BlackBerry. Intelligent Security. Everywhere.

BLACKBERRY VERHINDERT REVIL RANSOMWARE

BUSINESS BRIEF

Laut FBI[1] steckt hinter den massiven Ransomware-Angriffen vom 30. Mai 2021 auf JBS[2], den weltgrößten Fleischkonzern, und andere namhafte Firmen eine Ransomware-as-a-Service (RaaS)-Gruppe namens REvil[3]. Sie ist auch als Sodin/Sodinokibi[4] bekannt. Nach einer kurzen Stilllegung konnte JBS bereits am 2. Juni 2021[5] den Betrieb wieder aufnehmen.

Solche Ransomware-Angriffe sind eine echte Gefahr. Denn sie können potenziell die globale Versorgungskette nachhaltig unterbrechen. Und sie zeigen ganz deutlich auf, wie wichtig es ist, kritische Infrastrukturen weltweit abzusichern.

KEINE GEFAHR FÜR BLACKBERRY KUNDEN

Die intelligenten BlackBerry Lösungen BlackBerry® Protect, BlackBerry® Optics und BlackBerry® Guard haben auch bei diesen Angriffen ihre Effektivität wieder unter Beweis gestellt. Sie haben – wie schon bei anderen Ransomware-Attacken – die Angriffe von REvil auf BlackBerry Kunden zuverlässig gestoppt. Das Threat Research Team[6] von BlackBerry hat die Angriffsmethoden von REvil[3] gründlich analysiert und gibt seinen Kunden folgende Empfehlungen:

- BlackBerry Protect, die KI-gesteuerte Endpoint Protection Lösung von BlackBerry, schützt zuverlässig vor REvil-Angriffen. Denn sie hindert die Ransomware an der Ausführung. Zum Schutz vor Malware und Speicherausnutzung empfiehlt BlackBerry seinen Kunden, die Protect-Funktionen im vollständigen Blockiermodus zu aktivieren.
- BlackBerry Optics, die Endpoint Detection and Response Lösung von BlackBerry, ergänzt BlackBerry Protect mit Regelsätzen zur Erkennung- und Schadensminimierung. BlackBerry empfiehlt seinen Kunden folgende BlackBerry Optics Regeln zu aktivieren:
  - Win WMI Process Enumeration Mitre T1082
  - Win WMI IntrinsicEvent Mitre T1047
  - Win FileExtensions LocalSystemCollection NonSYS Mitre T1005

Außerdem empfiehlt BlackBerry seinen Kunden den Download und die Aktivierung der neuen BlackBerry Optics Regeln, da diese REvil über Telemetriedaten erkennen.

BlackBerry Guard, der abonnementbasierte Managed Detection and Response (MDR) Service von BlackBerry, schützt vor REvil-Ransomware und Zero-Day-Bedrohungen durch:

- Maßgeschneiderte Bereitstellung von BlackBerry Protect und BlackBerry Optics
- 24x7 Threat Monitoring durch BlackBerry® Security Services Experten für Incident Response und Prävention
- Monitoring, Verwaltung und Orchestrierung von Warnmeldungen
- Erkenntnisgestützte Bedrohungssuche

PREVENTION-FIRST: EIN ANSATZ, DER SICH LOHNT

BlackBerry minimiert nachhaltig Ihre Cyberrisiken. Denn der Prevention-First-Ansatz verhindert, dass Ihre Netzwerke, Mitarbeiter und Endgeräte durch Malware und Zero-Day-Bedrohungen gefährdet werden: Die Malware wird neutralisiert, bevor sie die Kill Chain erreicht. Dieser Ansatz von BlackBerry verhindert nicht nur Sicherheitsvorfälle, sondern reduziert auch die Komplexität der Infrastruktur und rationalisiert Ihr Sicherheitsmanagement.

BlackBerry® Cyber Suite Lösungen erkennen und verhindern Angriffe zuverlässig mithilfe einer Cylance® KI-Engine der siebten Generation. Denn diese wurde kontinuierlich mit mittlerweile Milliarden bekannter bösartiger und gutartiger Dateien trainiert. Die Detection and Response Logik bietet Ihnen einen mehrschichtigen Schutz direkt am Endpunkt. Unabhängig von Cloud-Lookups oder einer Internetverbindung.

1 FBI attributes JBS ransomware attack to REvil

2 Meat Buyers Scramble After Cyberattack Hobbles JBS

3 Threat Thursday: Dr. REvil Ransomware Strikes Again, Employs Double Extortion Tactics

4 Threat Spotlight: Sodinokibi Ransomware

5 JBS meat plants reopen across U.S.

6 Über das BlackBerry Research and Intelligence Team

BlackBerry Intelligent Security. Everywhere.

BlackBerry (NYSE: BB; TSX: BB) bietet intelligente Sicherheitssoftware und -dienste für Unternehmen und Regierungen weltweit. Das Unternehmen sichert mehr als 500 Millionen Endpunkte ab, darunter 195 Millionen Fahrzeuge. Das Unternehmen mit Sitz in Waterloo, Ontario, setzt KI und maschinelles Lernen ein, um innovative Lösungen in den Bereichen Cybersicherheit, Sicherheit und Datenschutz zu liefern, und ist in den Bereichen Endpoint Security, Endpoint Management, Verschlüsselung und eingebettete Systeme führend. Die Vision von BlackBerry ist klar – das Sichern einer vernetzten Zukunft, der Sie vertrauen können.

*Besuchen Sie für weitere Informationen **BlackBerry.com** und folgen Sie **@BlackBerry**.*