IT-Sicherheit: Kaspersky entdeckt Spionagesoftware für Android

Kelkheim, 25. Januar 2018

Flickr: John Mosbaugh CC Lizenz

Das Softwareunternehmen Kaspersky hat eine Spionagesoftware für das Handy-Betriebssystem Android entdeckt: Skygofree, wie KasFpersky die Software nennt, ist vermutlich eine Überwachungssoftware speziell für staatliche Ermittler. Denn die Software ist nicht dazu ausgelegt, breite Bevölkerungsschichten auszuspionieren, sondern dient der gezielten Überwachung. Gefunden wurde das Programm überwiegend in Italien; entwickelt wahrscheinlich auch von einem italienischen Unternehmen. Verbreitet wird der Trojaner über infizierte Websites, die denen der Mobilfunkanbieter nachgebaut wurden. Die Handy-Nutzer werden dort aufgefordert, ihr Gerät zu aktualisieren bzw. neu zu konfigurieren – so wird die Software heimlich installiert.

„Skygofree" gibt es vermutlich seit 2014 und wird immer weiterentwickelt. Der Trojaner nutzt eine Schnittstelle namens Accessibility Services, die eigentlich dazu gedacht ist, barrierefreie Apps zu entwickeln. Apps also, die zum Beispiel den Inhalt einer Whatsapp-Konversation vorlesen. Skygofree nutzt dieses Tor und leitet die Nachricht an die Ermittler weiter. Die Verschlüsselung von WhatsApp wird also nicht geknackt, sondern umgangen.

Doch nicht nur Whatsapp ist das Ziel. Skygofree kann insgesamt 48 verschiedene Funktionen aktivieren. Darunter das Mikrofon des infizierten Geräts, um den Beobachteten heimlich

abzuhören. Zudem kann die Kamera angeschaltet und unbemerkt Bilder und Videos gemacht werden. Sogar eine WLAN-Verbindung kann Skygofree herstellen und so Daten versenden, darunter zum Beispiel Standortdaten, SMS, Kalendereinträge und vieles weitere aus dem Speicher des Handys. Auch wenn einige der Funktionen, die Skygofree heimlich einschalten kann, noch nicht im realen Leben beobachtet wurden – möglich ist es.

Die Software ist in den vergangenen Jahren so weiterentwickelt worden, dass sie mehrere Root-Exploits mitbringt und auf verschiedenen Geräten einsatzfähig ist. Die Malware kann über HTTP, XMPP, Binär-SMS oder Firebase Cloudmessaging kontrolliert werden. Neben Android soll die Schadsoftware auch Windows-Nutzer im Visier haben. Darauf deuten einige Module hin, die Kaspersky gefunden hat. Infizierte Computer wurden bis jetzt allerdings noch nicht entdeckt.

Über die gb.online gmbh

Die gb.online gmbh hat sich auf die berufliche Absicherung von Freelancern spezialisiert und bietet mit www.easy-insure.eu das umfangreichste Online-Versicherungsportal für freie und beratende Berufe in Deutschland. Seit 2011 können Selbstständige und Unternehmen bis 1 Million Euro Umsatz pro Jahr hier ihre beruflichen Risiken versichern.

Steigt der Umsatz, und wird eine individuelle Lösung benötigt, so steht mit dem Schwesterunternehmen groot bramel versicherungsmakler gmbh ein verlässlicher Partner zur Seite, der seit über 25 Jahren Gewerbetreibende und industriellen Unternehmen in Versicherungsfragen vertritt. Die groot bramel versicherungsmakler gmbh ist in 18 Ländern vertreten und begleitet sie, wohin auch immer sich ihr Geschäftsfeld entwickelt.

Kontaktdaten

gb.online gmbh
Frankfurter Straße 93
65779 Kelkheim

Ansprechpartner: Lutz-Hendrik Groot Bramel, Geschäftsführer

Folgen Sie uns auch auf	

„Textil vernetzt“, „IT-Wirtschaft“ und „Usability“ – neue Mittelstand-4.0-Kompetenzzentren

Kelkheim, 12. Januar 2018

3D Drucker. Flickr: MKzero CC Lizenz

Seit 2015 fördert das Bundeswirtschaftsministerium die Digitalisierung von kleinen und mittleren Unternehmen durch so genannte Mittelstand-4.0-Kompetenzzentren. In diesen Kompetenzzentren finden die Unternehmen praxisrelevantes Wissen zur Industrie 4.0, wie auch die Möglichkeit, sich die neuen digitalen Anwendungen anzuschauen und zu erproben. Seit vergangenem Monat gibt es nun drei neue Kompetenzzentren: „Textil-vernetzt“, „IT-Wirtschaft“ und „Usability“. Damit stehen den Unternehmen nun flächendeckend insgesamt 22 Kompetenzzentren

zur Seite, die sie bei ihrem Weg zum Unternehmen 4.0 begleiten und sie fit für die Herausforderungen der digitalen Zeit machen.

Textil vernetzt – das Kompetenzzentrum für die Textilindustrie

Das Mittelstand-4.0-Kompetenzzentrum „Textil vernetzt“ hat seine Geschäftsstelle in Berlin sowie vier ‚Schaufenster‘ in Aachen, Chemnitz, Denkendorf und Stuttgart. Durch das Know-how des Kompetenzzentrums werden Unternehmen aus der Textilindustrie an technische Textilien bzw. textile Werkstoffe herangeführt; zum Beispiel an so genannte „Intelligente Textilien“, die Daten aus der Umgebung oder ihres Trägers erfassen und weitergeben oder an Faserverbundwerkstoffe, die in der Automobilindustrie und der Luft- und Raumfahrt eingesetzt werden, eine Rolle spielen.

„IT-Wirtschaft“ – das Zentrum für IT-Unternehmen und Start-ups

Das Mittelstand-4.0-Kompetenzzentrum „IT-Wirtschaft“ soll die Zusammenarbeit von mittelständischen IT-Unternehmen mit Start-ups verbessern. Kooperationen sollen zu interoperablen all-in-one IT-Lösungen für kleine und mittelständische Unternehmen führen. Zudem unterstützt das Zentrum kleinere und mittlere IT-Unternehmen in den Bereichen IT-Sicherheit und Datenschutz, Technologie-Scouting, Software Ergonomie und Digitale Geschäftsmodelle sowie bei der Entwicklung von Standards und Softwarelösungen. Auch wenn es darum geht, Potenziale technologischer Entwicklungen und Prozesse frühzeitig zu erkennen, ist das Kompetenzzentrum der Ansprechpartner; Technologie-Scouting- und Innovationsworkshops bieten Einblicke in zukünftige Trends.

Das Zentrum verfügt über vier regionale Stützpunkte in Berlin, Aachen, Kassel und Karlsruhe und ist

bundesweit über eine Online-Plattform erreichbar. Dort geben das Matching-Portal und das Konsortienregister den Unternehmen die Möglichkeit sich zu vernetzen. Auch rechtliche Fragen zur Bildung von Konsortien, des Datenschutzes und zum Entwickeln kollaborativer Geschäftsmodelle werden dort behandelt.

Kompetenzzentrum „Usability“ – Besser durch User Experience

Das Mittelstand-4.0-Kompetenzzentrum „Usability“ unterstützt kleine und mittlere Unternehmen dabei, ihre Produkte und Dienstleistungen mit Hilfe von Usability- und User-Experience-Methoden (UUX-Methoden) zu gestalten. So entwickelte Produkte führen zu einer höheren Produktivität und Kundenzufriedenheit, zu mehr Mitarbeitermotivation, besserer Vernetzung und somit zu mehr Umsatz. Zudem informiert das Zentrum mittelständische Softwareanbieter über UUX-Methoden und hilft Start-ups und UUX-Experten dabei, neue Lösungen und Geschäftsmodelle bekannt zu machen.

In den Regionen Berlin, Stuttgart, Bonn-Rhein-Sieg und Mannheim bietet das Mittelstand-4.0-Kompetenzzentrum Usability kostenfreie Unterstützungsangebote und Veranstaltungen. Darüber verfügt es über eine bundesweit verteilte Demonstrations- und Anschauungsinfrastruktur, wie Maker Spaces, Werkstätten für 3D-Druck, Living Labs im Bereich Smart Home und Smart Mobility, UUX-Labore mit Stationen für (mobiles) Eye-Tracking und vieles mehr.

Über die gb.online gmbh

Die gb.online gmbh hat sich auf die berufliche Absicherung von

Freelancern spezialisiert und bietet mit www.easy-insure.eu das umfangreichste Online-Versicherungsportal für freie und beratende Berufe in Deutschland. Seit 2011 können Selbstständige und Unternehmen bis 1 Million Euro Umsatz pro Jahr hier ihre beruflichen Risiken versichern.

Steigt der Umsatz, und wird eine individuelle Lösung benötigt, so steht mit dem Schwesterunternehmen groot bramel versicherungsmakler gmbh ein verlässlicher Partner zur Seite, der seit über 25 Jahren Gewerbetreibende und industriellen Unternehmen in Versicherungsfragen vertritt. Die groot bramel versicherungsmakler gmbh ist in 18 Ländern vertreten und begleitet sie, wohin auch immer sich ihr Geschäftsfeld entwickelt.

Kontaktdaten

gb.online gmbh
Frankfurter Straße 93
65779 Kelkheim

Ansprechpartner: Lutz-Hendrik Groot Bramel, Geschäftsführer

Folgen Sie uns auch auf	

Milliarden PCs und Smartphones betroffen: Sicherheitslücke durch Intel-

Chips

Kelkheim, 04. Januar 2018

Bildquelle: Flickr stargazer2020 CC Lizenz

Die neueste Cyberbedrohung betrifft so gut wie alle PCs, Smartphones und Server: Die Chips des größten Chip-Herstellers, Intel, ermöglichen aufgrund ihrer Funktionsweise, Hackern Passwörter und andere wichtige Informationen auszulesen – ohne dass der Nutzer es merkt. Von der Sicherheitslücke betroffen sind neben den Intel-Chips auch einige Prozessoren mit der Technologie des Chip-Designers Arm, der in Smartphones dominiert, und vermutlich auch einige des Intel-Konkurrenten AMD. Grund für die Sicherheitslücke ist eine Funktion, die die Chips schneller auf die Anfragen der

Nutzer reagieren lässt.

Speculative execution heißt eine Funktion, die seit mehr als 20 Jahren genutzt wird, um Computer, Handys und Server schneller zu machen. Wenn der Chip gerade nicht genutzt wird, führt er Berechnungen aus, von denen er annimmt, dass der Nutzer sie später brauchen wird.

Im Prinzip eine sinnvolle Funktion: Daten, die mit hoher Wahrscheinlichkeit früher oder später gebraucht werden, schon vor der eigentlichen Nutzung abzurufen, da der Chip so schneller reagieren kann. Aber genau das macht ihn anfällig für Angriffe. Das besonders Gefährliche an dieser Schwachstelle: In den Chips wird die Rechenarbeit des Computers erledigt, die Programme müssen dem Chip vertrauen.

Zwei mögliche Angriffsszenarien

Bis jetzt wird von zwei Angriffsszenarien ausgegangen: Meltdown und Spectre genannt. Bei Meltdown wird die Trennung zwischen den Programmen und dem Betriebssystem aufgehoben. So können Informationen aus dem Betriebssystem abgegriffen werden. Dies ist bisher nur bei Intel-Chips möglich.

Bei Spectre wird hingegen die Trennung zwischen den Programmen aufgehoben; so können andere Programme ausgespäht werden. Dies funktioniert bei Chips von Intel, von AMD und bei Chips mit Arm-Technologie. Laut Arm sind jedoch nur wenige Produktlinien betroffen.

Ob die Sicherheitslücke schon ausgenutzt wurde und es somit zu Meltdown- oder Spectre-Fällen gekommen ist, ist nicht bekannt. Denn ein Angriff auf den Chip würde in den Log-Dateien keine Spuren hinterlassen und ist somit nicht sichtbar zu machen. Intel geht davon aus, dass bisher jedoch nichts geschehen ist.

Sicherheitslücke ist seit dem Sommer bekannt

Die Sicherheitslücke war bereits im Juni entdeckt und verschiedenen Unternehmen bekannt gegeben, jedoch noch nicht an die Öffentlichkeit gebracht worden. So sollten Google, Microsoft und andere die Möglichkeit haben, ihre Server und Computer abzusichern. Eigentlich sollte auch nichts vor dem 9. Januar an die Öffentlichkeit gelangen, doch die erhöhte Update-Aktivität in den vergangenen Tagen war aufgefallen und erste Gerüchte über eine Sicherheitslücke kamen in Umlauf.

In den kommenden Tagen werden die Betriebssysteme Linux, Microsoft Windows, Apple (sowohl Mac OS als auch iOS) Patches erhalten. Diese machen die Rechner zwar etwas langsamer, dafür aber wieder sicherer.

Über die gb.online gmbh

Die gb.online gmbh hat sich auf die berufliche Absicherung von Freelancern spezialisiert und bietet mit www.easy-insure.eu das umfangreichste Online-Versicherungsportal für freie und beratende Berufe in Deutschland. Seit 2011 können Selbstständige und Unternehmen bis 1 Million Euro Umsatz pro Jahr hier ihre beruflichen Risiken versichern.

Steigt der Umsatz, und wird eine individuelle Lösung benötigt, so steht mit dem Schwesterunternehmen groot bramel versicherungsmakler gmbh ein verlässlicher Partner zur Seite, der seit über 25 Jahren Gewerbetreibende und industriellen Unternehmen in Versicherungsfragen vertritt. Die groot bramel versicherungsmakler gmbh ist in 18 Ländern vertreten und begleitet sie, wohin auch immer sich ihr Geschäftsfeld entwickelt.

Kontaktdaten

gb.online gmbh
Frankfurter Straße 93
65779 Kelkheim

Ansprechpartner: Lutz-Hendrik Groot Bramel, Geschäftsführer

Folgen Sie uns auch auf	