



 **BlackBerry**® Intelligent Security. Everywhere.

## **BLACKBERRY SCHÜTZT KUNDEN VOR NOBELIUM-ATTACKEN**



Am 27. Mai 2021 warnte das Microsoft Threat Intelligence Center<sup>1</sup> vor neuen Angriffen der NOBELIUM-Gruppe, die auch hinter den Angriffen auf SolarWinds steckt. Die neue Spear-Phishing-Kampagne traf mehr als 150 Regierungsbehörden, Think Tanks, Beratungsunternehmen und NGOs in 24 Ländern<sup>2</sup>. Eines der Opfer war die Behörde der Vereinigten Staaten für Entwicklungszusammenarbeit (USAID). Im ersten Schritt verschaffte sich die Gruppe Zugang zum E-Mail-System der Behörde, um dann im zweiten Schritt Spear-Phishing-Nachrichten zu versenden, die auf bösartige URLs führten.

Diese Nachrichten wurden so massenhaft verschickt, dass viele von ihnen automatisch von Spamfiltern abgefangen wurden. Nichtsdestotrotz gilt es bei Spear-Phishing-Kampagnen wachsam zu bleiben, da sich die Taktiken der Angreifer schnell ändern können.

## **BLACKBERRY KUNDEN WAREN GESCHÜTZT**

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 Malware-Angriffen – die Angriffe von NOBELIUM auf BlackBerry Kunden zuverlässig gestoppt. Das Threat Research Team<sup>3</sup> von BlackBerry hat die Angriffsmethoden von NOBELIUM gründlich analysiert und gibt seinen Kunden folgende Empfehlungen:

- BlackBerry Protect, die KI-gesteuerte Endpoint Protection Lösung von BlackBerry, schützt zuverlässig vor NOBELIUM-Angriffen. Denn sie hindert die Malware 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, sorgt für Schadensminimierung. BlackBerry empfiehlt seinen Kunden folgende Regeln zu aktivieren:
  - Win Rundll32 Usage Mitre T1218
  - Win Explorer.exe calling Rundll32 Mitre T1218
- Auch BlackBerry Guard schützt zuverlässig vor NOBELIUM-Angriffen. Der abonnementbasierte Managed Detection and Response (MDR) Service von BlackBerry bietet Ihnen:
  - 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

Sollten Sie den Verdacht haben, dass Sie selbst ein Opfer dieses Malware-Angriffs geworden sind, lesen Sie bitte den Abschnitt „Indicators of Compromise“ im Microsoft-Dokument [Breaking down NOBELIUM's latest early-stage toolset](#).

<sup>1</sup> [New sophisticated email-based attack from NOBELIUM](#)

<sup>2</sup> [Russian hackers launch major cyberattack through U.S. aid agency's email system, Microsoft says](#)

<sup>3</sup> [Über das BlackBerry Research and Intelligence Team](#)

## *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 bössartiger und gutartiger Dateien trainiert. Die Detection and Response Logik bietet Ihnen einen mehrschichtigen Schutz direkt am Endpunkt. Unabhängig von Cloud-Lookups oder einer Internetverbindung.

 **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.

© 2021 BlackBerry Limited. Marken, einschließlich aber nicht beschränkt auf BLACKBERRY und EMBLEM Design, sind Marken oder registrierte Marken von BlackBerry Limited, das sich die exklusiven Rechte an diesen Marken ausdrücklich vorbehält. Alle anderen Marken sind Eigentum ihrer jeweiligen Inhaber. BlackBerry ist nicht verantwortlich für Produkte oder Services von Drittanbietern.

Besuchen Sie für weitere Informationen [BlackBerry.com](https://www.blackberry.com) und folgen Sie [@BlackBerry](https://twitter.com/BlackBerry).

