Jahreshälfte 2018 wurden bei 31 % der aktiven Geräte Bedrohungen erkannt. Der Schweregrad der Bedrohung wurde unter Berücksichtigung der Risikotoleranz konfiguriert und ist in diesem Bericht nicht ausgewiesen. Manche Kunden dämmen eine Bedrohung automatisch ein, andere markieren diese nur zur weiteren Untersuchung. Alarmierend war, dass fast 4 % der Geräte zur Ausspähung auf interne Netze zugriffen oder sich bei einem unsauber konfigurierten Zugangspunkt anmeldeten. **Diese Fakten zeigen deutlich, dass Cyber-Kriminelle in zunehmendem Maße in Unternehmen genutzte Mobilgeräte zur Ausspähung nutzen.**

MITM-Angriffe im WLAN sind real

Netzwerkbedrohungen und Angriffe

Zu den gefährlichsten Bedrohungen zählen Man-in-the-Middle-Angriffe (MITM) und unsauber konfigurierte Zugangspunkte, mit denen ein Angreifer den Traffic im Netzwerk eines Mobilgeräts abfängt. Der Angreifer hat damit die Möglichkeit, Anmeldeinformationen, E-Mails, Kalenderdaten, Kontakte und andere sensible Daten zu lesen und zu erfassen und auf diese Weise einen spezifischeren Angriff vorzubereiten.

In der ersten Jahreshälfte 2018 erkannte nach unseren Daten jedes siebente Gerät eine MITM-Attacke (14,88 %). Die gestohlenen Daten können als Teil eines Angriffes auf den Benutzer, den Arbeitgeber oder für Betrug verwendet werden. Die Erkennung einer MITM-Attacke bedeutet noch nicht, dass diese erfolgreich war.

Sie weist allerdings auf einen erfolgreichen MITM-Versuch hin. Hätte der Benutzer nicht die App MobileIron Threat Defense auf seinem Gerät installiert, wäre der Angriff weder bemerkt noch erfasst worden. Wenn die Benutzer keine App zur Abwehr mobiler Bedrohungen installiert haben, welche die Angriffe auf ihre Geräte in Echtzeit erkennen kann, können ihre WLAN-Verbindungen auf einen Proxy umgeleitet und ihre Daten gefährdet werden. Die gestohlenen Daten können als Teil eines Angriffs auf den Benutzer, dessen Arbeitgeber oder für Betrug genutzt werden.

Unsauber konfigurierte Zugangspunkte, d. h. Zugangspunkte, die in einem sicheren Netzwerk ohne ausdrückliche Autorisierung durch den Administrator des lokalen Netzwerks installiert wurden, sind eine andere häufige Angriffsart auf Netzwerke, bei denen der Traffic umgeleitet wird. Unsauber konfigurierte Zugangspunkte können überall platziert werden. In der Regel verwenden sie vertraute Namenskonventionen, um den Traffic eines potenziellen Ziels abzugreifen. Ein unsauber konfigurierter Zugangspunkt in der Nähe eines Hotels oder eines Bürostandorts kann beispielsweise den tatsächlichen Namen verwenden, um ahnungslose Opfer zu täuschen.

Fast 2 % der Geräte war mit einem unsauber konfigurierten Zugangspunkt verbunden

MobileIron Threat Defense kann unsauber konfigurierte Zugangspunkte erkennen, dem Sicherheitsteam des Unternehmens melden und automatisch die Sitzung beenden, wenn diese Aktion durch die Sicherheitsrichtlinie vorgeschrieben und konfiguriert ist. Es wurden zusätzliche unsaubere Zugangspunkte in der Nähe erkannt, ein Verbindungsaufbau durch die betreffenden Mobilgeräte erfolgte jedoch nicht.

App-Bedrohungen sind real

Unternehmen und Benutzer sind nach wie vor besorgt wegen mobiler Apps und mobiler Malware, weil sie durch die konventionellen Antivirus-Softwarepakete bereits geschult sind. Es wird nach einer bekannten Malware-Datei gesucht und diese entfernt.

Das Problem bei diesem Konzept für Mobilgeräte ist, dass sich die mobilen Betriebssysteme weiterentwickeln und Funktionen sehr schnell ergänzt werden. Bei mobilen Betriebssystemen werden jedes Jahr Millionen Programmzeilen ergänzt und daher unbeabsichtigt Konsequenzen, Bugs und Sicherheitslücken verursacht.

2017 wurden für Android und iOS mehr CVEs registriert als für die Jahre 2016 und 2015 zusammen.

2017 wurden für mobile Betriebssysteme 1228 CVEs verzeichnet. Über die Hälfte dieser CVEs wurden mit 7 oder mehr Punkten bewertet, das heißt, es handelte sich um schwerwiegende Sicherheitslücken, die von Angreifern genutzt werden könnten. Wir rechnen damit, dass dieser Trend sich 2018 fortsetzt, da die mobilen Betriebssysteme immer ausgereifter werden und laufend weitere Funktionen hinzukommen.

Sicherheitsbewusste Organisationen verfeinern ihre Sicherheitsrichtlinien und Schulungsprogramme laufend, um das IT-Risiko zu reduzieren. Trotz aller Schulungen und Programme zur Erhöhung des Problembewusstseins finden die Benutzer immer noch Möglichkeiten, Sicherheitsrichtlinien und Kontrollen zu umgehen. Aus diesen Gründen entscheiden sich Unternehmen dafür, ihre Risiken durch Installation mobiler Sicherheitslösungen auf den mitarbeitereigenen und unternehmenseigenen Geräten zu reduzieren.

In der ersten Jahreshälfte 2018 identifizierten wir bekannte Apps mit Schadsoftware in der Umgebung von tausenden von Geräten. Bei Android-Geräten ist mobile Malware mit Schadsoftware häufiger zu finden. Malware in Apps wurde bei 3,5 % der Geräte festgestellt. Über 80 % der Apps, bei denen Schadsoftware festgestellt wurde, hatten einen Zugriff auf interne Netzwerke und scannten die benachbarten Ports. Solche Sondierungsoperationen sind ein Hinweis auf geplante weitere Malwareangriffe.

Im Februar 2018 wurde eine Fakeversion der legitimen App BBC News aus Google Play heruntergeladen, die bisher unbekannte Malware enthielt. Diese App wurde aufgrund der Technologie zur Erkennung von Bedrohungen als Malware klassifiziert. Erkenntnisse dazu wurden am 1. März 2018 veröffentlicht.

iOS-Malware wird über eine App nur bei 0,1 % aller Geräte übertragen. Bei iOS-Geräten sind häufiger manipulierte Profile auf den Geräten vorhanden, die oft über kostenlose Apps oder als Zusatz-Apps getarnt auf die Geräte gelangen. Ende 2017 zahlte ein Benutzer $15,95 für eine App im App-Store, die verschiedene Spiele anbot. Nach dem Kauf der App erhielt der Benutzer die Aufforderung, eine „Installationssoftware" bzw. eine „Hilfs-App" für die Spiele herunterzuladen. Die „Installations-App" erwies sich als manipuliertes Profil, das das Gerät gefährdete. Die Schadsoftware in dem Profil aktivierte das Gerät für den Download von Apps außerhalb des App Store, ohne dass ein Jailbreak des Gerätes erforderlich war. Das Sicherheitsteam des Unternehmens informierte den Benutzer und wies ihn an, wie er den Angriff eindämmen konnte.

Wenn Sie forensische Details wie oben erwähnt für Ihre Geräte im Unternehmen erhalten möchten, nehmen Sie bitte mit uns Kontakt auf, damit wir geeignete Schritte konfigurieren. Weitere Informationen über MobileIron Threat Defense finden Sie unter www.mobileiron.com/threatdefense.

Quellen:

- Apple iOS 11.2.2 Update
- Apple iOS 11.2.5 Update
- Apple iOS 11.2.6 Update
- Apple iOS 11.3 Update
- Apple iOS 11.3.1 Update
- Apple iOS 11.4 Update
- Android Security Bulletin - Januar 2018
  https://source.android.com/security/bulletin/2018-01-01
- Android-Sicherheitmitteilung - Februar 2018
  https://source.android.com/security/bulletin/2018-02-01
- Android-Sicherheitmitteilung - März 2018
  https://source.android.com/security/bulletin/2018-03-01
- Android-Sicherheitmitteilung - April 2018
  https://source.android.com/security/bulletin/2018-04-01
- Android-Sicherheitmitteilung - Mai 2018
  https://source.android.com/security/bulletin/2018-05-01
- Android-Sicherheitmitteilung - Juni 2018
  https://source.android.com/security/bulletin/2018-06-01
- CVE-Details
  https://www.cvedetails.com/product/15556/Apple-Iphone-Os.html?vendor_id=49
- CVE-Details
  https://www.cvedetails.com/product/19997/Google-Android.html?vendor_id=1224
- MobileIron
  https://www.mobileiron.com

MobileIron

401 East Middlefield Road
Mountain View, CA 94043, USA
globalsales@mobileiron.com
www.mobileiron.com
Tel.: +1.877.819.3451
Fax: +1.650.919.8006