Ransomware-Angriffe laut Check Point in der zweiten Hälfte 2016 verdoppelt

Check Points Global Threat Intelligence Trends Report für die zweite Jahreshälfte 2016 beleuchtet wichtige Trends bei Netzwerk- und mobiler Malware

23. Februar 2017, **San Carlos, CA.** - Check Point® Software Technologies Ltd. (Nasdaq: CHKP) veröffentlicht seinen H2 2016 Global Threat Intelligence Trends Report. Aus diesem geht hervor, dass sich Ransomware-Angriffe in der zweiten Hälfte des Vorjahres verdoppelt haben. Ausgehend von allen weltweit erkannten Vorkommnissen im Zusammenhang mit Malware stieg der Anteil der Angriffe mit Verschlüsselungsmalware zwischen Juli und Dezember 2016 von 5,5 auf 10,5 Prozent.

Der H2 2016 Global Threat Intelligence Trends Report verdeutlicht die derzeit von Cyberkriminellen für Angriffe auf Unternehmen eingesetzten Schlüsseltaktiken und liefert einen detaillierten Überblick über die Cyber-Bedrohungslandschaft in den führenden Malware-Kategorien - Ransomware, Banking und Mobil. Er basiert auf Threat-Intelligence-Daten, die Check Points ThreatCloud World Cyber Threat Map für den Zeitraum von Juli bis Dezember 2016 liefert.

Wichtige Trends

- **Das Monopol auf dem Ransomware-Markt –** 2016 wurden Tausende neuer Ransomware-Varianten beobachtet. Aktuell veränderte sich die Gefahrenlandschaft erheblich und zeigt einen Trend zu immer stärkerer Zentralisierung, wobei seit einigen Monaten einige wenige wichtige Malware-Familien den Markt dominieren und Unternehmen jeglicher Grösse treffen.
- **DDoS-Angriffe über IoT-Geräte –** im August 2016 wurde das berüchtigte Mirai Botnet entdeckt - das erste Internet-der-Dinge-Botnet (IoT-Botnet) seiner Art, das gefährdete internetfähige Digitalgeräte, wie zum Beispiel Videorekorder (DVR) und Überwachungskameras (CCTV) angreift. Es verwandelt sie in Bots und nutzt die kompromittierten Geräte, um zahlreiche umfangreiche Distributed Denial of Service (DDoS)-Angriffe auszuführen. Mittlerweile steht fest, dass in fast jedem Haushalt gefährdete IoT-Geräte genutzt werden und die massiven DDoS-Angriffe, die auf ihnen aufbauen, weiterhin vorkommen werden.
- **Verwendung neuer Dateiendungen in Spam-Kampagnen –** die häufigsten in bösartigen Spamkampagnen verwendeten Infektionsvektoren im zweiten Halbjahr 2016 waren Downloader, die auf Windows Script Engine (WScript) aufbauen. In Javascript (JS) und VBScript (VBS) geschriebene Downloader dominierten das Malspam-Verbreitungsfeld zusammen mit ähnlichen, jedoch weniger bekannten Formaten, wie JSE, WSF und VBE.

Top-Malware im zweiten Halbjahr 2016:

1. **Conficker (14,5 Prozent)** - Ein Wurm, der Fernoperationen und Malware-Downloads ermöglicht. Die infizierte Maschine wird von einem Botnet kontrolliert, das seinen Command-and-Control-Server kontaktiert, um Anweisungen zu erhalten.
2. **Sality (6,1 Prozent)** - Ein Virus, der Fernsteuerung und den Download von weiterem Schadcode auf ein Gerät ermöglicht. Sein Hauptziel ist der Verbleib in einem System, sowie die Fernsteuerung und Installierung weiterer Malware.
3. **Cutwail (4,6 Prozent)** - Ein Botnet, das hauptsächlich am Versand von Spam-Emails und einigen DDoS-Angriffen beteiligt ist. Einmal installiert, verbinden sich die Bots direkt mit dem Command-and-Control-Server und erhalten Anweisungen zu den Emails, die sie versenden sollen. Nachdem sie ihre Aufgabe erledigt haben, erstatten die Bots dem Spammer Bericht mit exakten Statistiken über ihre Operationen.

4. **JBossjmx (4,5 Prozent)** - Ein Wurm, der auf Systeme abzielt, auf denen eine gefährdete Version des JBoss Application Servers installiert ist. Die Malware erstellt in gefährdeten Systemen eine bösartige JSP-Seite, um beliebige Befehle auszuführen. Darüber hinaus wird ein weiteres Backdoor erstellt, das Befehle von einem entfernten IRC-Server akzeptiert.
5. **Locky (4,3 Prozent)** – Die Ransomware wütet seit Februar 2016 und verbreitet sich hauptsächlich über Spam-Emails, die einen Downloader enthalten. Dieser tarnt sich als Word- oder Zip-Dateianhang und lädt die Malware herunter, um damit Daten auf dem Zielsystem zu verschlüsseln.

Top-Ransomware im zweiten Halbjahr 2016:
Bezogen auf alle erkannten Angriffe weltweit hat sich der Anteil der Attacken mit Verschlüsselungs-schädlingen in der zweiten Jahreshälfte 2016 von 5,5 Prozent auf 10,5 Prozent nahezu verdoppelt. Die am häufigsten entdeckten Varianten waren:

1. **Locky (41 Prozent)** - Die dritthäufigste Ransomware im 1. Halbjahr, die in der zweiten Hälfte des Jahres einen dramatischen Anstieg verzeichnete.
2. **Cryptowall (27 Prozent)** – Ursprünglich ein Doppelgänger von Cryptolocker, diesen aber schliesslich übertraf. Nach der Entfernung von Cryptolocker entwickelte sich Cryptowall zu einer der bislang bekanntesten Ransomware-Arten. Cryptowall ist für ihre Verwendung von AES-Verschlüsselung und die Durchführung von C&C-Kommunikationen über das anonyme Netzwerk Tor bekannt. Sie wird über Exploit-Kits, Malvertising und Phishing-Kampagnen weit verbreitet.
3. **Cerber (23 Prozent)** - das grösste Ransomware-as-a-Service-Konzept der Welt. Cerber ist ein Franchise-Konzept, bei dem sein Entwickler Partner rekrutiert, die Malware gegen Gewinnbeteiligung verbreitet.

Top Mobile Malware im zweiten Halbjahr 2016:
1. **Hummingbad (60 Prozent)** - Android-Malware, die erstmals vom Check Point-Forschungsteam entdeckt wurde, und die ein persistentes Rootkit auf dem Gerät einrichtet. Danach werden betrügerische Anwendungen installiert und mit leichten Änderungen zusätzliche bösartige Aktivitäten der Zugang verschlüsselten Email-Container aufgehebelt.
2. **Triada (9 Prozent)** - Modulares Backdoor für Android, das Superuser-Privilegien zum Download von Malware gewährt und die Einbettung in Systemprozesse unterstützt. Triada hat auch im Browser geladene URLs gespooft.
3. **Ztorg (7 Prozent)** – Trojaner, der ohne Wissen der Nutzer Root-Privilegien zum Download und zur Installation von Anwendungen auf Mobiltelefonen nutzt.

Top Banking-Malware:
1. **Zeus (33 Prozent)** - Trojaner, dessen Ziel Windows-Plattformen sind, und der mithilfe von Man-in-the-Browser Keylogger und Form Grabbing oft zum Stehlen von Banking-Daten eingesetzt wird.
2. **Tinba (21 Prozent)** - Banking-Trojaner, der die Zugangsdaten seiner Opfer mithilfe von Web-Injektionen stiehlt.
3. **Ramnit (16 Prozent)** – Banking-Trojaner, der Bankzugangsdaten, FTP-Passwörter, Sitzungscookies und persönliche Daten stiehlt.

Maya Horowitz**,** Threat Intelligence Group Manager bei Check Point, erläutert: „Der Bericht zeigt den Charakter des heutigen Cyber-Umfelds, in dem Ransomware-Angriffe rasant zunehmen. Der Grund dafür ist einfach: Sie funktionieren und generieren enorme Einnahmen für die Angreifer. Organisationen bemühen sich, der Bedrohung wirksam gegenzusteuern: Viele haben nicht die

richtigen Abwehrmassnahmen getroffen und ihr Personal nicht richtig geschult, so dass die Anzeichen für einen potentiellen Angriff in eingehenden Emails nicht erkannt werden."

„Darüber hinaus zeigen unsere Daten, dass nur wenige Familien für die Mehrzahl der Angriffe verantwortlich sind, während tausende anderer Malware-Familien kaum auftreten", erläutert Horowitz weiter. „Die meisten Cyberbedrohungen treten weltweit und überregional auf. Die APAC-Region hebt sich jedoch ab, denn ihre Top-Malware-Charts enthalten 5 Familien, die in den anderen regionalen Charts nicht auftauchen."

Die Statistik in diesem Bericht beruht auf Daten aus der ThreatCloud World Cyber Threat Map. Check Points ThreatCloud ist das grösste kollaborative Netzwerk zur Bekämpfung von Internetkriminalität und liefert aktuellste Bedrohungsdaten und Cyberangriffstrends aus einem weltumspannenden Netz von Bedrohungssensoren. Die ThreatCloud-Datenbank identifiziert täglich Millionen Malware-Typen und enthält über 250 Millionen auf Bot-Erkennung untersuchte Adressen sowie über 11 Millionen Malware-Signaturen und 5,5 Millionen infizierte Webseiten.

Eine vollständige Version des Berichts finden Sie hier.

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

Über Check Point Software Technologies
Check Point Software Technologies (www.checkpoint.com) ist der grösste Pure-Play Netzwerk- und Cybersicherheitsanbieter weltweit. Als Marktführer der Cybersicherheitsbranche bietet Check Point die führende Technologie und schützt seine Kunden vor Cyberattacken mit einer unschlagbaren Fangquote bei Malware und anderen Bedrohungen. Check Point bietet eine umfassende Sicherheitsarchitektur, um Unternehmen zu schützen. Egal, ob Netzwerk oder Mobilgerät – Check Point deckt alle Bereiche ab und kann diese über seine leicht verständliche Sicherheitsmanagementplattform verwalten. Über 100'000 Organisationen vertrauen auf den Schutz von Check Point. Check Point, one step ahead of cyber criminals.
Check Point Alps (Schweiz und Österreich) mit Sitz in Zürich und Wien und einem Branchoffice in Vevey (Schweiz) beschäftigt mehr als 30 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