Check Point entdeckt neue Rogue Adware-Kampagne im Google Play Store: 150 Millionen Nutzer von ‚SimBad' betroffen

San Carlos, Kalifornien – 14. März 2019. Die Sicherheitsforscher von Check Point® Software Technologies Ltd. (NASDAQ: CHKP) haben eine neue Adware-Kampagne im Google Play Store gefunden, die sich auf 206 Apps verteilt hatte. SimBad, so der Name des Schadprogramms, betrifft 150 Millionen Nutzer. Google wurde bereits informiert und hat die betroffenen Apps aus dem Store entfernt, allerdings sind die Applikationen noch auf den Geräten der Nutzer installiert, sodass die Cyber-Kriminellen weiter Umsätze erzielen.

Die Malware befindet sich innerhalb des 'RXDrioder'-Software Development Kits (SDK), das von 'addroider[.]com' als werbebezogenes SDK bereitgestellt wird. Die Sicherheitsforscher glauben, dass die Entwickler durch einen Betrug dazu gebracht wurden, dieses bösartige SDK zu verwenden und den tatsächlichen Inhalt nicht kannten. Dieser Betrug führte dazu, dass die Kampagne nicht auf ein bestimmtes Land zielte oder nur von einem Entwickler alleine genutzt wurde. Check Point hat diese Malware „SimBad" genannt, da ein grosser Teil der infizierten Anwendungen Simulator-Spiele sind.

Sobald eine App mit SimBad an Bord installiert wurde, registriert sich die Malware unter „Boot Complete" und „User Present", was ihr ermöglicht, nach einem Neustart aktiv zu werden. Der erste Kontakt wird zum Command and Control (C&C)-Server aufgebaut und daraufhin beispielsweise das Symbol der App entfernt, um die Löschung zu erschweren. Die Einnahmequelle der Cyber-Kriminellen stellt das Einblenden von unzähligen Werbeanzeigen auf dem Bildschirm der Smartphones dar.

SimBad verfügt über Funktionen, die in drei Arten unterteilt werden können – Werbung, Phishing und Exposition gegenüber anderen Anwendungen. Aufgrund der Möglichkeit, eine bestimmte URL in einem Browser zu öffnen, können die Kriminellen, die hinter SimBad stecken, Phishing-Seiten für mehrere Plattformen generieren und auf den infizierten Geräten öffnen, um so Spear-Phishing-Angriffe auf den Benutzer durchzuführen.

Wegen der drei Funktionen, Werbung anzuzeigen, willkürlich andere Anwendungen zu öffnen, sowie URLs über den lokalen Browser aufzurufen, firmiert SimBad als Adware. Das Schadprogramm besitzt in seinem Code aber bereits die Struktur, um sich zu einer grösseren Bedrohung, einer echten Malware, zu entwickeln.

Den vollständigen Blog-Beitrag (auf Englisch) lesen Sie unter https://research.checkpoint.com/simbad-a-rogue-adware-campaign-on-google-play/

Folgen Sie Check Point auf:
Twitter: http://www.twitter.com/checkpointsw
Facebook: https://www.facebook.com/checkpointsoftware
Blog: http://blog.checkpoint.com
YouTube: http://www.youtube.com/user/CPGlobal
LinkedIn: https://www.linkedin.com/company/check-point-software-technologies

Über Check Point Research
Check Point Research bietet führende Cyber-Bedrohungsinformationen für Check Point Software-Kunden und die grössere Intelligenz-Community. Das Forschungsteam sammelt und analysiert globale Cyber-Angriffsdaten, die auf der ThreatCloud gespeichert sind, um Hacker fernzuhalten und gleichzeitig sicherzustellen, dass alle Check Point Produkte mit den neuesten Schutzmassnahmen aktualisiert werden. Das Forschungsteam besteht aus über 100 Analysten und Forschern, die mit anderen Sicherheitsanbietern, der Strafverfolgung und verschiedenen CERTs zusammenarbeiten.

Über Check Point Software Technologies Ltd.
Check Point Software Technologies Ltd. (www.checkpoint.com) ist ein führender Anbieter von Cyber-Sicherheitslösungen für Unternehmen und Regierungen weltweit. Seine Lösungen schützen Kunden vor Cyber-Angriffen der 5. Generation mit einer branchenführenden Fangrate von Malware, Ransomware und anderen gezielten Angriffen. Check Point bietet eine mehrstufige Sicherheitsarchitektur mit der neuen Gen V Advanced Threat Prevention, die alle Netzwerke, Clouds und mobilen Devices eines Unternehmens vor allen bekannten Angriffen schützt, kombiniert mit dem umfassendsten und intuitivsten Single Point of Control Management System der Branche. Check Point schützt über 100‘000 Unternehmen jeder Grösse.
Check Point Alps (Schweiz und Österreich) mit Sitz in Zürich und Wien beschäftigt rund 50 Mitarbeitende.

Pressekontakt:
Check Point Software Technologies (Switzerland) AG
Sonja Meindl
Tel: +41 44 316 64 44
E-Mail: smeindl@checkpoint.com

Jenni Kommunikation
Sylvana Zimmermann
Tel: +41 44 388 60 80
E-Mail: sylvana.zimmermann@jeko.com

