Lookout®

WHITEPAPER

Phishing auf Mobilgeräten: Irrtümer und Fakten im Geschäftsalltag

Mobilgeräte sind für Cyberkriminelle ein profitables neues Einfallstor für Phishing-Angriffe. Dabei umgehen sie erfolgreich konventionelle Phishing-Schutzmechanismen, die Mobilgeräte meist nicht abdecken. Solche Angriffe machen Sicherheitslücken deutlich, die sensible und persönliche Daten in alarmierendem Maße erheblichen Risiken aussetzen.

Die meisten Unternehmen schützen sich mittlerweile mit Firewalls, sicheren E-Mail-Gateways und Virenschutz auf Endgeräten vor Phishing-Versuchen per E-Mail. Darüber hinaus werden die Nutzer immer besser darin, Phishing zu erkennen. Auf Mobilgeräten hingegen haben es nicht nur Menschen, sondern auch die vorhandenen Sicherheitstechnologien schwer, Phishing-Angriffe zu erkennen und zu blockieren.

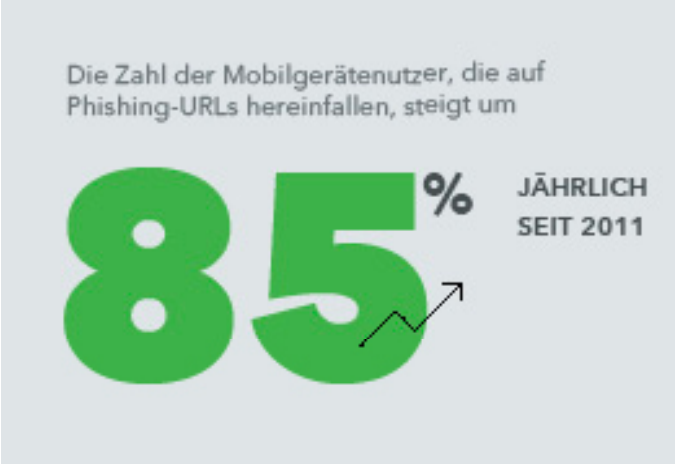
Phishing auf Mobilgeräten ist nicht nur anders, sondern auch problematischer als herkömmliche Phishing-Attacken.

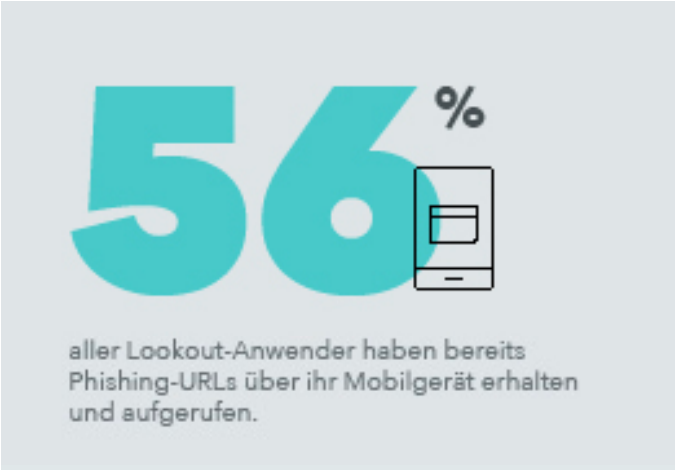
Mobilgeräte bewegen sich außerhalb von schützenden Firewalls, verfügen meist nicht über Endpoint-Sicherheitslösungen und greifen auf eine Vielzahl neuer Messaging-Plattformen zu, die auf Desktops nicht verwendet werden. Darüber hinaus bietet die Nutzerschnittstelle von Mobilgeräten nicht die nötige Detailtiefe, um Phishing-Angriffe erkennen zu können (z. B. indem man den Mauszeiger über Hyperlinks bewegt, um die Ziel-URL anzuzeigen). Demzufolge fallen Mobilgerätenutzer laut IBM dreimal eher auf Phishing-Betrug herein.

Auch die Unmengen von persönlichen und Unternehmensdaten auf Mobilgeräten machen Smartphones und Co. zum neuen Lieblingsziel von Phishern.

Doch trotz aller konventionellen Phishing-Schutzmechanismen und erhöhter Wachsamkeit der Nutzer haben zwischen 2011 und 2016 bereits 56 % aller Lookout-Anwender Phishing-URLs über ihr Mobilgerät erhalten und aufgerufen. Diese Angriffe konnte Lookout glücklicherweise abwehren. Leider jedoch ist seit 2011 die Zahl der Lookout-Anwender, die Phishing-URLs auf ihren Mobilgeräten erhalten und antippen, jährlich um durchschnittlich 85 % gestiegen.

Phishing auf Mobilgeräten ist wesentlich vielschichtiger als viele Unternehmen vielleicht glauben. Um also einen umfassenden Schutz vor Phishing-Angriffen zu erzielen, der wirklich alle Vektoren – auch Mobilgeräte – abdeckt, müssen Sicherheits- und IT-Verantwortliche wissen, welche häufigen Irrtümer zum Thema Phishing den Blick trüben, und sich mit den Fakten vertraut machen. Nur so können sie fundierte Entscheidungen zum Schutz von Unternehmensdaten treffen.





INHALTSVERZEICHNIS

Phishing auf Mobilgeräten – Irrtum Nr. 1

Viele glauben, dass konventionelle Phishing-Schutzmechanismen auch Mobilgeräte abdecken.

Phishing auf Mobilgeräten – Irrtum Nr. 2

Viele glauben, dass sich Phishing-Angriffe nur auf E-Mails richten.

Phishing auf Mobilgeräten – Fakt Nr. 1

Auf Mobilgeräten ist es einfacher, Nutzer in die Phishing-Falle zu locken als auf Desktop-PCs.

Phishing auf Mobilgeräten – Fakt Nr. 2

Entwicklern von Malware für Mobilgeräte, vor allem mAPT-Programmierern, gelingt es, ihre Phishing-Methoden erfolgreich in der Praxis anzuwenden.

Phishing auf Mobilgeräten – Fakt Nr. 3

Unternehmen müssen sich auch darüber Gedanken machen, dass Apps (nicht nur Menschen) unbeabsichtigt Phishing-URLs öffnen und sie nichts ahnenden Mobilgerätenutzern zur Verfügung stellen.

Phishing auf Mobilgeräten – Irrtum Nr. 1

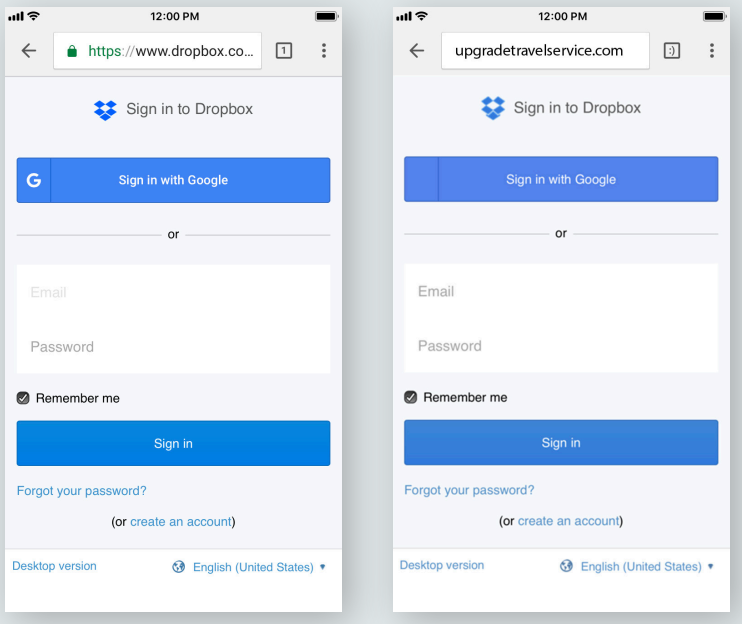
Konventioneller Phishing-Schutz eignet sich auch für Mobilgeräte.

Bisher verhindern Unternehmen, dass Mitarbeiter Phishing-Nachrichten erhalten oder schlimmstenfalls darauf hereinfallen, hauptsächlich durch Firewalls, sichere E-Mail-Gateways, Virenschutz auf Endgeräten und die Aufklärung der Nutzer. Dieser Ansatz funktioniert auch, allerdings nur auf stationären und traditionellen Firmenrechnern, die das Unternehmen selbst verwaltet. Wie jedoch viele CISOs aus eigener Erfahrung wissen, lässt sich dieses Modell nicht einfach auf Mobilgeräte übertragen.

Die meisten Mobilgeräte werden nun einmal auch für persönliche Zwecke verwendet, selbst wenn es sich um Firmengeräte handelt. Mitarbeiter nutzen heute ein und dasselbe Smartphone, um ihr Mittagessen zu bezahlen, eine private E-Mail zu versenden, Familienfotos aufzunehmen, in den sozialen Netzwerken zu kommunizieren, Kundendatensätze einzusehen, Anfahrtsbeschreibungen zu Meetings abzurufen und Finanzberichte zu überfliegen. Neben Reader-Programmen für Dokumente, Apps für Geschäfts-E-Mails und die Dateifreigabe und vielen anderen Apps mit wichtigen Unternehmensdaten tummeln sich Spiele-, Dating- und Messaging-Apps.

E-Mails sind zweifelsohne das beliebteste Angriffswerkzeug für Phisher. 66 % aller E-Mails werden dem „U.S. Consumer Device Preference Report" von MovableInk zufolge mittlerweile zuerst auf Mobilgeräten geöffnet. Zwar haben die meisten Unternehmen einen Schutz für ihre geschäftlichen E-Mails eingerichtet, jedoch eröffnen private E-Mail-Konten ein neues Einfallstor für Bedrohungen.

Auch wenn die meisten seriösen Anbieter privater E-Mail-Dienste einen standardmäßigen Phishing-Schutz bieten, finden Angreifer immer neue Wege, diese Technologien zu umgehen und Mitarbeiter dazu zu verleiten, sensible Daten preiszugeben oder präparierte Apps herunterzuladen. Damit steht ihnen der Zugang zu Unternehmensdaten offen. Versierte Angreifer zielen auf private E-Mail-Konten ab, wenn sie Firmendaten ausspähen wollen, weil sie wissen, dass für diese nicht dieselben strengen Schutzmechanismen gelten wie für Geschäfts-E-Mails. Und sie wissen auch, dass beide E-Mail-Konten auf Mobilgeräten genutzt werden.



Wenn die Adresszeile verborgen ist, um die URL zu verschleiern, sehen sich diese beiden Anmeldebildschirme auf Mobilgeräten zum Verwechseln ähnlich.

Angesichts der professionellen Optik von Phishing-Seiten (oder präparierten Webseiten, die Nutzer zur Preisgabe ihrer Daten verleiten sollen) verwundert es kaum, dass dies eine so beliebte Angriffsmethode ist. Ein kurzer Blick auf die folgenden Anmeldebildschirme verdeutlicht das Problem. Selbst Experten fällt es schwer, den Unterschied zwischen echten und gefälschten Nutzerschnittstellen zu erkennen, vor allem auf den relativ kleinen Mobilgeräte-Displays.

Dennoch stellen E-Mails nur einen der Angriffsvektoren dar, die für Phishing genutzt werden, und Mobilgeräte eröffnen dabei völlig neue Zugangswege.

Die Phishing-Kill-Chain für Mobilgeräte

Ein unbedachter Fingertipp genügt, um ein Mobilgerät zu infizieren. Vielleicht tippen Sie auf eine präparierte URL, die im Browser-Fenster verkürzt angezeigt wurde, oder eine URL, die eine App im Hintergrund aufgerufen hat und damit unbeabsichtigt eine Verbindung zu einem schädlichen Anzeigennetzwerk herstellt, oder auf einen Link in einer privaten E-Mail, die Sie dazu verleitet, Ihre Firmenzugangsdaten preiszugeben. So gelangen Angreifer in Ihre IT-Infrastruktur und können sich systematisch zu Ihren wertvollen Daten vorarbeiten.

Phishing auf Mobilgeräten – Irrtum Nr. 2

Phishing erfolgt nur über E-Mails.

Entgegen der weit verbreiteten Meinung beschränken sich Phishing-Versuche nicht nur auf E-Mails, denn Mobilgeräte eröffnen Hackern völlig neue Angriffswege. Dabei bedienen sie sich mittlerweile auch SMS und MMS für ihre Phishing-Attacken und nicht zuletzt auch der beliebtesten und am weitesten verbreiteten Social-Media-Apps und Messaging-Plattformen wie WhatsApp, Facebook Messenger und Instagram.

Mitarbeiter fallen auf SMS-Phishing herein.

Einer Lookout-Studie zufolge tippten mehr als 25 % der Mitarbeiter auf einen Link in einer SMS von einer Telefonnummer, die wie eine Nummer aus ihrer Region wirkte.

Sicherheitsverantwortliche, die diese neuen Angriffspunkte außer Acht lassen, setzen ihre Unternehmen einem hohen Risiko aus. Ein kurzer Blick auf aktuelle Phishing-Beispiele, die sich nicht E-Mails bedienten, verrät warum.

ViperRAT

ViperRAT ist eine ausgefeilte Surveillanceware. Die Angreifer hinter ViperRAT locken ihre Opfer in eine Falle, indem sie sich in sozialen Netzwerken als Frauen ausgeben und die nichts ahnenden Nutzer zum Download einer präparierten Anwendung verleiten. Nachdem sie eine persönliche Beziehung zur Zielperson aufgebaut haben, senden sie ihrem Opfer eine Nachricht über das soziale Netzwerk, in der sie es bitten, eine App herunterzuladen, um die „Kommunikation zu vereinfachen".

Ein Angreifer kann anhand der von ViperRAT gestohlenen Informationen feststellen, wo sich die Zielperson aufhält, zu wem sie Kontakt hat (einschließlich der Profilfotos der Kontaktpersonen) und welche Nachrichten sie verschickt. Außerdem haben Angreifer Zugriff auf den Browserverlauf, Screenshots mit Daten aus anderen auf dem Gerät installierten Apps und sie können in der Nähe des Geräts geführte Gespräche und wiedergegebene Audiodaten abhören und alles sehen, worauf die Gerätekamera gerichtet wird.

Mehr zu ViperRAT

Phishing-Kampagne auf Facebook

Die Experten von F-Secure entdeckten eine Phishing-Kampagne, die auf iOS und Android-Nutzer abzielt. Dabei schickten die Angreifer der Zielperson eine Nachricht über Facebook Messenger, in der sie dem Opfer glauben machen wollten, es sei in einem YouTube-Video zu sehen. Wenn das Opfer über ein iOS- oder Android-Gerät einen Link antippte, wurde der Gerätetyp erkannt und eine entsprechende Seite angezeigt, die wie der jeweilige Facebook-Anmeldebildschirm aussah, um die Zugangsdaten des Opfers abzugreifen. Bei PC-Nutzern sah die Nutzerschnittstelle anders aus. Diese Art von Angriff könnte Opfer mittels Social Engineering dazu bewegen, ihre Zugangsdaten für beliebige Dienste, darunter auch geschäftlich genutzte, preiszugeben.

Mehr zur Facebook-Phishing-Kampagne

Diese Beispiele – und es gibt noch viele mehr – zeigen, dass Phisher sich längst nicht mehr auf E-Mails beschränken, sondern auch gezielt Mobilgeräte ins Visier nehmen. Doch wie konnten Mobilgeräte so schnell zu einem primären Angriffsvektor für Phishing werden?

- Mobilgeräte bieten neue Messaging-Plattformen wie die oben genannten.
- Da viele dieser Geräte nicht von Sicherheitsexperten verwaltet werden und meist auch über keinen Virenschutz verfügen, sind sie Angriffen oft schutzlos ausgesetzt.
- Aufgrund der besonderen Funktionen von Mobilgeräten (wie Ortungsdiensten, Front- und Rückkameras, Mikrofon, Sprachanrufe, SMS, E-Mail und Apps) und der Tatsache, dass die Opfer ihr Telefon meist bei sich tragen, lassen sie sich effektiver überwachen.

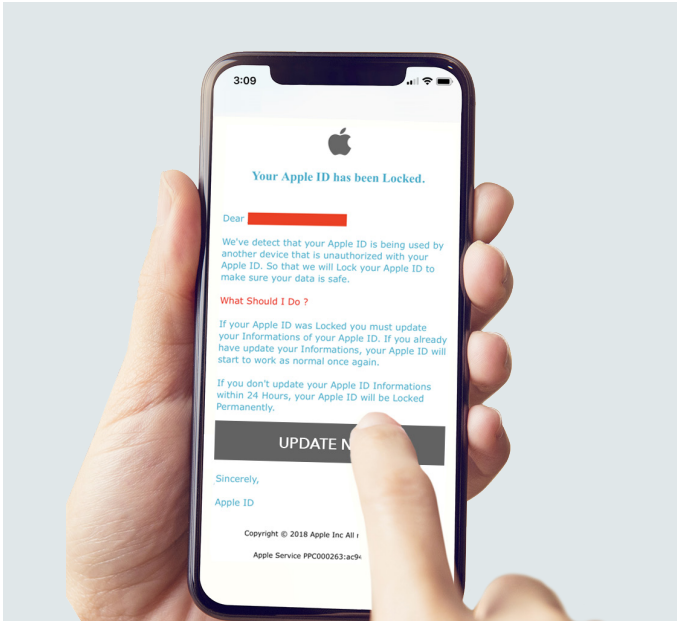
Phishing auf Mobilgeräten – Fakt Nr. 1

Auf Mobilgeräten ist es einfacher, Nutzer in die Phishing-Falle zu locken als auf Desktop-PCs.

Die Besonderheiten, Funktionen und selbst die Displaygröße moderner Mobilgeräte verschaffen Phishing-Angreifern einen entscheidenden Vorteil, denn auf Mobilgeräten ist es für Nutzer schwerer, zu erkennen, was echt und was gefälscht ist. Außerdem befinden sie sich oft außerhalb des konventionellen Sicherheitsbereichs von Unternehmen.

1. Beispiel:

Studien zeigen, dass Nutzer auf einem Smartphone dreimal eher einem Link folgen würden als an einem PC. Im Vergleich zu Desktop-Computern, wo die Nutzer den Mauszeiger über Hyperlinks bewegen können, um den vollständigen Linktext zu sehen, lässt sich die Echtheit von Links auf Mobilgeräten vor dem Anklicken wesentlich schwieriger überprüfen. Hinzu kommt die Tatsache, dass Webansichten in Apps (wie der von Facebook) es nahezu unmöglich machen, zu erkennen, welche URLs der Nutzer gerade aufruft. Daran wird deutlich, warum Angreifer sich verstärkt auf Mobilgeräte konzentrieren.

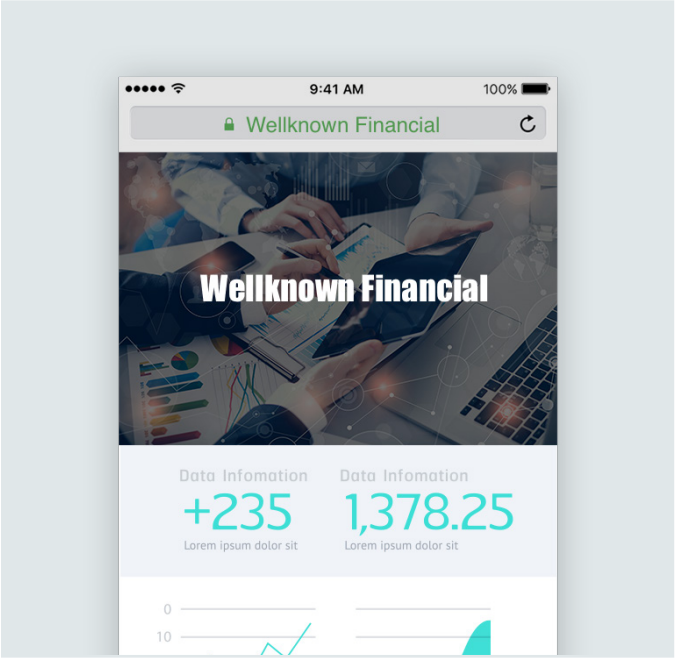


Was passiert hier? Auf einem Mobilgerät ist es wesentlicher schwerer zu erkennen, wohin ein Link führt. Hält der Nutzer einen Link in iOS gedrückt (anstatt ihn anzutippen), wird 3D Touch aktiviert und die verlinkte Seite geladen. Wenn ein Angreifer eine überzeugend echt wirkende Phishing-Seite bereitstellt, hätte der Nutzer noch immer Schwierigkeiten, die Fälschung vom Original zu unterscheiden.

2. Beispiel:

Bei einem Desktop-Monitor würde Ihnen wahrscheinlich auffallen, dass eine URL „wellknownfinancial.com----------fakesite.xyz" lautet anstatt „wellknownfinancial.com", da aber mobile Browser die URL in der Adresszeile verkürzen, sehen Sie jeweils nur „wellknownfinancial.com---". Bisweilen ersetzt der Browser die URL sogar durch den Namen des Unternehmens, auf dessen Website Sie zugreifen (siehe Beispiel rechts). So lässt sich deutlich schwerer erkennen, ob eine URL echt ist.

Mobile Browser verbergen auch oft die Website-URLs in der Adressleiste, während der Anwender auf dem Bildschirm scrollt, und limitieren die in der Adressleiste angezeigten Zeichen in Abhängigkeit von der Bildschirmbreite. Solche an sich durchaus nützlichen Designoptimierungen erleichtern es Angreifern, ihre Phishing-Attacken auszuüben.



Was passiert hier? In der Adresszeile wird nur der Firmenname angezeigt, aber nicht die URL.

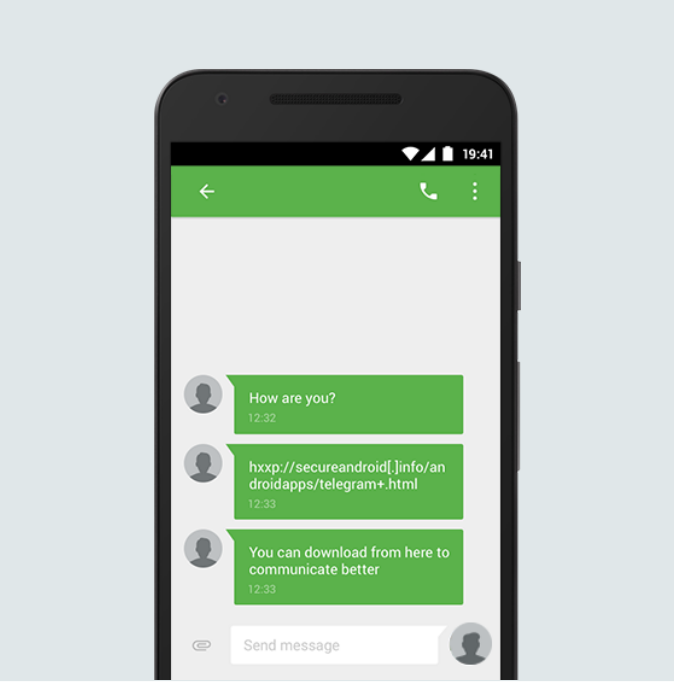
3. Beispiel:

Wenn ein Mobilgerät durch eine Firewall geschützt ist und ein Nutzer einen Phishing-Link anklickt, greift die Firewall ein und stoppt die Verbindung. Wie der Name schon sagt sind Mobilgeräte aber vor allem eins – nämlich mobil – und damit oft außerhalb der schützenden Firewall. Da sie sich also die meiste Zeit außerhalb des Schutzbereichs bewegen, kann die Firewall einen Mitarbeiter (z. B. auf seinem Heimweg im Zug) nicht davor bewahren, eine präparierte URL aufzurufen. Somit haben Angreifer leichtes Spiel und können ungehindert in das Netzwerk des Unternehmens eindringen – sofern es seinen Schutz nicht auch auf Mobilgeräte ausgedehnt hat.

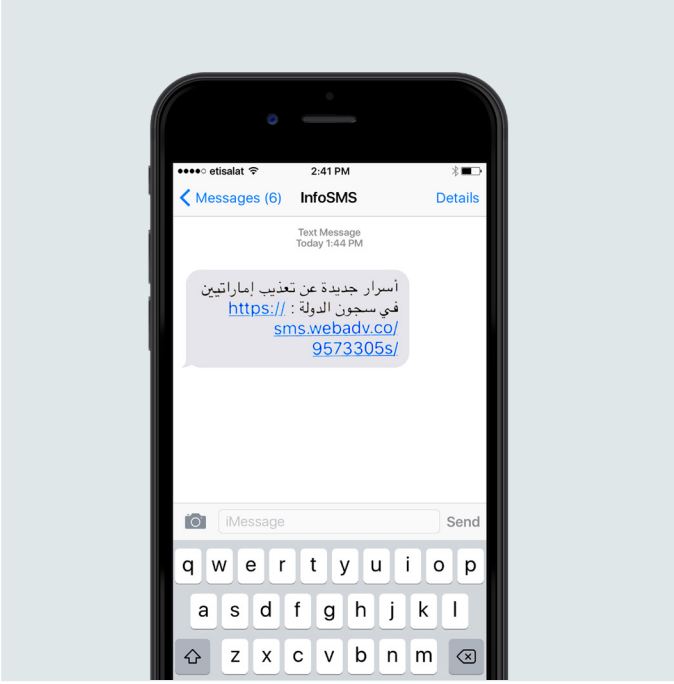
Phishing auf Mobilgeräten – Fakt Nr. 2

Entwicklern von Malware für Mobilgeräte, vor allem mAPT-Programmierern, gelingt es, ihre Phishing-Methoden erfolgreich in der Praxis anzuwenden.

Phishing auf Mobilgeräten ist in zunehmendem Maße das erste Angriffswerkzeug bei großangelegten, komplexen Angriffen. Zu den häufigsten Bedrohungen zählen Mobile Advanced Persistent Threats (mAPT). Der Ausdruck „Advanced Persistent Threat" bezeichnet den zielgerichteten, anhaltenden, effektiven Angriff einer Gruppe (in der Regel ein Nationalstaat) auf die Behörden anderer Nationalstaaten, Groß- und Mittelstandsunternehmen oder Einzelpersonen, um über einen längeren Zeitraum Informationen auszuspähen, die dem persönlichen finanziellen Gewinn des Angreifers oder der Spionage dienen. Mit mAPT wird diese Form der Bedrohung nun auch auf Mobilgeräte ausgeweitet. Hier ein paar aktuelle Beispiele aus der Praxis:



SMS von Dark Caracal



Phishing-SMS von Pegasus, erkannt von Citizen Lab

- **Dark Caracal**
  Dark Caracal versendet Phishing-Nachrichten über WhatsApp und Facebook, um potenzielle Opfer dazu zu verleiten, Android-Malware über präparierte Links herunterzuladen. Die Android-Malware namens Pallas überwacht dann das Gerät des Opfers und sammelt große Mengen an Daten.

  Dark Caracal richtet sich vor allem an Regierungsbehörden, das Militär, Versorgungsunternehmen, Finanzinstitutionen sowie Unternehmen aus der Fertigungs- und Verteidigungsindustrie. Die dabei ausgespähten Daten sind sehr umfangreich, darunter Dokumente, Anrufprotokolle, Audioaufnahmen, abgesicherte Inhalte von Messaging-Clients, Kontaktdaten, SMS/Textnachrichten, Fotos und Kontoinformationen.

- **Pegasus**
  Die Surveillanceware Pegasus erlangte weltweite Aufmerksamkeit durch die besonders schwerwiegenden Folgen, die solche Angriffe nach sich ziehen. Dabei senden die Pegasus-Hacker ihren Opfern eine Phishing-Nachricht per SMS. Wenn das Opfer sie anklickt, wird eine Kette von Ereignissen ausgelöst, die unbemerkt im Hintergrund ablaufen. Diese auf iOS-Geräte ausgelegte Angriffsmethode ist eine der professionellsten, die Lookout je gesehen hat. Auf dem Gerät selbst belauschte Pegasus sämtliche Aktivitäten und sammelte dabei enorme Mengen sensibler Daten.

Da mAPT-Angriffe eine neue Ebene komplexer Bedrohungen darstellen, ist hier besondere Wachsamkeit geboten.

Phishing auf Mobilgeräten – Fakt Nr. 3

Unternehmen müssen sich auch darüber Gedanken machen, dass Apps (nicht nur Menschen) unbeabsichtigt präparierte URLs öffnen und sie nichts ahnenden Mobilgerätenutzern zur Verfügung stellen.

URLs werden aber nicht nur von Anwendern geöffnet (bzw. angeklickt). Auch in die Codebasis von Apps sind URLs eingebettet und rufen Informationen in Echtzeit ab. Diese Funktion nutzen Angreifer aus, um wertvolle Daten von Opfern auszuspähen. Damit müssen Unternehmen nun eine weitere Angriffsfläche absichern: seriöse Apps, die auf präparierte URLs zugreifen.

App-Entwickler verdienen ihr Geld oft mit Werbung. Dazu integrieren sie Anzeigen-SDKs in den App-Code. Diese SDKs stellen dann im Hintergrund eine Verbindung zu URLs her, um dem Nutzer Anzeigen einzublenden. Wenn nun ein Angreifer ein Anzeigen-SDK einer seriösen App steuert, kann er mithilfe des SDK auf schädliche URLs zugreifen und dem Nutzer Werbung anzeigen, die ihn dazu verleiten sollen, vertrauliche Daten preiszugeben.

Solche Bedrohungen nutzen zwar Hintergrundfunktionen aus, aber Phishing-Attacken müssen nicht zwangsläufig versteckt ablaufen, um effektiv zu sein.

So löst Lookout das Phishing-Problem

Der in Lookout Mobile Endpoint Security enthaltene Phishing- und Content-Schutz bewahrt Unternehmen auch in unserer mobilen Welt vor Phishing-Angriffen.

Phishing- und Content-Schutz von Lookout

Erkennung – Phishing-Versuche auf Mobilgeräten werden unabhängig von ihrem Ursprung, z. B. E-Mails (geschäftlich wie privat), SMS, Chat-Apps, soziale Medien und vieles mehr, erkannt. Außerdem lassen sich Richtlinien zum Schutz vor Phishing-Angriffen festlegen.

Schutz – Verbindungen auf Mobilgeräten zu bekannten schädlichen URLs, die über präparierte Websites gehostet werden und möglicherweise versuchen, Zugangsdaten auszuspähen oder andere rechtswidrige Handlungen vorzunehmen, werden blockiert.

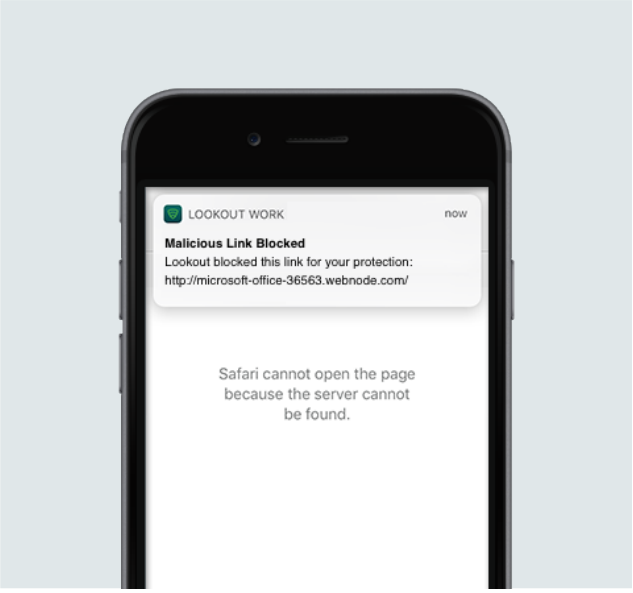
- Als schädliche URLs gelten betrügerische Anzeigen, Botnets, Command and Control Center (C&C), infizierte Anzeigen-Links zu Malware, Call Home, Malware-Verbreitungspunkte, Phishing/Betrug, Spam-URLs, gefährliche Inhalte wie präparierte Apps oder Websites mit bekannten Schwachstellen sowie Spyware.

Beseitigung – Die Nutzer werden bei Zugriff auf die URL sofort benachrichtigt.
Durch diese Echtzeitwarnung wird verhindert, dass Nutzer auf Phishing- oder präparierte Websites zugreifen.

Analyse – Sie erhalten einen Überblick über die Häufigkeit und den Schweregrad von Phishing-Angriffen, bei denen Nutzer präparierte Links anklicken. Außerdem dokumentiert unsere Lösung, ob Geräte den Phishing- und Content-Schutz aktiviert haben oder nicht. Geräte, deren Schutz deaktiviert ist, werden als nicht konform markiert. Damit ist das übliche Beseitigungsverfahren durch die Integration in führende EMM-Lösungen möglich.

So funktioniert es

Der Phishing- und Content-Schutz von Lookout blockiert sämtliche Verbindungsversuche zu schädlichen und Phishing-URLs auf Netzwerkebene, wenn das Gerät oder der Mitarbeiter versucht, eine Seite aufzurufen. Wichtig ist dabei, dass der Inhalt von Nachrichten nicht überprüft wird. Dadurch unterscheidet sich unser Ansatz von herkömmlichen Lösungen. Die Anwender vieler Kommunikationskanäle und Messaging-Plattformen, die über Mobilgeräte genutzt werden, wie SMS, WhatsApp, Facebook Messenger und private E-Mails, tauschen darüber private, vertrauliche Informationen aus. Da nur die URL zum Zeitpunkt des Verbindungsversuchs geprüft wird, bleibt mit dem Phishing- und Content-Schutz von Lookout die Privatsphäre des Nutzers gewahrt. Und da die URLs auf Netzwerkebene geprüft werden, ist Lookout in der Lage, Nutzer vor präparierten und Phishing-URLs in E-Mails, SMS, sozialen Netzwerken und allen sonstigen Apps zu schützen.



Die Vorteile des Phishing- und Content-Schutzes von Lookout

Seit jeher sorgt Lookout Mobile Endpoint Security für vollständigen Einblick in die gesamte Bandbreite mobiler Risiken Ihres Unternehmens. Darüber hinaus vereinfacht es die Anwendung von Sicherheitsrichtlinien, um diese Risiken messbar zu vermindern, und lässt sich mühelos in vorhandene Lösungen für das Sicherheits- und Mobilgeräte-Management integrieren. Unser Phishing- und Content-Schutz bietet Ihnen nun noch zahlreiche weitere Vorteile. Die Funktion:

- Ausdehnung des Schutzes vor Phishing und schädlichen Websites auf Mobilgeräte, sodass sowohl private E-Mails als auch Kommunikationskanäle und Messaging-Plattformen auf Mobilgeräten abgedeckt sind
- Umfassender Schutz vor allen Facetten mobiler Risiken, einschließlich des Web- und Content-Bedrohungsvektors, der von Angreifern am häufigsten genutzt wird, um Unternehmensdaten über Mobilgeräte auszuspähen
- Fördert den digitalen Wandel in Unternehmen, denn damit steht der Nutzung von Smartphones für die Arbeit nichts mehr im Wege. Daten und Systeme sind vor schädlichen Inhalten geschützt, unabhängig davon, ob sich der Mitarbeiter innerhalb des geschützten Unternehmensnetzwerks befindet oder nicht.
- Wahrung des Datenschutzes durch Einhaltung der Prinzipien der Datenminimierung und zielgerichteten Datenerfassung inkl. robuster Datenschutzkontrollen sowie der Möglichkeit, die Erfassung personenbezogener Daten von Anwendern oder verwalteten Geräten einzuschränken.

Mit Lookout Mobile Endpoint Security inklusive Phishing- und Content-Schutz profitiert Ihr Unternehmen von einer bewährten Lösung zur Risikominderung, die den sicheren Einsatz von Mobilgeräten bei der Arbeit ermöglicht.

Echter Schutz in Aktion

Die Mobilität hat zu einem Wandel in der modernen Arbeitswelt, konkret der Arbeitsweise geführt. Unternehmen suchen immer nach Möglichkeiten, die Mitarbeiterproduktivität und -flexibilität zu steigern, dabei aber gleichzeitig sensible Daten, Mitarbeiter- und Kundeninformationen sowie die kritische Netzwerkinfrastruktur zu schützen.

- Der Phishing- und Content-Schutz von Lookout geht dabei auf die praktischen Anforderungen und Probleme ein, denen Administratoren tagtäglich begegnen.
- Administratoren möchten es Mitarbeitern ermöglichen, ungehindert auf ihren Mobilgeräten im Internet zu surfen, müssen gleichzeitig aber auch bekannte schädliche Websites blockieren.
- Dabei bereitet ihnen vor allem Sorgen, dass Mitarbeiter auf ihren Geräten verschiedene Browser verwenden und bei riskanten Websites keine Warnung erhalten, deshalb möchten sie sicherstellen, dass Nutzern auf Mobilgeräten eine Warnung angezeigt wird, bevor sie eine Seite aufrufen.
- Sicherheitsteams möchten, dass alle Endgeräte gleichermaßen geschützt sind. Damit wäre die mobile Sicherheitslücke geschlossen.
- IT-Abteilungen müssen keinen Backhaul für den Datenverkehr einrichten und Mobilgeräte damit im Grunde hinter die Firewall verbannen, was das Nutzererlebnis und die Performance für Mitarbeiter beeinträchtigen würde. Mit unserer Lösung hingegen können Unternehmen sich voll und ganz auf den digitalen Wandel einstellen und Mitarbeitern eine sichere Möglichkeit bieten, ihre Mobilgeräte bei der Arbeit zu verwenden, egal ob im Unternehmen ein BYOD- oder ein COPE-Modell angewendet wird.

Lookout Mobile Endpoint Security wurde speziell dazu entwickelt, Unternehmen vor den Sicherheitsbedrohungen zu schützen, die eine mobile Arbeitsweise mit sich bringt. Mit dieser neuen Funktion können IT- und Sicherheitsverantwortliche nun auf die Probleme reagieren, die Phishing auf Mobilgeräten nach sich ziehen.

Machen Sie den nächsten Schritt: Erfahren Sie, wie Lookout helfen kann

Böswillige Akteure nutzen ausgefeilte Formen von Phishing, um an sensible Unternehmensdaten zu gelangen.

Während Sicherheits- und IT-Experten im Allgemeinen die Gefahren erkennen, die mit Phishing-Angriffen einhergehen, konzentriert sich die Mehrheit der Unternehmen noch immer auf die Absicherung traditioneller Endpunkte wie PCs. Doch das allein genügt nicht mehr.

Phishing auf Mobilgeräten ist nicht nur anders, sondern auch problematischer als Phishing-Attacken auf konventionellen Endgeräten. Unternehmen, die einen umfassenden Schutz vor Phishing-Angriffen auf allen Vektoren einschließlich Mobilgeräten suchen, benötigen mehr als die üblichen Lösungen. Hier bietet Lookout Mobile Endpoint Security den nötigen Zusatzschutz.

Um zu erfahren, wie Sie Ihre mobile Flotte noch heute sichern können, kontaktieren Sie uns unter info@lookout.com

* Methodik: Oben genannte Daten stammen aus einer Analyse von 67 Mio. Mobilgeräten, die zwischen 2011 und 2016 mit Lookout Personal geschützt wurden. Die Datenerfassung erfolgte anonym, Unternehmensdaten oder Daten aus Netzwerken oder Systemen wurden nicht erfasst.