Cryptominer infizierten Unternehmen im Jahr 2018 zehnmal häufiger als Ransomware – nur jeder fünfte IT-Profi ist informiert

Das zweite Kapitel des Security Reports hebt die allgemeine Nutzbarkeit der Cyberkriminalität durch Malware-as-a-Service sowie die grössten Cyber-Bedrohungen hervor

CPX360 LAS VEGAS, USA – 6. Februar 2019. Check Point® Software Technologies Ltd. (NASDAQ: CHKP), ein weltweit führender Anbieter von Cybersicherheitslösungen, hat das zweite Kapitel seines Sicherheitsberichts 2019 veröffentlicht. Darin zeigt sich, wie die Instrumente und Dienste, die zur Begehung von Internet-verbrechen eingesetzt werden, allgemein verfügbar gemacht wurden. Fortschrittliche Angriffsmethoden stehen jetzt jedem zur Verfügung, der bereit ist, für sie zu zahlen. Sie sind Teil der wachsenden „Malware-as-a-Service"-Industrie, die sich auch inhaltlich stetig weiterentwickelt.

Das zweite Kapitel des Security Reports 2019 enthüllt die wichtigsten Cyber-Angriffstrends, die Forscher von Check Point im Jahr 2018 beobachtet haben, und zeigt das signifikante Wachstum getarnter, komplexer Angriffe, die darauf abzielen, unter dem Radar der Unternehmenssicherheit zu bleiben. Das Kapitel zeigt auch die Arten von Cyberangriffen, die IT- und Sicherheitsteams in Unternehmen als die grössten Bedrohungen für ihre Unternehmen einstufen. Zu den Highlights gehören:

- **Cryptominer, die unentdeckt in Netzwerken schürfen:** Cryptominer infizierten im Jahr 2018 zehnmal häufiger Unternehmen als Ransomware. Davon wusste jedoch nur jeder fünfte IT-Sicherheitsexperte. 37 Prozent der Unternehmen weltweit wurden 2018 von Cryptominern befallen, und 20 Prozent der Unternehmen werden weiterhin jede Woche infiziert, trotz eines Rückgangs der Krypto-Währungswerte an den einschlägig bekannten Börsen um 80 Prozent.

- **Das Bedrohungsrisiko der Cryptominer wird von Unternehmen unterschätzt:** Auf die Frage, was sie als die grössten Bedrohungen für ihr Unternehmen einschätzen, antworteten nur 16 Prozent mit Crypto-Mining, verglichen mit DDoS-Angriffen (34%), Datenschutzverletzungen (53%), Ransomware (54%) und Phishing (66%). Dies ist bedenklich, da Cryptominer leicht als heimliche Hintertüren fungieren können, um andere Arten von Malware herunterzuladen und zu starten.

- **Malware-as-a-Service wird gefährlicher:** Das GandCrab Ransomware-as-a-Service Affiliate-Programm zeigt, wie nun auch Amateure vom Ransomware-Erpressungsgeschäft profitieren können. Cyberkriminelle behalten bis zu 60 Prozent der gesammelten Lösegelder, und ihre Entwickler bis zu 40 Prozent. GandCrab hat zum Beispiel über 80 aktive Partner und innerhalb von zwei Monaten im Jahr 2018 über 50'000 Netzwerke infiziert, sowie zwischen 300'000 und 600'000 US-Dollar als Lösegeld gefordert.

„Das zweite Kapitel unseres Security Reports 2019 zeigt, wie Cyberkriminelle erfolgreich und heimlich neue Ansätze und Geschäftsmodelle wie etwa Malware-Affiliate-Programme erforschen, um ihre illegalen Einnahmen zu maximieren und gleichzeitig das Risiko der Aufdeckung zu verringern. Aber aus den Augen sollte nicht aus dem Sinn heissen: Auch wenn Cyberangriffe im Jahr 2018 weniger auffällig waren, sind sie dennoch schädlich und gefährlich", sagt Peter Alexander, Chief Marketing Officer von Check Point Software Technologies. „Durch die Überprüfung und Hervorhebung dieser Entwicklungen können Unternehmen ein besseres Verständnis für die Bedrohungen entwickeln, denen sie ausgesetzt sind, und lernen, wie sie letztlich verhindern, dass sich diese auf ihr Unternehmen auswirken."

Der Security Report 2019 basiert auf den Daten der ThreatCloud Intelligence von Check Point, dem grössten kollaborativen Netzwerk zur Bekämpfung von Cyberkriminalität, das Bedrohungsdaten und Angriffstrends aus einem globalen Netzwerk von Bedrohungssensoren liefert. Gefüttert wird dieses Netzwerk mit den Erkenntnissen von Check Point innerhalb der letzten zwölf Monaten, sowie aus einer brandneuen Umfrage unter IT-Fachleuten, Führungskräften und Managern, die ihr Verständnis von und ihre Vorbereitungen auf die heutigen Bedrohungen bewertet. Der Bericht untersucht die neuesten Bedrohungen für verschiedene Industriesektoren und gibt einen umfassenden Überblick der Trends, die in der Malware-Landschaft, in neu entstehenden Datenverlust-Vektoren und bei staatlichen Cyberangriffen beobachtet werden. Er beinhaltet auch Expertenanalysen der Check Point-Sicherheitsforscher, um Unternehmen dabei zu unterstützen, sich auf die aktuellen, komplexen Cyberangriffe und Bedrohungen der vierten, sowie der kommenden fünften Generation vorzubereiten.

Der gesamte Report kann hier heruntergeladen werden.

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 Intelligence-Community. Das Forschungsteam sammelt und analysiert globale Cyber-Angriffsdaten, die in 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 internationalen 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

