BlackBerry | Cybersecurity

EXECUTIVE SUMMARY

GLOBAL THREAT INTELLIGENCE REPORT

JUNI 2024

BERICHTSZEITRAUM: 1. JANUAR – 31. MÄRZ 2024

Der neue BlackBerry® Global Threat Intelligence Report liefert Ihnen die wichtigsten Erkenntnisse zu aktuellen Cyberbedrohungen und Abwehrmaßnahmen, die Sie als SOC-Manager oder CISO kennen sollten.

Der Bericht analysiert umfangreiche Angriffsdaten, die aus internen Berichten und externen Quellen stammen und nach geografischen Regionen und Branchen geordnet sind. Die Hauptthemen sind:

- Vorherrschende Malware-Typen
- Dominante Bedrohungsgruppen
- Zweckentfremdete Software-Tools
- Schwachstellen in weitverbreiteter Software
- MITRE-Gegenmaßnahmen, mit denen Ihr SOC-Team Cyberbedrohungen identifizieren und beseitigen kann

Die Zahl der Cyberangriffe ist im ersten Quartal 2024 erneut gestiegen. BlackBerry verzeichnete **3,1 Millionen versuchte Cyberangriffe** auf seine Kunden. Das sind **17 Prozent mehr pro Tag** als im letzten Bericht.

Darüber hinaus beobachtete die Telemetrie insgesamt **630.000 einzigartige Malware-Hashes**, die auf BlackBerry Kunden abzielten. **Dies entspricht einem Anstieg von mehr als 40 Prozent pro Minute** im Vergleich zum letzten Berichtszeitraum Ende 2023.

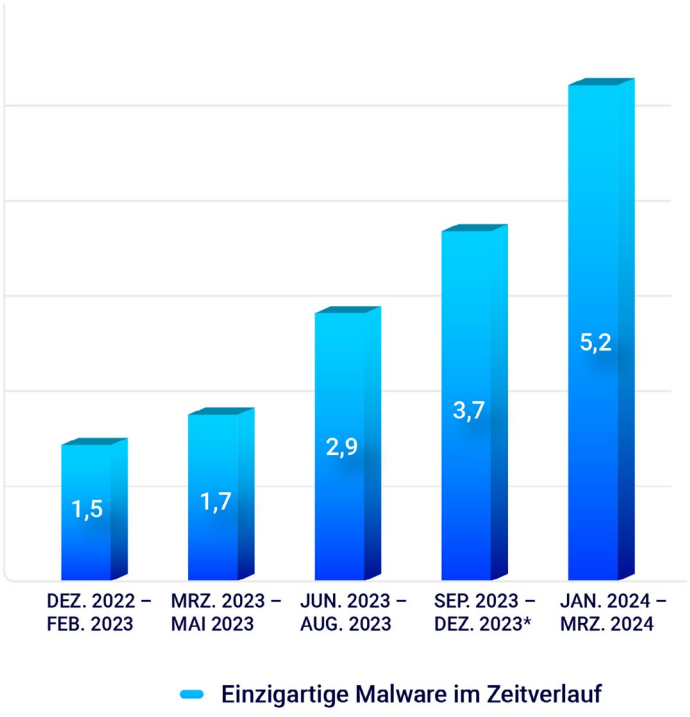

Abbildung 1: Einzigartige Malware-Hashes pro Minute, die von den BlackBerry Cybersecurity-Lösungen erkannt wurden.
(*Der Zeitraum von Sept. 2023 bis Dez. 2023 umfasste 120 Tage).

Ob Angreifer bekannte Malware verwenden oder einen einzigartigen Malware-Hash erstellen, hängt von der Art des Angriffs und dem Ziel ab. Wenn große Unternehmen in einer bestimmten Branche das Ziel sind, werden die Angreifer das Unternehmen in der Regel mit Phishing-E-Mails und Standard-Malware-Anhängen überfluten, in der Hoffnung, dass diese arglos geöffnet werden.

Hat es eine professionell ausgerüstete Bedrohungsgruppe jedoch auf ein bestimmtes, hochrangiges Ziel – wie etwa einen CFO – abgesehen, wird maßgeschneiderte Malware eingesetzt, um die Sicherheitsmaßnahmen zu umgehen.

ZENTRALE ERKENNTNISSE

Dies sind die wichtigsten Ergebnisse des aktuellen Berichtszeitraums:

- 60 Prozent der Angriffe richteten sich gegen kritische Infrastrukturen. Die BlackBerry® Cybersecurity-Lösungen **stoppten über 1,1 Millionen Angriffe**. Die meisten Angriffe zielten auf den Finanzsektor, das Gesundheitswesen sowie Regierungen und Behörden.

  Die US-amerikanische Cybersicherheitsbehörde CISA zählt 16 Sektoren zu den kritischen Infrastrukturen, darunter das Gesundheitswesen, Regierungen und Behörden, Energie- und Landwirtschaft, Finanzen und Verteidigung. Der Trend zur Digitalisierung erhöht auch in diesen Sektoren die Anfälligkeit für Cyberkriminalität. Neu entdeckte Schwachstellen und Social-Engineering-Kampagnen, um wertvolle Zugangsdaten zu stehlen und Malware zu verbreiten, sind bei Angreifern besonders beliebt.

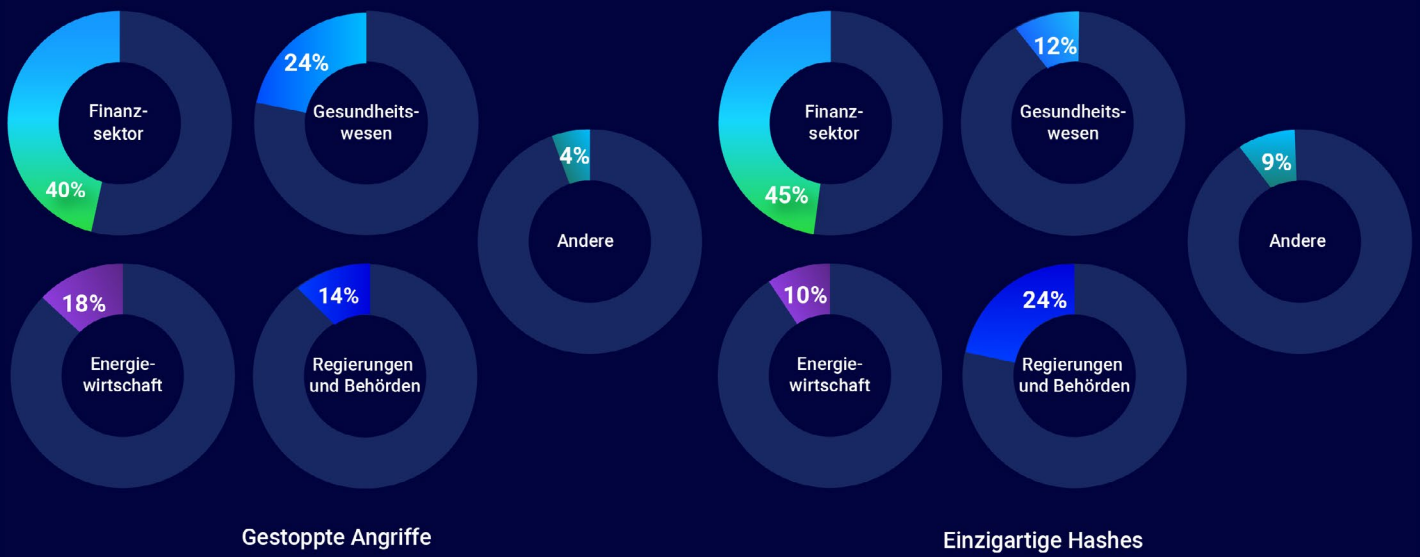

Abbildung 2: Branchenspezifische Angriffe im Vergleich zu einzigartigen Malware-Hashes.

- **Cyberkriminelle nutzen zunehmend Schwachstellen** in gängigen Software-Tools und Dienstprogrammen aus. BlackBerry verzeichnete im Berichtszeitraum rund **9.000 neue Common Vulnerabilities and Exposures (CVEs)**. Bedrohungsgruppen nutzten beispielsweise die legitime Software ConnectWise ScreenConnect und mehrere echte IT-Management-Produkte von Ivanti, um Malware zu verbreiten.

- **Auch die Ransomware-Angriffe auf das Gesundheitswesen haben wieder zugenommen.** Wenn Krankenhäuser, Kliniken, Apotheken und Ausgabestellen von Arzneimitteln lahmgelegt werden, können Patienten lebenswichtige Medikamente und medizinische Behandlungen nicht erhalten: Menschenleben stehen auf dem Spiel. Zudem lassen sich sensible Daten aus dem Gesundheitswesen im Darknet leicht versilbern. Deshalb wird diese Branche auch in Zukunft verstärkt unter Beschuss stehen.

- **Die neue Rubrik „Who's Who in Ransomware“** befasst sich mit den derzeit wichtigsten Ransomware-Angreifern und neu entstehenden Gruppen. So ist beispielsweise Hunters International erst seit Ende 2023 aktiv und bereits ein bekanntes, weltweit agierendes Ransomware-as-a-Service (RaaS)-Verbrechersyndikat. Ransomware-Gruppen haben sich darauf spezialisiert, herkömmliche Cybersicherheitsmaßnahmen zu umgehen. Jede neue Sicherheitslücke ist für sie eine gute Gelegenheit, Kasse zu machen. Das macht Ransomware auch weiterhin zu einer ernsthaften Bedrohung.

- **Politisch motivierte Cyberangriffe dominieren die Rubrik „Geopolitical Analysis“.** Internationale Spannungen und regionale Unruhen spiegeln sich in einer deutlichen Zunahme von Spyware, Datendiebstahl und Spionageangriffen wider. Im Februar entdeckten Mitglieder des Unterausschusses für Sicherheit und Verteidigung des Europäischen Parlaments Spionagesoftware auf ihren Mobiltelefonen. Im März 2024 fingen russische Cyberkriminelle Gespräche zwischen deutschen Militärs über eine mögliche militärische Unterstützung der Ukraine ab. Ebenfalls im März entdeckten das US-Justizministerium und das FBI, dass chinesische Cyberkriminelle mehrere britische, europäische, US-amerikanische und kanadische Mitglieder der Interparlamentarischen Allianz gegen China (IPAC) ins Visier genommen hatten. Auch israelische, palästinensische und iranische Gruppen haben es auf kritische Infrastrukturen und Wirtschaftsunternehmen der jeweils anderen Seite abgesehen.

- **56 Prozent** der CVEs haben einen Schweregrad von 7 oder höher auf dem Common Vulnerability Scoring System (CVSS), das von 1 bis 10 reicht. Diese CVEs werden direkt von Malware-Entwicklern für Ransomware-Kampagnen und Informationsdiebstahl ausgenutzt.

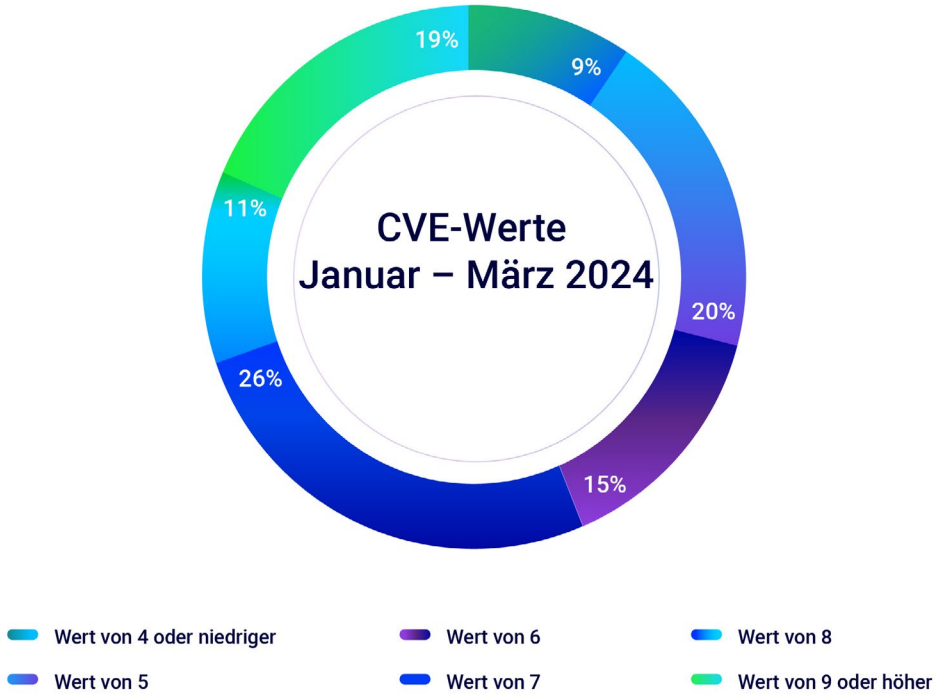

Abbildung 3: CVE-Werte in den ersten drei Monaten des Jahres 2024.

▶ Der Abschnitt über **gängige MITRE-Techniken und angewandte Gegenmaßnahmen** hilft SOC-Teams, bösartige Taktiken und Techniken besser zu erkennen und abzuwehren. Aus dem MITRE ATT&CK®-Framework mit über 300 Angriffsarten hat BlackBerry die 20 wichtigsten Techniken dokumentiert, die von Angreifern verwendet werden. Für die fünf wichtigsten Techniken haben die Analysten von BlackBerry® Gegenmaßnahmen entwickelt.

Der BlackBerry Global Threat Intelligence Report fasst die Recherchen, Analysen und Ergebnisse unseres Cyber Threat Intelligence (CTI)-Teams, unseres Incident Response (IR)-Teams und unserer CylanceMDR™*-Spezialisten zusammen. Er bietet Expertenanalysen zu aktuellen kritischen Themen und Herausforderungen im Bereich der Cybersicherheit.

Weitere Informationen finden Sie im vollständigen *BlackBerry Global Threat Intelligence Report – Juni 2024.*

*Früher bekannt als CylanceGUARD®.

BlackBerry Intelligent Security. Everywhere.

BlackBerry (NYSE: BB; TSX: BB) bietet intelligente Sicherheitssoftware und -dienste für Unternehmen und Regierungen weltweit. Zudem schützt es über 235 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.