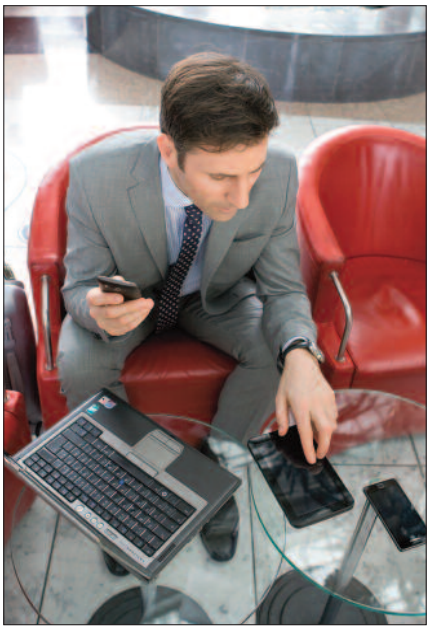
Smartphone-Schädlinge

Die Verbreitung von Schadsoftware für mobile Geräte nimmt zu. Die Schädlinge richten sich fast ausschließlich gegen Geräte, die Android-Betriebssysteme verwenden.

Die steigende Beliebtheit von mobilen Geräten wie Tablets und Smartphones sowie ein scheinbar grenzenloses Angebot verschiedenster Anwendungen (Apps) bewirkt auch einen rasanten Anstieg von kriminellen Handlungen und Angriffen auf diese Systeme. Angreifer tarnen ihre Schad- oder Spionagesoftware als harmlose Anwendungen (z. B. Taschenlampen-App) oder verleiten Smartphone-Benutzer gezielt zur Installation von veränderten Original-Apps. Sollte das Smartphone auch für Online-Banking genutzt werden, empfiehlt sich besondere Vorsicht, wenn zur Installation eines „Sicherheitszertifikates" aufgefordert wird. Dahinter steckt oftmals ein Trojaner, der unbemerkt SMS-TANs und Kontodaten ausspioniert und an Kriminelle weiterleitet, die damit umgehend das Konto plündern. Nicht weniger effektiv ist die Sperre des Smartphones mit einhergehender „Lösegeldforderung". Dabei wird das Smartphone durch eine bösartige App infiziert und für den Besitzer gesperrt. Erst nach Zahlung der geforderten Summe wird die Sperre vom Angreifer aufgehoben.

Erpresser-Programme. „2013 sind weltweit 2,7 Millionen Attacken durch Crypto-Malware registriert worden – neunmal so viele wie 2012", sagt Stefan Kremel, Mitarbeiter der Softwarefirma *Kaspersky-Lab*. Mittlerweile sind etwa 350.000 mobile Malware-Modifikationen bekannt – und die Zahl nimmt ständig zu. Stark im Umlauf ist ein Erpresser-Programm (Ransomware), das Smartphones angreift, die Android-Systeme verwenden. Der Schädling heißt „Trojan.AndroidOS.Koler.a".

Mit dem Schadprogramm blockieren die Kriminellen das Display und fordern Lösegeld für die Freigabe der Sperre in der Höhe von 100 bis 300 Dollar. Bezahlt ein Betroffener das Lösegeld, wird die Sperre meist aufgehoben, aber das Schadprogramm bleibt am Gerät und bietet die Möglichkeit, den Nutzer weiterhin auszuspionieren. „Man sollte sich vor solchen Fällen wappnen, indem man alle wichtigen



Laut einer Studie von Kaspersky Lab und Interpol wird jeder fünfte Android-Anwender innerhalb eines Jahres von Malware attackiert.

Daten auf dem Smartphone wie Kontakte und Einstellungen extern sichert", rät Kontrollinspektor Horst Reisner, MSc, Mitarbeiter im Cybercrime-Competence-Center (C4) des Bundeskriminalamts in Wien. Denn die zuverlässigste Möglichkeit, das Schadprogramm loszukriegen, besteht oftmals nur noch darin, dass man das Gerät auf die Werkseinstellung zurücksetzt. Dieser Vorgang bewirkt, dass alle Einstellungen und Daten verlorengehen. Deshalb empfiehlt der Cybercrime-Experte, Benutzerdaten regelmäßig zu sichern. Im Idealfall nicht in der Cloud, sondern am lokalen Heim-PC. Denn man muss

Erpresser-Programm: Der Bildschirm eines Gerätes wird blockiert und es wird Lösegeld für dessen Entsperrung gefordert.

den Nutzungsbedingungen von Anbietern von Cloud-Diensten zustimmen und gibt ihnen damit die Rechte z. B. an den Kontaktdaten weiter.

Smartphone-Nutzer holen sich den Schädling, wenn sie präparierte Porno-Seiten besuchen. Am Display erscheint eine Mitteilung, dass der Nutzer auf einer „verbotenen" Pornoseite war und deswegen gesperrt wurde. Auf der Mitteilung befindet sich ein Polizeilogo, das den Eindruck einer behördlichen Maßnahme erwecken soll. „Trojan.AndroidOS.Koler.a" wurde im Mai 2014 entdeckt. Er verschlüsselt keine Dateien und blockiert – außer dem Bildschirm – keine anderen Funktionen auf dem Gerät.

„Dieser Schädling hat maßgeschneiderte Nachrichten für 30 Länder zu bieten, darunter Österreich", erläutert Christian Funk, IT-Sicherheitsexperte von *Kaspersky Lab*. Er wird über eine Verteilungsinfrastruktur verschickt. Sie besteht aus einem Netzwerk von schädlichen Pornoseiten, verbunden mit einem Traffic-Richtungssystem, das das Opfer zu einer schädlichen App umleitet, die eine APK-Datei mit der Bezeichnung animalporn.apk enthält. APK ist die Abkürzung für Android Package File. Dieses File ist notwendig, um eine App auf Smartphones mit Android OS zu installieren.

Kaspersky-Experten fanden 49 schädliche Porno-Websites, die von 200.000 Besuchern aufgerufen wurden, 80 Prozent davon in den USA. „Die Nutzung eines Porno-Netzwerks für diese Polizei-Erpressersoftware ist kein Zufall", erklärt Funk. „Die Opfer fühlen sich viel eher schuldig, wenn sie derartigen Content besuchen, und sie bezahlen daher auch eher die angeblich von den Behörden geforderte Strafe."

Manchmal verzichten die Cyber-Kriminellen auf jegliche List – die Daten werden einfach verschlüsselt und für die Dechiffrierung wird Geld verlangt. So geschehen im Fall des Trojaners „Cryptolocker", den *Kaspersky Lab* im Oktober 2013 analysierte. Die Kriminellen gaben ihren Opfern nur drei Tage Zeit, um sich freizukaufen. Sie drohten ihren Opfern damit, dass

Fotos: Kaspersky Lab

ihre Daten für immer verloren seien, wenn sie nicht rechtzeitig bezahlen würden. Am stärksten von dieser Bedrohung betroffen waren Großbritannien und die USA. Für „Cryptolocker“ gibt es das Entschlüsselungstool „DecryptCryptolocker“.

Falsches Antivirenprogramm. Seit Juni 2013 haben es die *Kaspersky*-Experten mit der Android-App „Free Calls Update“ zu tun – einem gefälschten Antiviren-Programm, das seine Opfer dazu bringen soll, Geld für das Entfernen nicht existierender Malware zu zahlen. Einmal auf dem Gerät installiert, versucht die App Administratoren-Rechte zu erhalten. Dadurch ist sie in der Lage, die WiFi- und 3G-Module ein- und auszuschalten und kann das Opfer daran hindern, die App einfach zu entfernen. Die Installationsdatei wird danach gelöscht, um zu vermeiden, dass auf dem Gerät installierte echte Antiviren-Programme das Schadprogramm entdecken. Die App gibt vor, Malware zu identifizieren und fordert das Opfer auf, eine Lizenz für die Vollversion zu kaufen, um die Schadsoftware zu entfernen.

Die neue Erpresser-Malware „Zerolocker“ soll ausschließlich *Windows*-Systeme angreifen und kann Dateien mit einem starken Algorithmus verschlüsseln. „Zerolocker“ soll fast alle Dateien eines betroffenen Systems verschlüsseln, ausgenommen Dateien, die größer als 200 MB sind oder solche, die in den Verzeichnissen Windows, Programme, Desktop der Zerolocker liegen. Ausgeführt wird die Malware im Verzeichnis C:\Zerolocker. Für die Freigabe fordern die Kriminellen zwischen 300 und 1.000 Dollar, das nur in der Digitalwährung *Bitcoin* bezahlt werden kann. Im Falle einer Infektion mit „Zerolocker“ sollten Betroffene nicht zahlen, raten Sicherheitsexperten. Die Hintermänner könnten wegen eines Fehlers in dem Schadprogramm vermutlich keinen korrekten Schlüssel für die Entschlüsselung liefern. Bislang sei „Zerolocker“ nicht weit verbreitet, was auf den Fehler zurückzuführen sei.

Die Cyber-Kriminellen akzeptieren unterschiedliche Zahlungsarten, auch *Bitcoins*. Sie passen ihre Vorgangsweise auf verschiedene Regionen an. In Regionen, in denen Software-Piraterie verbreitet ist, würden die Betrüger behaupten, dass sie bei einem Internet-

SMS-Trojaner sind die Ursache für die Hälfte aller Angriffe auf Android-Geräte.

Foto: Kaspersky Lab

nutzer unlizenzierte Software auf dem Computer gefunden haben und Geld für die Wiederherstellung des Zugriffs auf den Computer verlangen. An anderen Orten zeigen diese Schädlinge Pop-up-Benachrichtigungen an, die angeblich von der Polizei stammen und in denen behauptet wird, dass auf dem Computer Kinderpornografie oder andere illegale Inhalte gefunden wurden. Dann wird die Zahlung einer Strafe verlangt. Es sind meist Android-Geräte, die von Schadprogrammen betroffen sind. Cyber-Kriminelle nutzen die Tatsache aus, dass Nutzer Apps von *Google Play,* von anderen Marktplätzen oder von anderen Webseiten herunterladen. Das ermöglicht es den Kriminellen, Fake-Webseiten zu erstellen, die als App Stores getarnt sind. „Der überwiegende Teil von Smartphone-Apps ist aus datenschutzrechtlicher Sicht als sehr bedenklich einzustufen“, sagt Kriminalist Horst Reisner. „Speziell Gratis-Apps dienen dazu, das Benutzerverhalten und Benutzerdaten auszuspionieren, damit diese analysiert und gewinnbringend verwertet werden können.“

Die Bedrohung durch Schadsoftware nimmt nicht nur mengenmäßig zu. Die Kaspersky-Experten beobachten zudem eine wachsende Komplexität. Im Juni 2013 analysierten sie einen der raffiniertesten mobilen Trojaner – das Programm „Obad“. Dessen Bedrohung ist multifunktional: Obad schickt Nachrichten an Premium-Nummern, lädt und installiert andere Schadprogramme, nutzt Bluetooth, um sich selbst an andere Geräte zu senden und

PRÄVENTION

Smartphone-Sicherheit

- Vorsicht bei der Nutzung öffentlicher WLAN-Hotspots.
- Handy nie unbeaufsichtigt lassen oder fremden Personen anvertrauen.
- Anti-Viren-Programme (Virenscanner) für Smartphones nutzen.
- Betriebssystem und Anwendungen regelmäßig updaten.
- Nur Apps aus sicheren Quellen beziehen.
- Werden für die Installation von Apps mehr Berechtigungen eingefordert, als für deren Funktion erforderlich ist, sollte diese Anwendung nicht heruntergeladen werden.
- Nicht benötigte Zusatzdienste wie WLAN, GPS, Bluetooth deaktivieren.
- Vorsicht bei E-Mails oder SMS, die dem Anschein nach von einer Bank oder von Online-Zahlungsdiensten stammen und zum Download einer Datei auffordern bzw. die Installation von Security-Anwendungen (z. B. „Sicherheitszertifikat“) anregen. Dahinter stecken oftmals Schadprogramme, die unbemerkt Zugangsdaten und mTANs für Online-Banking ausspionieren.

führt Befehle an der Konsole aus. Der Code ist stark verschleiert und nutzt drei vorher unbekannte Sicherheitslücken aus. Eine erlaubt es dem Trojaner, die erweiterten Rechte eines Geräteadministrators zu erhalten – allerdings ohne in der Liste der Programme zu erscheinen, die diese Rechte haben. So wird es dem Opfer unmöglich, die Malware von seinem Gerät zu entfernen. Außerdem ist der Trojaner in der Lage, den Bildschirm zu blockieren. Er macht das für nicht länger als zehn Sekunden, doch das reicht dem Schädling aus, sich selbst und andere Malware an die umliegenden Geräte zu senden – ein Trick, der verhindern soll, dass das Opfer die Aktivität des Trojaners registriert.

Die Cyberkriminellen hinter „Obad“ können den Trojaner so steuern, dass er vordefinierte Text-Strings in den Kurzmitteilungen benutzt. Der Schädling kann verschiedene Aktionen ausführen, unter anderem SMS versenden, als Proxy-Server agieren, sich mit einer speziellen Adresse verbinden, eine bestimmte Datei herunterladen und installieren, eine Liste der auf dem Gerät installierten Apps senden, Informationen über eine bestimmte App verschicken, die Kontakte des Opfers an den Server schicken und Befehle vom Server ausführen. Der Trojaner sammelt Daten über das Gerät und schickt sie an den „Command-und-Control-Server“ (C2). Dazu zählen unter anderem die MAC-Adresse des Gerätes, der Gerätename, die IMEI, das Kontoguthaben, die lokale Zeit sowie Informationen darüber, ob der Trojaner die Rechte eines Geräteadministrators erhalten hat oder nicht. Alle diese Daten werden auf den C2 von „Obad“ hochgeladen: Der Trojaner versucht zuerst, eine aktive Internetverbindung zu nutzen. Ist keine verfügbar, sucht er nach der nächstgelegenen WLAN-Verbindung, die keine Authentifizierung erfordert.

Cybercrime-Meldestelle. Wer mit einer Lösegeldforderung erpresst wird, um eine Smartphone-Sperre loszuwerden, sollte eine Anzeige bei der nächsten Polizeidienststelle erstatten. Die Polizisten der jeweiligen Dienststelle nehmen in solchen Fällen Kontakt mit der zuständigen Dienststelle in den Bundesländern oder mit der Cybercrime-Meldestelle im Bundeskriminalamt auf *(against-cybercrime@bmi.gv.at)*.

Siegbert Lattacher