RANSOMWARE-ANGRIFFE NEHMEN RASANT ZU

Check Points Global Threat Intelligence Trends Report zeigt: Der Anteil der Attacken mit Ransomware hat sich in der zweiten Hälfte 2016 von 5,5 Prozent auf 10,5 Prozent nahezu verdoppelt. Das klassische IT-Security-Modell, welches auf Bedrohungen lediglich reagiert, reicht heute nicht mehr aus, um Unternehmen zu schützen.

→ VON SONJA MEINDL

Check Points Global Threat Intelligence Trends Report für die zweite Hälfte 2016 beleuchtet die wichtigsten Trends bei Netzwerk- und mobiler Malware. Besonders auffällig: Angriffe mit Verschlüsselungsschädlingen haben sich beinahe verdoppelt. Die Statistiken beruhen auf Daten aus der ThreatCloud World Cyber Threat Map für den Zeitraum von Juli bis Dezember 2016.

GLOBALES NETZ

Check Points ThreatCloud ist das grösste kollaborative Netzwerk zur Bekämpfung von Internetkriminalität und liefert aktuellste Bedrohungsdaten und Cyberangriff-Trends 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.

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 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, stark zunehmen werden.

NEUE 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.

DIE 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 eine weitere Backdoor erstellt, welche 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.

DIE TOP-RANSOMWARE IM ZWEITEN HALBJAHR 2016:

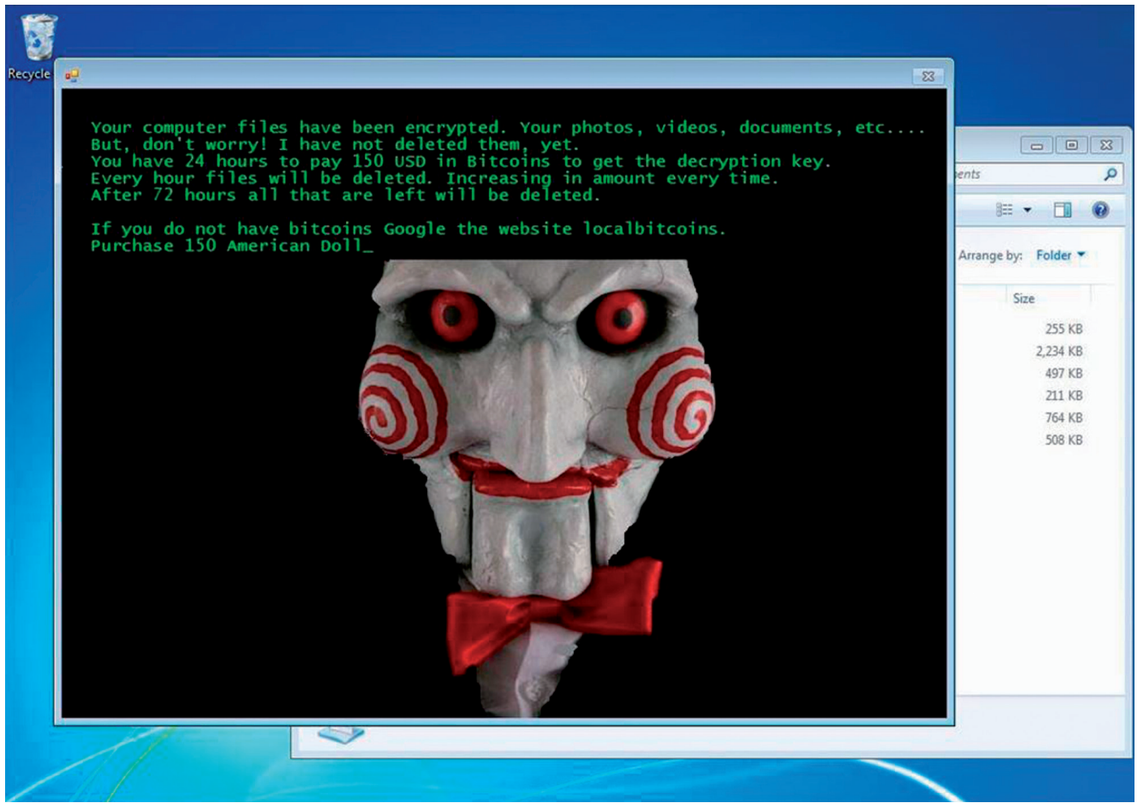
Bezogen auf alle erkannten Angriffe weltweit hat sich der Anteil der Attacken mit Verschlüsselungsschädlingen in der zweiten Jahreshälfte 2016 von 5,5 Prozent auf 10,5 Prozent nahezu verdoppelt. Die am häufigsten entdeckten Varianten waren:

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.

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

THREAT PREVENTION: INFEKTIONEN VOR DEM EINDRINGEN STOPPEN

Der Bericht zeigt auch: Infektionen müssen gestoppt werden, bevor sie ins Netzwerk eindringen. Threat-Prevention-Lösungen der nächsten Generation können mit advanced Sandboxing neue, unbekannte Malware stoppen. Ein Endpunktgerät wird imitiert und der Datenverkehr geprüft, sodass Dateien, die Malware enthalten, blockiert werden, bevor sie ins Netzwerk gelangen. Lösungen zur Dokumentbereinigung entfernen jegliche Schadcodes aus allen eingehenden Dateien und Dokumenten und verbessern somit erheblich den Schutz. Diese Techniken unterstützen vorhandene, signaturbasierte Schutzmassnamen und rüsten Organisationen für die Abwehr von Angriffen. ←



Der Anteil der Attacken mit Ransomware hat sich in der zweiten Hälfte 2016 nahezu verdoppelt.

Zur Autorin

Sonja Meindl ist diplomierte Wirtschafts-Ingenieurin und verantwortet als Country Manager seit 2012 die Geschäfte von Check Point in der Schweiz und in Österreich.

Zum Unternehmen:
Check Point Software Technologies 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 Alps (Schweiz und Österreich) mit Sitz in Zürich und Wien beschäftigt mehr als 30 Mitarbeitende.

Mehr Informationen:
www.checkpoint.com

Check Point SOFTWARE TECHNOLOGIES LTD.

Dieser Beitrag wurde von **Check Point Software Technologies** zur Verfügung gestellt und stellt die Sicht des Unternehmens dar. Computerworld übernimmt für dessen Inhalt keine Verantwortung.