IBM DACH Newsroom

IBM X-Force Report: Cyberkriminelle setzten 2018 vermehrt auf Kryptojacking

Mehr als die Hälfte der Cyberangriffe waren keine Malware-basierten Angriffe/ Zahl der Attacken auf geschäftliche E-Mail-Adressen gestiegen

CAMBRIDGE, MA, USA - 26 Feb 2019: IBM Security gibt die Ergebnisse des X-Force Threat Intelligence Index 2018 bekannt: Erhöhte Sicherheitsmaßnahmen und ein gestiegenes Bewusstsein gegenüber Cyberangriffe zwingen Cyberkriminelle dazu, ihre Angriffstechniken auf der Suche nach Profit zu ändern. Der Bericht beschreibt insbesondere zwei wesentliche Veränderungen: Ein geringerer Einsatz von Malware und eine überraschende Abkehr von Ransomware.

IBM X-Force verzeichnete einen deutlichen Rückgang der Angriffe mit Ransomware. So verfolgten die IBM Spam-Forscher im letzten Jahr nur eine Ransomware-Kampagne aus dem weltweit größten Botnetz zur Verteilung von Malware-Spam, Necurs. Auffällig ist auch, dass die Anzahl der Kryptojacking-Angriffe fast doppelt so hoch war wie die der Ransomware-Angriffe im Jahr 2018. Grund dafür ist die höhere Profitabilität: Indem heimlich die Rechenleistung der Opfer genutzt wird, sind Kryptojacking-Angriffe weniger risikoreich und mit geringerem Aufwand verbunden. Zudem erreichten Kryptowährungen wie Bitcoin 2018 einen Preis von fast 20.000 US-Dollar.

Generell ändern sich die Tarnmethoden der Datendiebe, anstelle von Malware, missbrauchen Cyberkriminelle zunehmend Betriebssystem-Tools. Mehr als die Hälfte aller Cyberattacken (57 Prozent) nutzten gängige Administrationsanwendungen wie PowerShell oder PsExec, um unentdeckt zu bleiben. Gezielte Phishing-Angriffe machen hingegen fast ein Drittel (29 Prozent) aller Cyberangriffe aus.

Der IBM X-Force Threat Intelligence Index umfasst Erkenntnisse und Beobachtungen aus der Überwachung von 70 Milliarden Sicherheitsereignissen pro Tag in mehr als 130 Ländern. Darüber hinaus werden Daten aus verschiedenen Quellen gesammelt und analysiert, darunter X-Force IRIS, X-Force Red, IBM Managed Security Services und öffentlich zugängliche Informationen über Datenschutzverletzungen. Außerdem legt die IBM X-Force Einheit Tausende von Spam-Fallen weltweit aus und beobachtet täglich Millionen von Spam- und Phishing-Angriffen. Milliarden von Webseiten und Bildern werden analysiert, um betrügerische Handlungen und Markenmissbrauch aufzudecken.

Weitere Ergebnisse des Reports:

- Anstieg von Schwachstellen: Beinahe ein Drittel (42.000) der insgesamt 140.000 von IBM X-Force erfassten Schwachstellen wurden allein in den vergangenen drei Jahren gemeldet. IBM X-Force fand durchschnittlich 1.440 einmalige Schwachstellen pro Unternehmen.
- Fehlkonfigurationen machen Unternehmen immer noch zu schaffen: Im Jahresvergleich stiegen die öffentlich bekannt gegebenen Fehlkonfigurationen um 20 Prozent an. Interessant ist, dass im Gegensatz dazu die Anzahl kompromittierter Datensätze um 52 Prozent sank.
- BEC-Betrug ist weiterhin Spitzenreiter: Phishing-Kampagnen zielten besonders auf Business Email Compromise (BEC)-Betrügereien ab. Sie machten 45 Prozent der von X-Force verfolgten Phishing-Angriffe aus.

- Transportbranche rückt ins Visier von Cyberangriffen: Die Transportbranche entwickelte sich 2018 zum zweithäufigsten angegriffenen Sektor – sie stieg von Platz 10 (2017) auf Platz 2 (2018).

„Wenn wir uns den geringen Einsatz von Malware, die Abkehr von Ransomware und den Anstieg von gezielten Angriffen anschauen, ist zu erkennen, dass der Return-on-Investment (ROI) eine große Motivation für Cyberkriminelle ist. Wir sehen aber auch, dass die Bemühungen, Systeme besser vor Angriffen zu schützen, funktionieren. Durch den Diebstahl von 11,7 Milliarden Datensätzen in den letzten drei Jahren, haben personenbezogene Daten an Wert verloren. Stattdessen werden neue illegale Profit-Modelle erforscht“, sagt Wendi Whitmore, Director, IBM X-Force Threat Intelligence. „Rechenleistung zählt zu den begehrtesten Waren, die mit der Entstehung von Kryptowährungen zusammenhängt. Das führt dazu, dass Unternehmensnetzwerke und Verbrauchergeräte heimlich gehackt werden, um diese digitalen Währungen zu schürfen.“

Der Aufstieg krimineller Power-User von PowerShell

Die Studie zeigt, dass Cyberkriminelle viel häufiger bestehende Betriebssystem-Tools angreifen, um damit ihre Ziele zu erreichen. Der Fokus liegt bei dieser Technik auf PowerShell. Hierbei handelt es sich um ein integriertes Betriebssystems-Tool, das in der Lage ist, Codes auf dem Speicher auszuführen und direkten administrativen Zugriff auf das Gerät zu gewähren. Ebenso beobachtete IBM X-Force Incident Response and Intelligence Services (IRIS) Cyberangreifer, die Windows Management Interface Command (WMIC)-Abfragen ausführen. Ziel ist es, ferngesteuerte PowerShell-Befehle und -Skripte zu automatisieren und somit unter Anderem, Zugriff auf bestimmte Systeme, Benutzerverzeichnisse oder Datenbanken zu erhalten.

Geschäfte machen mit Cyberangriffen auf Kosten von Unternehmen

Cyberkriminelle geben nicht viel Geld für teure Hardware oder Kryptowährungen aus. Stattdessen haben sie verschiedene Werkzeuge und Taktiken entwickelt, um sowohl Unternehmensserver als auch einzelne Nutzer mit Coin-Mining-Malware zu infizieren und sie damit zu kapern. Unerkanntes Mining erhöht die CPU-Auslastung und setzt die Leistungsfähigkeit der Systeme für ihre regulären Aufgaben massiv herab. Dieser Trend des Kryptojackings boomt geradezu.

Während illegale Kryptojacking-Angriffe auf dem Vormarsch sind, nimmt die Bedeutung von Ransomware für Cyberkriminelle ab. Im Laufe des Jahres 2018 sanken die Versuche, Ransomware auf X-Force-überwachten Geräten in Q4 (Oktober bis Dezember) zu installieren, auf weniger als die Hälfte (45 Prozent) der Versuche in Q1. Stattdessen haben sich die Kryptojacking-Angriffe im gleichen Zeitraum um 450 Prozent mehr als vervierfacht.

Transportbranche gerät ins Visier der Hacker

Cyberkriminelle ändern nicht nur ihre Vorgehensweise, sondern auch ihre Zielgruppe. Zwar war die Finanzindustrie mit 19 Prozent aller Angriffe erneut Spitzenreiter unter den Angriffszielen, die Transportindustrie holte jedoch deutlich auf. Gegenüber dem Vorjahr verdreifachten sich hier die Angriffsversuche: Während sie 2017 nicht einmal unter den Top 5 war, steht diese Industrie 2018 an Platz zwei.

Dabei geht es nicht nur um die Anzahl der Cyberangriffe, sondern auch um die Auswahl der Opfer. X-Force

beobachtete, dass 2018 wesentlich mehr Angriffe im Transportsektor öffentlich bekannt gemacht wurden als in den Vorjahren. Dadurch fühlten sich Hacker wahrscheinlich ermutigt, denn diese Offenlegung zeigt ihnen: Diese Unternehmen sind anfällig für Cyberangriffe und verfügen über wertvolle Kundendaten wie Zahlungskarteninformationen, personenbezogene Daten und Treuepunkte.

Der neue IBM Bericht enthält Daten, die das X-Force-Security-Team zwischen dem 1. Januar 2018 und dem 31. Dezember 2018 erhoben hat, um Informationen über die globale Bedrohungslandschaft zu liefern und Sicherheitsexperten über die für ihr Unternehmen wichtigsten Bedrohungen zu informieren. Um eine Kopie des IBM X-Force Threat Index 2019 herunterzuladen, besuchen Sie bitte: https://www.ibm.com/security/data-breach/threat-intelligence.

Über IBM Security
IBM Security bietet eines der fortschrittlichsten und integriertesten Portfolios an Produkten und Dienstleistungen für die Unternehmenssicherheit. Das Portfolio, das von der weltweit agierenden IBM X-Force®-Forschung unterstützt wird, ermöglicht es Unternehmen, Risiken effektiv zu managen und sich gegen neue Bedrohungen zu schützen. IBM betreibt eine der weltweit breitesten Forschungs-, Entwicklungs- und Serviceorganisationen für Sicherheit, überwacht 70 Milliarden Sicherheitsereignisse pro Tag in mehr als 130 Ländern und hält weltweit mehr als 10.000 Sicherheitspatente. Weitere Informationen finden Sie unter www.ibm.com/security, folgen Sie @IBMSecurity oder besuchen Sie den IBM Security Intelligence blog

Kontaktinformation

Annette Fassnacht

Unternehmenskommunikation IBM Deutschland +49 (0)160 90105052 annettefassnacht@de.ibm.com

---

https://de.newsroom.ibm.com/2019-02-26-IBM-X-Force-Report-Cyberkriminelle-setzten-2018-vermehrt-auf-Kryptojacking