BlackBerry | Cybersecurity

# GLOBAL THREAT INTELLIGENCE REPORT

UMSETZBARE THREAT INTELLIGENCE
ZUR ERFOLGREICHEN ABWEHR
VON CYBERANGRIFFEN

Berichtszeitraum: 1. September bis 30. November 2022

# INHALTE


**5 90 Tage in Zahlen**
Gesamtzahl der Angriffe
Geografische Verteilung der verhinderten Angriffe

**9 Beliebte Malware-Arten im Berichtszeitraum**
Windows
- Downloader
- Ransomware
- Infostealer
- Datei-Infektoren
- Remote Access Trojaner

macOS/OSX
- Ad- und Spyware
- Browser-Hijacker
- Proxy-Malware und -Agenten

Linux
- Bots und Botnetze
- Malware und Tools
- Kryptominer und Kryptojacking

Mobile Geräte
- Android
- iOS

**15 Branchenspezifische Angriffe**
Automotive
- Aktuelle Bedrohungstrends
  - Downloader
  - Infostealer
  - Ransomware
  - Dual-Use-Tools
- Bedrohungslandschaft in der Automobilindustrie
- Angriffe auf die Lieferkette
- Zukunftstrends

Gesundheitswesen
Finanzindustrie

**21 Aktivste Bedrohungsakteure**
TA505
ALPHV
APT32
APT29 (the Dukes)
Mustang Panda
TA542

**23 Gängige MITRE-Techniken**
Verhaltensbeispiele für gängige Techniken
MITRE D3FEND Abwehrmaßnahmen

**25 Bekannteste Angriffe**
DJVU: Seltsam vertraute Ransomware
Mustang Panda missbraucht legitime Apps, um Opfer in Myanmar anzugreifen
BianLian Ransomware verschlüsselt Dateien in einem Wimpernschlag
Unbekannter RomCom-Bedrohungsakteur fälscht beliebte Apps und greift jetzt das ukrainische Militär an
Bedrohungsakteur hinter RomCom nutzt beliebte Software-Marken, um der Ukraine und potenziell auch Großbritannien zu schaden
Ransomware ARCrypter breitet sich von Lateinamerika auf die ganze Welt aus
Mustang Panda nutzt den Ukrainekrieg für Angriffe auf Ziele in Europa und im asiatisch-pazifischen Raum

**28 Weitere Attacken**
Emotet
CryWiper

**29 Schlussfolgerungen und Vorschau für Q1 2023**
Lessons Learned/Erkenntnisse
Vorschau auf das 1. Quartal 2023

**30 Ressourcen**
Indicators of Compromise (IoCs)
Öffentliche Regeln
Gängige MITRE-Techniken
MITRE Defend Abwehrmaßnahmen

# EINFÜHRUNG

*THREAT INTELLIGENCE GILT ALS **„DIE KUNST, DEN GEGNER DURCH EINEN ÜBERRASCHUNGSCOUP ZU BEZWINGEN.“** DAS PRIMÄRZIEL VON ERFOLGREICHEN THREAT INTELLIGENCE PROGRAMMEN IST DIE GEDANKLICHE VORWEGNAHME, DIE MINIMIERUNG UND DIE VERHINDERUNG VON FOLGENSCHWEREN CYBERATTACKEN.*

Um dieses Ziel zu erreichen, ist ein proaktiver Ansatz gefragt. Ein Ansatz, der Ihnen Antworten auf folgende sicherheitskritische Fragen bietet: Welche Bedrohungsakteure sehen in Ihrem Unternehmen ein attraktives Ziel? Was treibt diese an und was führen sie im Schilde? Über welche Fähigkeiten verfügen sie? Wie verhalten sie sich und welche Cyberwaffen nutzen sie für ihre Angriffe? Doch am wichtigsten ist die Frage: Welche Abwehrmaßnahmen können Sie ergreifen, um die Cybersicherheit Ihres Unternehmens zu stärken?

Unser Team ist stolz auf die Veröffentlichung unseres ersten **BlackBerry Cybersecurity Global Threat Intelligence Reports.** Wir haben den Report erstellt und umsetzbare Informationen zusammengetragen, damit Sie sich vorbereiten können. Sie sollen im Ernstfall fundierte Entscheidungen treffen und unverzüglich Abwehrmaßnahmen einleiten können. Uns geht es darum, dass Sie gezielten Attacken, kriminellen Bedrohungsakteuren und Kampagnen gegen Ihr Unternehmen nicht hilflos ausgeliefert sind.

In dieser ersten Ausgabe finden Sie Berichte der besten Threat Researcher und Intelligence Analysten des BlackBerry Threat Research and Intelligence Teams. Spezialisten auf Weltklasse-Niveau, die sich nicht nur mit technischen Bedrohungen, sondern auch mit lokalen und geostrategischen Entwicklungen und ihren Auswirkungen auf Unternehmen auskennen. Dieser Report analysiert Cybervorfälle, die sich in den 90 Tagen zwischen dem 1. September und dem 30. November 2022 ereignet haben. Die Datengrundlage hierfür stammt von unseren eigenen KI-gesteuerten Lösungen und analytischen Fähigkeiten, die durch öffentlich zugängliche und private Informationsquellen ergänzt werden.

## Dies sind einige Highlights unseres Reports:

- **90 Tage in Zahlen.** Hier finden Sie eine statistische Auswertung für den Berichtszeitraum. Dazu gehören auch die Zahlen und die geopolitische Verteilung einmaliger Malware-Samples, die BlackBerry daran gehindert hat, die eigenen Kunden zu attackieren. Achtung Spoiler: Unsere Technologien stoppten durchschnittlich 62 neue Malware-Samples pro Stunde bzw. ungefähr einen neuen Sample pro Minute.
- **Die gängigsten Angriffswaffen.** Hier geht es um die Angriffsmethoden, die in diesem Zeitraum am häufigsten zum Einsatz kamen. Erfahren Sie mehr über das Wiederaufleben von schädlichen Loadern wie Emotet, die allgegenwärtige Präsenz des Trojaners Qakbot und die Zunahme von Downloadern wie GuLoader.

- **Remote-Zugriff fördert Infostealer.** Mit der pandemiebedingten Zunahme von Remote- und Hybrid-Arbeit wurde der sichere Remote-Zugriff zu einem erfolgskritischen Faktor. Denn die Angreifer haben schnell festgestellt, dass sie mithilfe von Infostealern leicht wertvolle Anmeldedaten stehlen und meistbietend verkaufen können. In diesem Report nehmen wir die Infostealer unter die Lupe, die wir in unserem Berichtszeitraum am häufigsten entdeckt haben.
- **Keine Plattform ist „sicher".** Hacker nutzen mehr als eine Strategie, um die verschiedensten Server, Desktops und mobilen Plattformen anzugreifen. Trotz vorherrschender Meinung ist beispielsweise macOS keine „sicherere" Plattform. Typische Malware für und Schwachstellen von macOS sind reichlich vorhanden. Darüber hinaus beleuchten wir die zunehmenden Angriffe auf Linux-Plattformen und die Verwendung seltener Programmiersprachen wie GoLang zur Entwicklung von plattformübergreifender Malware. Auch auf die aktuellen Bedrohungen für mobile Android- und iOS-Geräte gehen wir detailliert ein.
- **Branchensicht auf Bedrohungen.** Dank unserer starken Präsenz in der Cybersecurity und unserer IoT-Expertise für die industrielle Nutzung sind wir in der Lage, Bedrohungen für spezifische Branchen aufzudecken, die nur selten in anderen Reports diskutiert werden. Hier finden Sie Informationen zu Cybersecurity-Trends, mit denen die Autoindustrie sowie das Finanz- und Gesundheitswesen gleichermaßen zu kämpfen haben.
- **Abwehrmaßnahmen gegen Top-Bedrohungsakteure.** Unsere Telemetriedaten decken die Aktivitäten der verschiedensten Bedrohungsakteure und Netzwerke auf. Hier finden Sie nicht nur Informationen über einige der häufigsten Taktiken, Techniken und Verfahren (TTPs), sondern auch Links zu öffentlichen Listen der angewandten Abwehrmaßnahmen, die MITRE ATT&CK und MITRE D3FEND zugeordnet sind. Dadurch wollen wir es Ihnen erleichtern, Ihre Verteidigungsfähigkeiten und Ihre Bedrohungsmodelle, die auf umsetzbaren Informationen basieren, auf dem neuesten Stand zu halten.
- **Abschlussdiskussion und Ausblick.** Hier finden Sie ein Fazit unserer Erkenntnisse und eine Prognose für die Cyberbedrohungen in 2023.

Ich möchte den **Spitzenforschern unseres internationalen BlackBerry Threat Research und Intelligence Teams** herzlich danken. Sie haben diesen Report erst möglich gemacht. Ohne Unterlass produzieren sie unzählige topaktuelle Research-Berichte, verbessern zugleich die Datenlösungen von BlackBerry und die KI-gesteuerten Cylance Produkte und Services.

**Ismael Valenzuela**
Vice President, Threat Research & Intelligence bei BlackBerry
@aboutsecurity

## BLACKBERRY CYBERSECURITY THREAT INTELLIGENCE AUTOREN

**Dmitry Bestuzhev**

**Pedro Drimel**

**Jacob Faires**

**Dean Given**

**Eoin Healy**

**Geoff O'Rourke**

**Jose Luis Sanchez**

*Die Daten, die dieser Report verwendet, stammen von der BlackBerry Cybersecurity-Telemetrie und sind Eigentum von BlackBerry Limited.*

# 90 TAGE IN ZAHLEN

## GESAMTZAHL DER ANGRIFFE

In den 90 Tagen zwischen dem 1. September und dem 30. November 2022 stoppte die Cylance® Endpoint Security Lösung von BlackBerry 1.757.248 Malware-basierte Cyberattacken. Bedrohungsakteure setzten durchschnittlich 19.524 böswillige Samples pro Tag gegen unsere Kunden ein. Unter diesen Bedrohungen fanden sich 133.695 einmalige Malware-Samples, die sich durchschnittlich in 1.485 neuartige Malware-Samples pro Tag und 62 Samples pro Stunde wandelten. Damit reden wir im Schnitt von einem neuen Sample pro Minute.

Die folgende Grafik zeigt das Auftreten von potenziellen Cyberattacken, die unsere Cylance Endpoint Security Lösung zwischen dem 1. September und dem 30. November 2022 verhindert hat. Die Spitzen nach der 4. Woche (29.09.–07.10.22) und nach der 7. Woche (20.10.–26.10.22) lassen sich darauf zurückführen, dass Bedrohungsakteure ihre Malware-Samples erneut eingesetzt haben.

### DYNAMIK DER VERHINDERTEN ATTACKEN

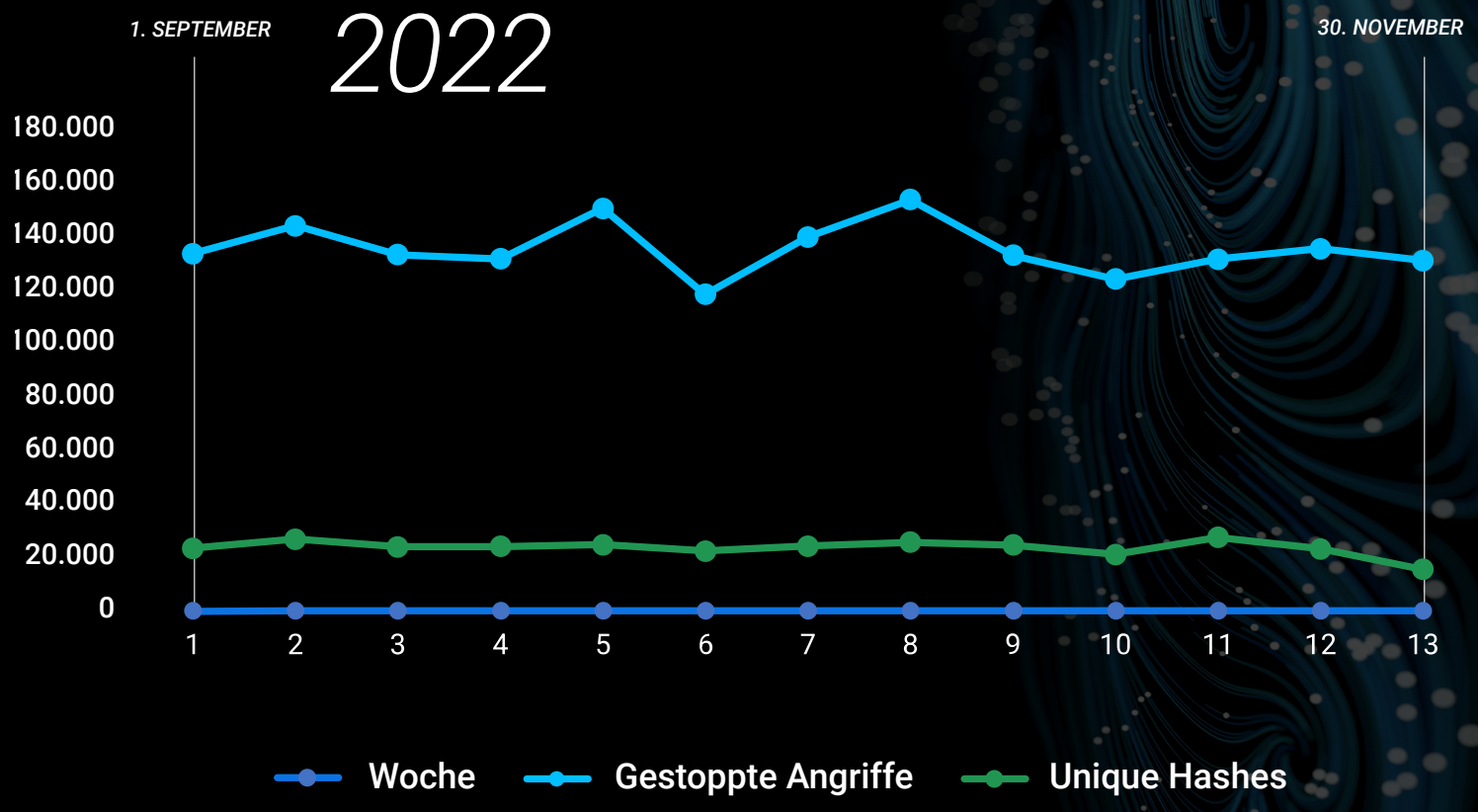
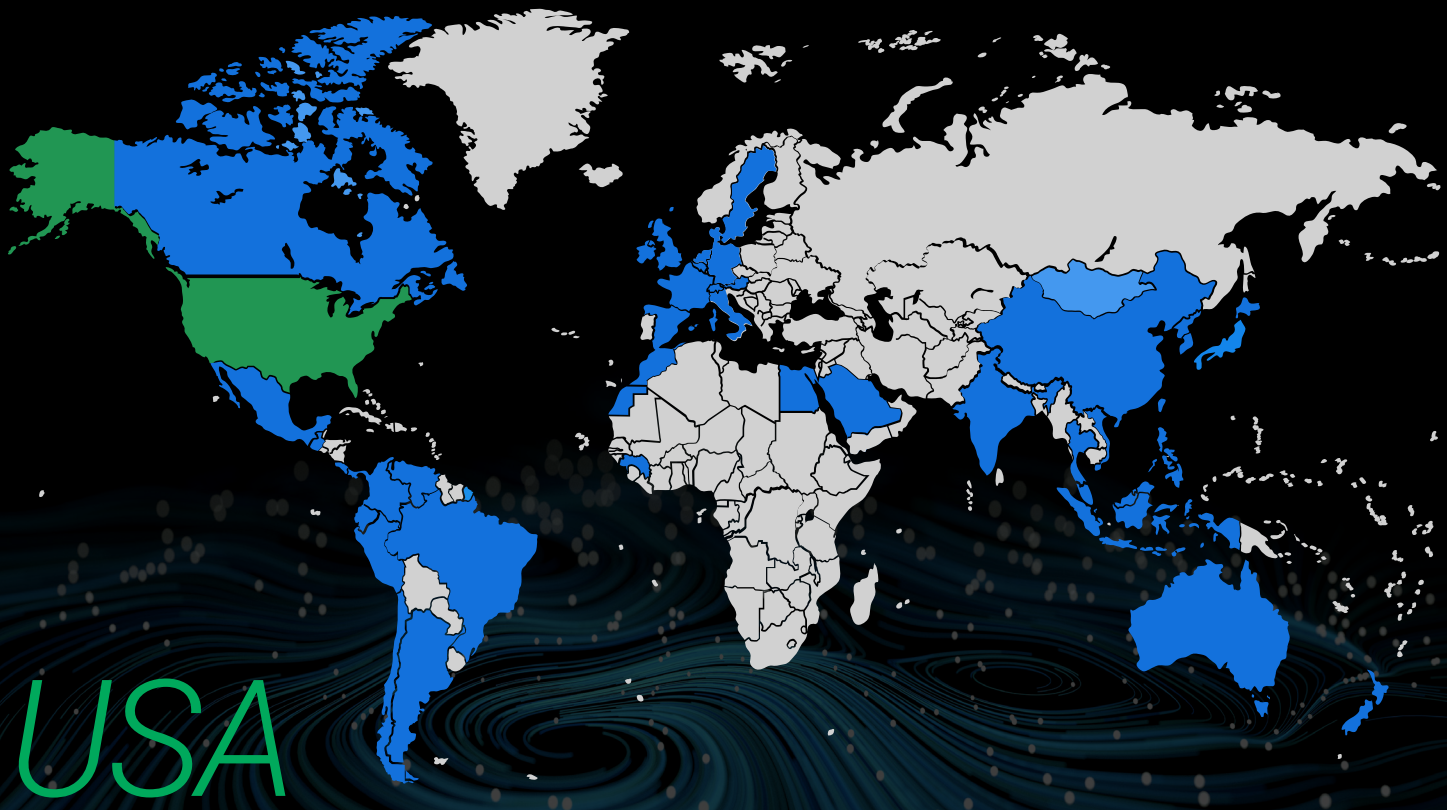



*Abb. 1: Cyberattacken, die BlackBerry zwischen dem 1. September und dem 30. November 2022 verhindert hat.*

## GEOGRAFISCHE VERTEILUNG DER VERHINDERTEN ANGRIFFE

Ganz allgemein kann man sagen, dass Länder mit einer hohen Internetnutzung, großen Wirtschaftskraft und Bevölkerungsdichte den meisten Angriffen ausgesetzt sind. Unsere Telemetrie zeigt, dass die Angreifer im Berichtszeitraum BlackBerry Kunden auf der ganzen Welt angegriffen haben.

***LÄNDER, IN DENEN BLACKBERRY SEINE KUNDEN VOR CYBERANGRIFFEN GESCHÜTZT HAT***



# USA

***WAR DAS LAND, IN DEM DIE MEISTEN CYBERATTACKEN GESTOPPT WURDEN. INSGESAMT MEHR ALS EINE MILLIONEN ANGRIFFE.***

*Abb. 2: Länder, in denen BlackBerry seine Kunden vor Cyberattacken geschützt hat. Je dunkler die Blaufärbung ist, desto höher die Anzahl der verhinderten Cyberattacken. Länder ohne Färbung weisen keine statistisch signifikante Anzahl an BlackBerry Kunden auf.*

*ABB. 3 ZEIGT DIE TOP TEN DER LÄNDER MIT DER HÖCHSTEN ANZAHL AN CYBERANGRIFFEN, DIE DURCH DIE CYLANCE ENDPOINT SECURITY LÖSUNGEN VERHINDERT WURDEN.*

## TOP 10 DER LÄNDER, DIE IM 4. QUARTAL AM HÄUFIGSTEN CYBERANGRIFFEN AUSGESETZT WAREN

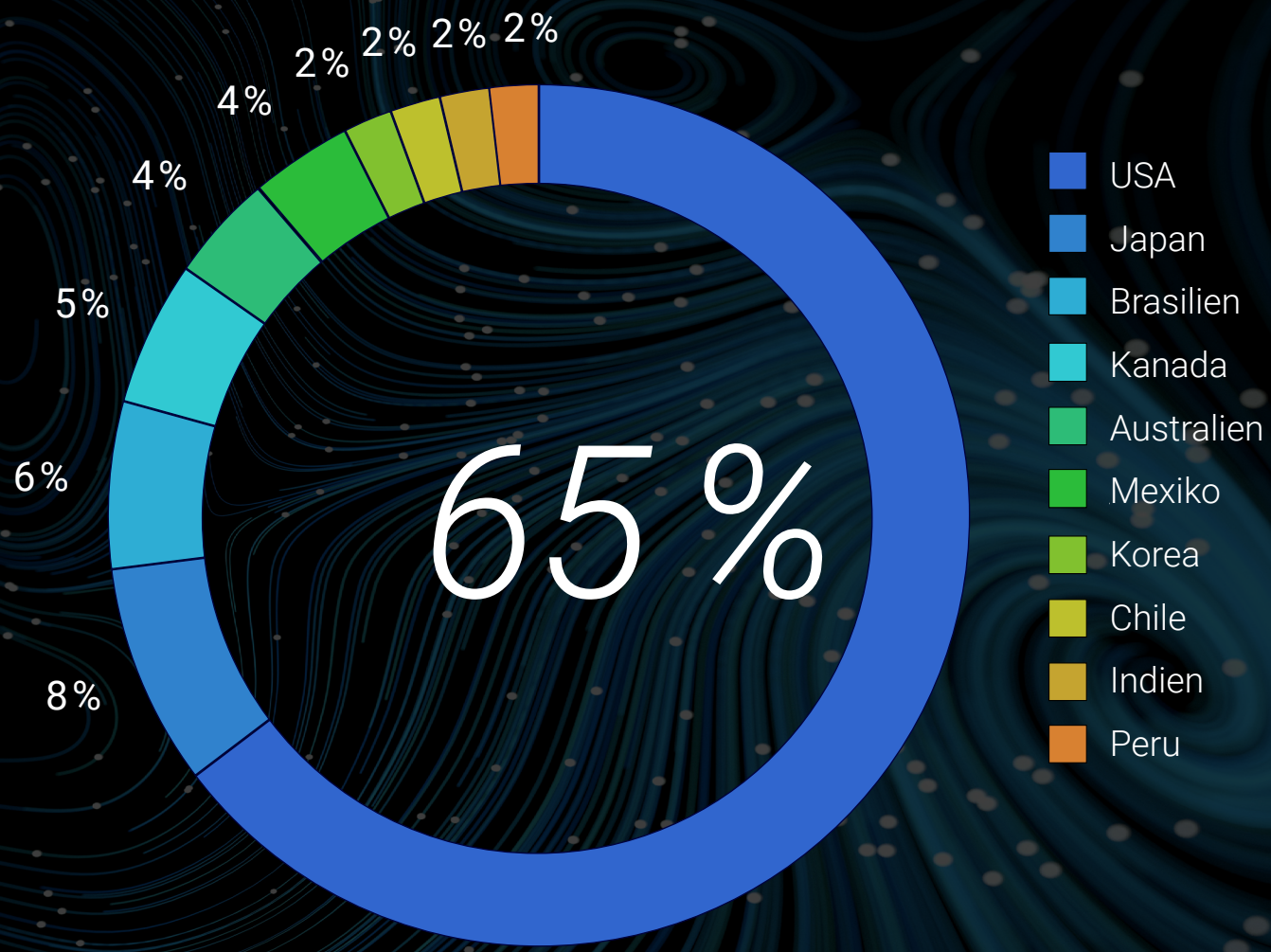



*Abb. 3: Top 10 der Länder, in denen BlackBerry Kunden Ziel von Cyberangriffen waren.*

*ABB. 4 ZEIGT LÄNDER, IN DENEN BLACKBERRY KUNDEN AM **HÄUFIGSTEN** UND WIEDERHOLT MIT EINMALIGEN SCHÄDLICHEN SAMPLES ANGEGRIFFEN WURDEN.*

### *TOP 10 DER LÄNDER, IN DENEN EINMALIGE MALWARE-SAMPLES EINGESETZT WURDEN*

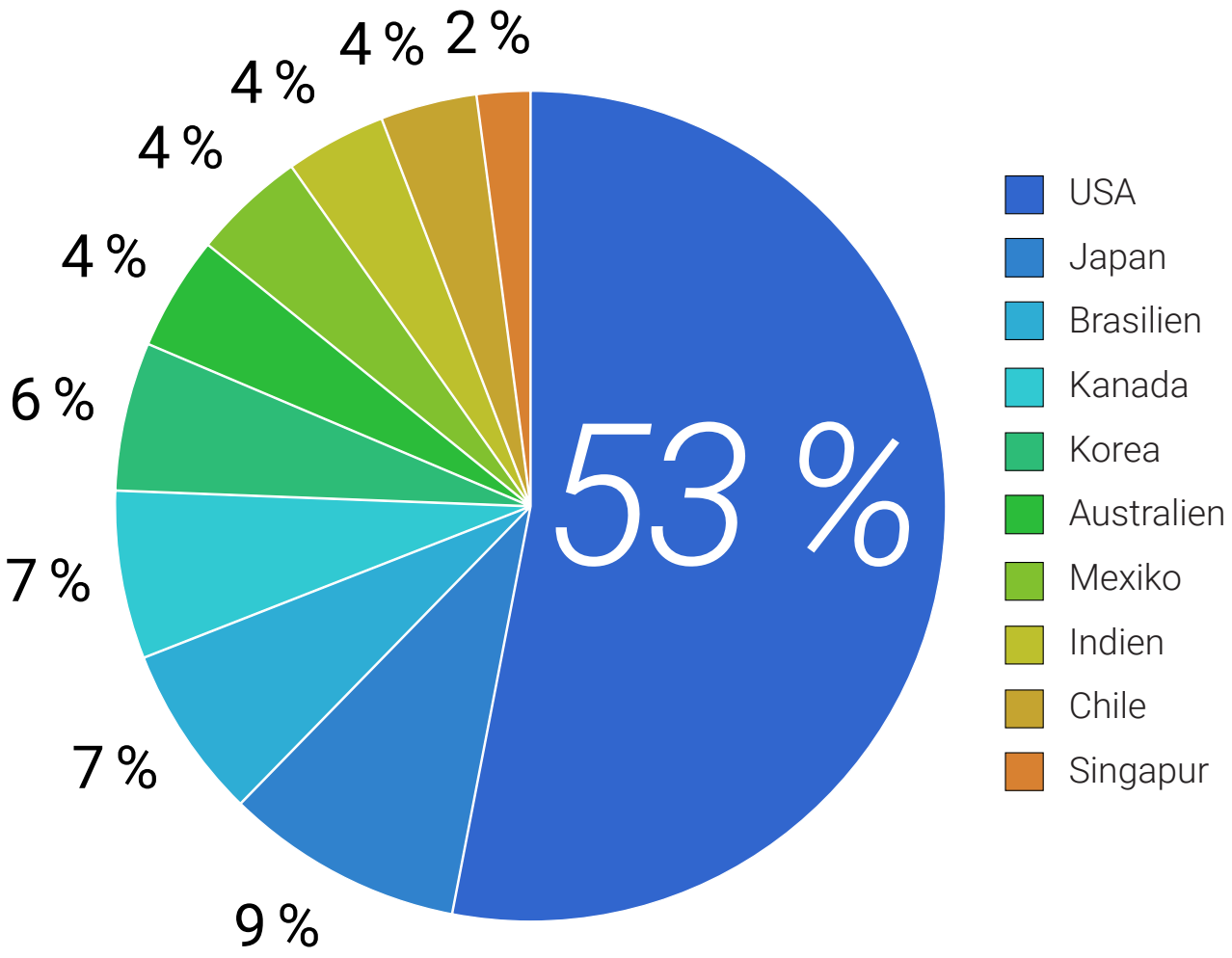



*Abb. 4: Top 10 der Länder, in denen einmalige Malware-Samples gegen BlackBerry Kunden eingesetzt wurden.*

# BELIEBTE MALWARE

## IM BERICHTSZEITRAUM

**Zwischen dem 1. September und dem 30. November 2022 nutzten Bedrohungsakteure eine Vielzahl an Malware-Arten, um ihre finanziellen, geopolitischen, militärischen und taktischen Ziele zu erreichen. Die häufigsten und interessantesten Malware-Familien finden Sie auf den folgenden Seiten nach Betriebssystemen aufgeschlüsselt.**

Bemerkenswert ist, dass Windows® zwar das Betriebssystem ist, das am häufigsten angegriffen wird, allerdings sind seine Anwender besser auf Malware-Angriffe vorbereitet als Nutzer anderer Betriebssysteme, die sich häufig für immun gegenüber Cyberangriffen halten. Die BlackBerry® Telemetriedaten zeigen eindeutig, dass Nutzer von macOS®, Linux®und Mobilgeräten genauso häufig attackiert werden. Keine Plattform ist immun gegen Angriffe.

### *WINDOWS*

Malware kann auf jedem Betriebssystem laufen, allerdings bleibt Microsoft® Windows® der Spitzenreiter bei den Attacken. Die Gründe hierfür sind vielfältig. Zum einen liegt es an der Beliebtheit des Betriebssystems und der großen Bandbreite an Dokumentationen für Entwickler. Und zum anderen kann die Community der Cyberkriminellen auf eine lange Tradition geballter Erfahrungen zurückblicken, da sie Tripps und Tricks regelmäßig in Foren miteinander teilen.

### *Downloader*

Downloader verführen ihre Opfer dazu, Dateien zu öffnen, die Malware herunterladen können. Diese Dateien präsentieren sich wie legitime digitale Dokumente oder vertrauenswürdige ausführbare Dateien. Die bekanntesten Downloader sind:

- Emotet ist eine der produktivsten Bedrohungen, die derzeit im Umlauf sind. Seit 2014 trieb die Schadsoftware weltweit ihr Unwesen, bis sie im April 2021 durch eine koordinierte, multinationale Aktion der Strafverfolgungsbehörden gestoppt wurde. Ende 2021 tauchte Emotet wieder aus der Versenkung auf. Im vergangenen Quartal wurde Emotet, nach einer 4-monatigen Pause, mit bereits bekannten Techniken wiederbelebt. Dazu gehörten auch Phishing-Kampagnen, die kompromittierte Microsoft® Office-Dokumente verteilen. Diese Dokumente versuchen ihre Opfer davon zu überzeugen, sie in das Microsoft Active Directory zu kopieren, wo Makros automatisch ausgeführt werden. Und zwar ohne den Anwender zuvor um Erlaubnis zu fragen. Emotet war lange bekannt dafür, den Banking-Trojaner IcedID zu platzieren, der eng mit verschiedenen Ransomware-Gruppen verbunden ist.
- Qakbot verbreitet sich durch Phishing-Techniken via Köder-E-Mails. Typisch für diese E-Mails ist ein LNK-Hyperlink, der zu einer schädlichen Webseite führt, die eine passwortgeschützte ZIP-Datei bereithält, die ein ISO-Image beinhaltet. Die LNK-Datei führt eine JavaScript-Datei aus, die wiederum eine bösartige Qakbot-DLL mit einer .DAT-Erweiterung ausführt. Eine bemerkenswerte Funktion von Qakbot ist, dass es existierende E-Mail-Verläufe zur Verbreitung nutzt. Durch seine Fähigkeiten vorhandene E-Mails zu beantworten, können Empfänger leicht getäuscht werden, da sie annehmen, dass eine vertrauenswürdige Quelle ihnen einen Link oder einen Anhang geschickt hat. Qakbot wird regelmäßig von den verschiedensten Ransomware-Gruppen eingesetzt. In diesem Quartal wird es vor allem mit Black Basta, einem möglichen Conti Rebranding in Verbindung gebracht. Diese Gruppe zielte 2022 vor allem auf Unternehmen mit Sitz in den USA.

- GuLoader kann ausführbare Dateien herunterladen und remote implementieren. Es wird häufig zum Download und zur Ausführung von Infostealern wie RedLine und Raccoon eingesetzt. GuLoader zweckentfremdet sehr gern cloudbasierte Dienste wie Google Cloud™ und OneDrive®, um seine Nutzlasten zu hosten. Allerdings nutzt es auch Telegram-Bots für seine Zwecke aus.

## *Ransomware*

LockBit war der aktivste und erfolgreichste Ransomware-as-a-Service (RaaS), der 2022 zum Einsatz kam. Im Berichtszeitraum zeigten sich keine Anzeichen für ein Nachlassen oder eine Verlangsamung der Aktivitäten dieser Gruppe. Im Gegenteil. LockBit gibt es mittlerweile in der Version 3.0, die verschiedene Anti-Debugging-Techniken einsetzt, was die Analyse von String-Verschlüsselungen und anderen Techniken, die an die frühere BlackMatter Ransomware anknüpfen, erheblich erschwert.

## *Infostealer*

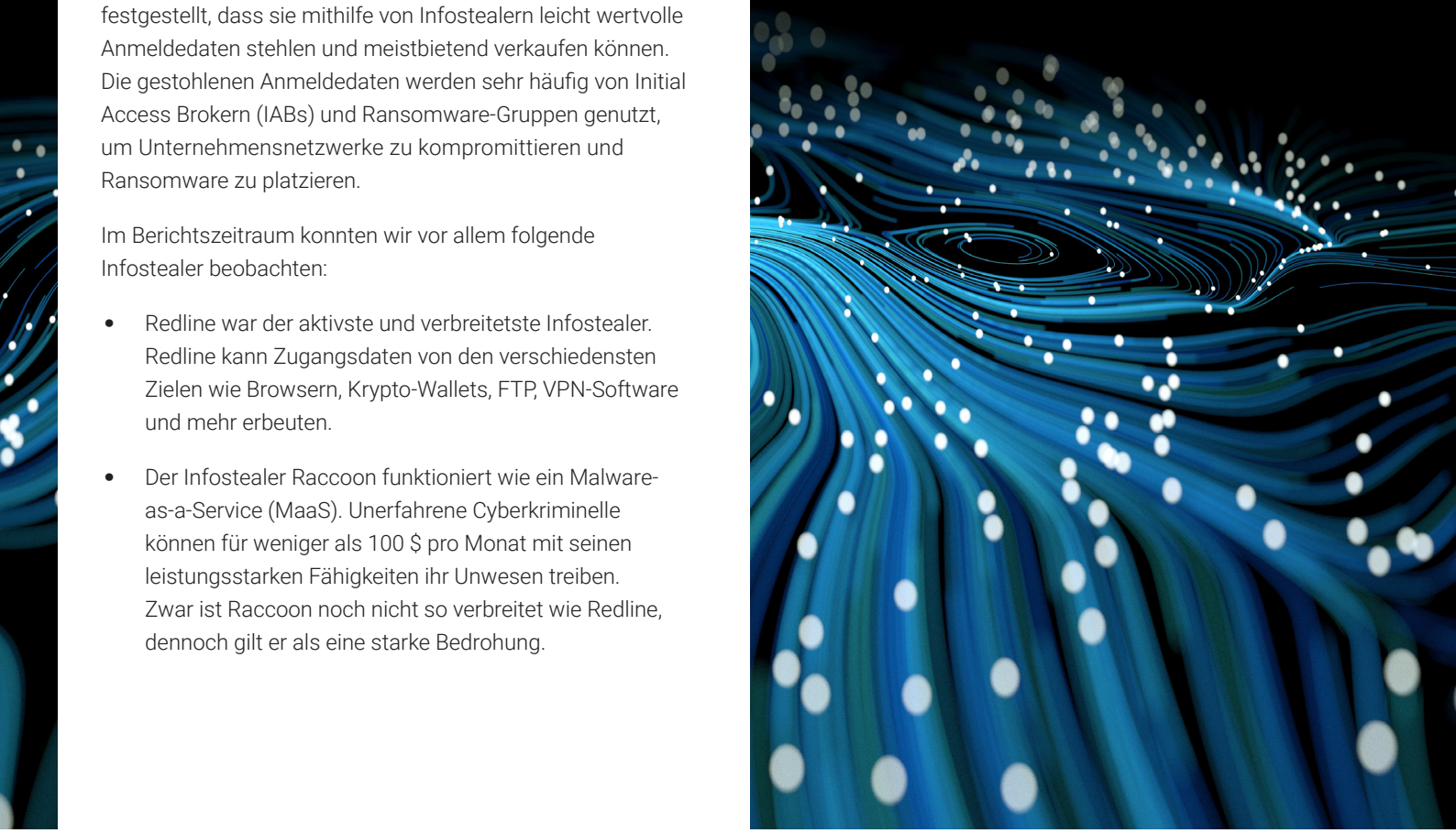
Mit der pandemiebedingten Zunahme von Remote- und Hybrid-Arbeit wurde der sichere Remote-Zugriff zu einem erfolgskritischen Faktor. Denn die Angreifer haben schnell festgestellt, dass sie mithilfe von Infostealern leicht wertvolle Anmeldedaten stehlen und meistbietend verkaufen können. Die gestohlenen Anmeldedaten werden sehr häufig von Initial Access Brokern (IABs) und Ransomware-Gruppen genutzt, um Unternehmensnetzwerke zu kompromittieren und Ransomware zu platzieren.

Im Berichtszeitraum konnten wir vor allem folgende Infostealer beobachten:

- Redline war der aktivste und verbreitetste Infostealer. Redline kann Zugangsdaten von den verschiedensten Zielen wie Browsern, Krypto-Wallets, FTP, VPN-Software und mehr erbeuten.
- Der Infostealer Raccoon funktioniert wie ein Malware-as-a-Service (MaaS). Unerfahrene Cyberkriminelle können für weniger als 100 $ pro Monat mit seinen leistungsstarken Fähigkeiten ihr Unwesen treiben. Zwar ist Raccoon noch nicht so verbreitet wie Redline, dennoch gilt er als eine starke Bedrohung.

# REDLINE

***KANN ANMELDEDATEN VON MEHREREN ZIELEN STEHLEN, EINSCHLIESSLICH BROWSERN, KRYPTO-WALLETS, FTPS, VIRTUAL PRIVATE NETWORKS (VPN) SOFTWARE UND VIELEN MEHR.***



BlackBerry hat sogar Fälle entdeckt, bei denen Raccoon infolge einer Redline-Infektion eingeschleust wurde. Raccoon kann Zugangsdaten von Krypto-Wallets, Browser-Erweiterungen, Discord- und Telegram-Konten stehlen. Es kann Screenshots erstellen und wie ein Loader schädliche Nutzlasten platzieren.

Im September 2022 haben Bedrohungsakteure versucht Uber[1] zu kompromittieren. Der Angriff wurde offiziell Angehörigen der Lapsus$-Gruppe zugeschriebenen. Dank des schnellen Handelns des Unternehmens und der erfolgreichen Abwehr der Attacke kam die Ransomware nicht zum Zuge.

## Datei-Infektoren

Datei-Infektoren infizieren andere ausführbare Dateien und werden durch Netzwerkfreigaben und Wechseldatenträger verbreitet. Der Datei-Infektor Neshta wurde erstmals 2003 identifiziert und wird auch noch heute – Jahrzehnte später – eingesetzt. Neshta wurde früher mit BlackPOS in Verbindung gebracht, einer Point-of-Sale (POS)-Malware, die Kreditkartendaten aus POS-Systemen abgesaugt hat. Besonders häufig kam Neshta 2018 bei Angriffen gegen Unternehmen der Konsumgüter-, Energie-, Finanz- und Fertigungsindustrie zum Einsatz. In einem detaillierten Bericht über Neshta sind wir 2019 der Sache nachgegangen und beobachten seither jedes Jahr ähnliche Vorgänge.

***BLACKBERRY RESEARCHER STELLTEN FEST, DASS GANZE***

# 34 %

***DER KUNDEN, DIE MACOS NUTZEN, DOCK2MASTER IN IHREM NETZWERK HATTEN, WO ES BEI 26 % DER GERÄTE GEFUNDEN WURDE.***

## Remote Access Trojaner

Remote Access Trojaner (RATs) können Tastenanschläge protokollieren, Webcams steuern, Anmeldedaten für Browser stehlen und Angreifern die administrative Kontrolle über infizierte Geräte und andere Geräte in einem Netzwerk bieten. Die folgenden RATs konnten wir im Berichtszeitraum identifizieren:

- njRAT wurde erstmals 2015 entdeckt und gehört immer noch zu den gängigsten RATs. Er wird vor allem durch finanziell motivierte Bedrohungsakteure verbreitet. Allerdings kam er auch bei sehr gezielten Attacken zum Einsatz. Da der Builder von njRAT sehr weit verbreitet ist, können ihn Bedrohungsakteure sehr leicht an ihr bevorzugtes Angriffsmodell anpassen. Besonders beliebt ist er bei Angreifern aus dem Nahen Osten. Unsere proprietäre Telemetrie hat eine Instanz von njRAT mit einem Command-and-Control-Server (C2) identifiziert, der in Jordanien gehostet wird.
- FlawedAmmyy tauchte erstmals 2018 auf. Er basiert auf durchgesickertem Quellcode für das robuste Remote Access Tool Ammyy Admin. Das offizielle Tool wird sowohl von Unternehmen als auch von Privatpersonen zur Fernsteuerung und Diagnose von Microsoft Windows Maschinen genutzt. FlawedAmmyy wurde anfänglich vor allem der kriminellen TA505-Gruppe zugeordnet, die bekannt für ihre Angriffe mit der Ransomware Cl0p ist. Doch mittlerweile wird er von den verschiedensten kriminellen Bedrohungsakteuren benutzt.

## MACOS/OSX

Zwar gehört macOS nicht zu den am meisten genutzten Unternehmensplattformen, allerdings ist es auf einer wachsenden Anzahl von Unternehmenssystemen installiert[2]. Es hat den Ruf sicherer als Windows zu sein, dennoch gibt es macOS-spezifische Malware und Schwachstellen.

## Ad- und Spyware

Adware und Spyware sind weitverbreitete Bedrohungen für macOS. Sie tarnen sich als legitime Software, um die Anwender auszunutzen. Anders als Bedrohungen, die durch gezielte Infektionskampagnen eingeschleust werden, installieren Anwender oftmals die Ad- und Spyware im guten Glauben selbst.

Da sie annehmen, dass es sich um legitime Anwendungen handelt und sie sich der Gefahren durch die oftmals kostenlose Software nicht bewusst sind. Während des 90-tägigen Berichtszeitraums war die bösartige Applikation Dock2Master die häufigste Bedrohung für macOS: Die Researcher von BlackBerry haben festgestellt, dass ganze 34 Prozent der Kunden, die macOS nutzen, Dock2Master in ihrem Netzwerk hatten, wo es bei 26 Prozent der Geräte gefunden wurde. Offiziell gilt Dock2Master als potenziell unerwünschte Applikation (PUA), da es heimlich Werbung in Webseiten einbaut, um sensible Daten über den Besucher und sein System abzufischen und auf dem Schwarzmarkt zu verkaufen.

## *Browser-Hijacker*

Browser-Hijacking führt zu veränderten Suchergebnissen und manipulierten Browser-Einstellungen. Diese Masche ist zwar nicht mehr so allgegenwärtig wie in den frühen 2000er-Jahren, aber immer noch weit verbreitet. Der häufigste Effekt von Browser-Hijacking besteht darin, dass die Standard-Suchmaschine ohne Einwilligung des Users geändert wird. Um aus dem Hijacking Kapital zu schlagen, verkaufen die Cyberkriminellen die sensiblen Informationen zur Benutzeridentität, die im Browser gespeichert sind und über die infizierte Werbung auf den angezeigten Webseiten ermittelt wurden. In diesem Quartal kamen beim Browser-Hijacking auch OriginalModule und SearchInstaller zum Einsatz, die InstallCore nutzen, um Multi-Plattformen anzugreifen.

## *Proxy-Malware und -Agenten*

Proxy-Malware ist eine Trojaner-Art, die infizierte Systeme in einen Proxy-Server verwandeln kann. Dies erlaubt einem Angreifer, unter falschem Namen Aktionen auszuführen und seine wahre Identität zu verschleiern. Proxy-Agenten sind Proxy-Malware, die über ähnliche Fähigkeiten wie RATs verfügen, wie beispielsweise das Ausführen lokaler Befehle auf infizierten Maschinen. Proxy-Malware neigt dazu, weniger Funktionen zu unterstützen als andere Malware-Arten. Dadurch ist sie in der Lage, den Kreis möglicher Opfer auszuweiten, da viel weniger Bibliotheken benötigt werden. Die Programmiersprache GoLang ist in dieser Malware-Klasse sehr gebräuchlich, da sie Support für Proxy-Bibliotheken wie Proxit bietet und so auch unerfahrenen Cyberkriminellen die Entwicklung erleichtert.

BlackBerry hat festgestellt, dass die zunehmende Verwendung von GoLang bei Angriffen auf macOS-Systeme zum Tragen kommt. Und zwar als Bestandteil einer groß angelegten Attacke gegen Multi-Plattformen für rücksichtslose Angriffe mit Malspam. Um diese Multi-Plattformen effektiv auszunutzen, verwenden die Angreifer einfache Funktionen, die auch plattformübergreifend funktionieren. Die meisten Proxy-Agenten, die beobachtet wurden, attackieren Browser, die für diese Multi-Plattformen verfügbar sind.

## *LINUX*

Linux ist ein leistungsstarkes, flexibles Betriebssystem, das mit Open-Source-Software läuft und allgegenwärtig ist: Bis zu 90 Prozent der Public-Cloud-Dienste laufen auf Linux[3]. Daher verwundert es nicht, dass Linux zu einem attraktiven Ziel für Cyberkriminelle geworden ist, die darauf aus sind, Schwachstellen schnell als Waffe einzusetzen und auszunutzen, die von Anbietern und anderen Branchenakteuren bekannt gemacht werden.

## *Bots und Botnetze*

Ein Bot ist ein automatisiertes Programm, dass Kommandos ohne menschliche Intervention ausführen kann. Und von Botnetzen spricht man, wenn eine Gruppe von Bots durch einen einzigen Bedrohungsakteur kontrolliert wird. Botnetze werden gerne genutzt, um Fehlkonfigurationen oder ungepatchte Schwachstellen auszunutzen, um die Rechner der Opfer mithilfe von bösartigem Code dem Botnetz hinzuzufügen. Seit dem Auftreten des berühmt-berüchtigten Mirai Botnetzwerks, das 2016 zu einer groß angelegten Denial-of-Service (DDoS)-Attacke führte, kommen immer mehr Linux-Botnetze zum Vorschein.

Bekannte Internet Relay Chat (IRC) Botnetze wie ShellBot existierten auch noch Ende 2022. Sie nutzten Brute-Force-Taktiken, um über fehlkonfigurierte oder Standard-Anmeldedaten[4] in Systeme einzudringen. Außerdem haben wir gesehen, wie das Sysrv-Botnetz Schwachstellen bei der Remote-Code-Ausführung (RCE)[5] via CVE-2022-22947[6] ausgenutzt hat, um Systeme zu kompromittieren und sein Botnetz in großem Umfang auszubauen.

## *Malware und Tools*

BlackBerry hat in diesem Berichtszeitraum noch weitere Malware und bösartige Tools beobachtet und identifiziert. SSH-Tools (basierend auf dem Secure-Shell-Protokoll, das den Fernzugriff ermöglicht) werden häufig in Verbindung mit bösartigem Code eingesetzt, um Anmeldedaten zu erzwingen und/oder Netzwerke auf Ausbreitungsmöglichkeiten zu scannen.

Während des 90-tägigen Berichtszeitraums wurde das Tool Faster than Lite (FTL) verstärkt eingesetzt. Dieses Tool wird häufig von der Bedrohungsgruppe OutLaw[7] ausgenutzt und wurde mit ShellBot gebündelt.

Unsere Telemetrie ergab ähnliche Kampagnen, bei denen das GoLang-basierte SSH-Brute-Force-Tool Spirit eingesetzt wurde, das ebenfalls als Verbreitungswerkzeug genutzt wird. Spirit wird in der Regel zusammen mit den IRC-Bots Pwnrig und Tsunami eingesetzt, die wir mit ziemlich hoher Wahrscheinlichkeit der Hackergruppe 8220 Gang zuordnen können.

Die inzwischen berühmte Log4j-Schwachstelle wurde im Berichtszeitraum regelmäßig von verschiedenen Malware-Familien und Bedrohungsakteuren ausgenutzt. Der Kinsing-Trojaner beispielsweise nutzte die Java Log4j-Paketschwachstelle[8] CVE-2021-44228[9] für RCE auf Linux-Plattformen aus und wurde in jüngster Zeit bei der Ausnutzung der Oracle WebLogic Server-Schwachstelle[10] CVE-2020-14882[11] beobachtet. Dieser Trojaner versucht, die Sicherheits- und Cloud-Service-Agenten eines Geräts zu deaktivieren und jegliche konkurrierende Malware und Kryptowährungsminer (Kryptominer) auf dem System der Opfer zu zerstören, bevor er seinen eigenen Kryptominer einsetzt.

## *Kryptominer und Kryptojacking*

Beim Kryptojacking nutzen Bedrohungsakteure die Rechenleistung ihrer Opfer aus, um mithilfe von Kryptomining-Software wertvolle Kryptowährung zu schürfen. Und zwar ohne das Wissen des eigentlichen Besitzers. Kryptominer sind eine permanente Plage in der Bedrohungslandschaft seit fast einem Jahrzehnt. Sie können alle großen Computersysteme befallen und lange im Hintergrund agieren, bevor sie entdeckt werden.

Im Berichtszeitraum hat die Kryptowährung zwar allgemein an Wert verloren, dennoch ist das Kryptomining für Kriminelle immer noch ein lohnendes Unterfangen. Auch wenn sich der Markt ändert, halten viele der auf Linux spezialisierten Bedrohungsakteure an der Kryptowährung fest.

In diesem Quartal machten Linux-Geräte einen signifikanten Anteil beim Kryptomining aus. Denn Kryptomining wird immer ressourcenintensiver und kostspieliger. Aus diesem Grund haben die Angreifer damit begonnen, die Umgebung der verschiedensten Opfer zu kompromittieren, um Miner zu platzieren und fremde Computerressourcen auszunutzen. Insbesondere der zuvor genannte ShellBot und der Sysrv-Bot kamen hierbei zum Einsatz.

***IM BERICHTSQUARTAL MACHTEN KRYPTOMINER EINEN ERHEBLICHEN ANTEIL DER***

# *BEDROHUNGEN*

***AUF LINUX-GERÄTEN AUS.***


Typischerweise gelangen Kryptominer erst nach einer Kompromittierung in die Umgebung eines Opfers. Dies gelingt ihnen meist mithilfe einer Nutzlast oder einer Schwachstelle wie CVE-2022-26134[12] (Atlassian Confluence) oder CVE-2019-2725[13] (WebLogic), wie es häufig beim PwnRig Kryptominer vorkommt[14]. Kryptominer versuchen, sich in Standard-Hintergrundressourcen wie Cronjobs, die Routineaufgaben zur Wiederholung zu bestimmten Zeiten planen, einzunisten und möglichst lange unentdeckt zu bleiben.

Das Berichtsquartal enthüllte auch einen Zusammenhang mit CryptoNight, einem Mining-Algorithmus, der verwendet wird, um Netzwerke zu sichern und Transaktionen in einigen Kryptowährungen wie Monero und Webchain zu validieren. Zudem zeigte sich ein Anstieg bei der Verwendung des Webchain-Miners sowie mehrerer XMRig-basierter Miner. XMRig ist ein beliebtes Open-Source-Programm, das häufig zum Mining von Kryptowährungen wie Bitcoin und Monero verwendet wird. Insbesondere bei Bedrohungsakteuren steht Coin-Miner hoch im Kurs und wird sehr häufig eingesetzt.

## MOBILE GERÄTE

Mobile Geräte lösen Laptops und Desktop-Computer in vielen Bereichen immer mehr ab: Insbesondere beim Online-Banking, bei mobilen Zahlungen, Messaging-Apps und sozialen Netzwerken. 2022 wurden bereits 59,54 Prozent des gesamten Internettraffics über mobile Geräte abgewickelt[15].

### Android

2022 nutzten weltweit fast 71 Prozent der mobilen Geräte Android™ als Betriebssystem. Im Berichtszeitraum konnten wir folgende Bedrohungen entdecken:

- Lotoor ist ein Tool, das sowohl für harmlose als auch für bösartige Zwecke verwendet werden kann. Android-Besitzer können mit Lotoor ihre Geräte rooten und ergänzende Funktionen freischalten. Das Tool kann aber auch eingebettete Sicherheitsfunktionen von Google umgehen und persistente Malware implantieren.
- AdvLibrary infiziert Geräte, um aus Traffic Einnahmen zu generieren. Es zeigt unerwünschte Werbung an und erzeugt ausgehenden Traffic über bezahlte Anzeigen. Den Opfern entsteht in der Regel zwar kein direkter finanzieller Schaden, allerdings kann der erhöhte Datenverkehr zusätzliche Kosten mit sich bringen. Mit AdvLibrary können Cyberkriminelle durch Klicks auf Werbung und Datenverkehr zu böswillig beworbenen Websites Kapital schlagen.

### iOS

iOS® hat den Ruf sicherer als andere mobile Betriebssysteme zu sein. Immerhin sind Zero-Day-iOS-Exploits teuer und werden daher nur selten für unkontrollierte Angriffe verwendet. Allerdings ist iOS nicht immun gegen Exploits, die bei iPhone®-Geräten einen Jailbreak bewirken können. Dieses „Entsperren" ist eine potenziell gefährliche Aktivität, da sie die originalen Apple®-Sicherheitsfunktionen entfernt und vollständigen Zugriff auf die Geräte gewährt. Es gibt zwar Besitzer, die einen Jailbreak bei ihren iPhones absichtlich herbeiführen, um beispielsweise unerwünschte Standardanwendungen zu entfernen, allerdings nehmen sie dadurch das Risiko in Kauf, anfällig für Angriffe zu sein.

Nicht nur erfahrene Bedrohungsakteure nutzen iPhone-Jailbreaks, um Malware auf den Geräten der Opfer zu installieren. Eine dieser bösartigen Malware-Familien, die iOS-User ins Visier nehmen, ist Vortex. Sie ist das Pendant zum Android-Rooter Looter und kann iPhones entsperren. Eine Sache, die Cyberkriminellen bei der Installation von Malware entgegenkommt. Diese Technik ist vor allem bei Angreifern verbreitet, die zwar schon etwas Erfahrung haben, aber technisch nicht in der Lage sind, Zero-Day-Bedrohungen zu starten. Im letzten Quartal wurden von BlackBerry bereits zwei verschiedene Vortex-Versionen entdeckt, die iOS-Geräte entsperren können.

# BRANCHENSPEZIFISCHE ANGRIFFE

**Auch wenn alle Branchen anfällig für Cyberangriffe sind, gibt es einige, die einzigartige Möglichkeiten für Cyberkriminelle bereithalten. Dies betrifft insbesondere die Automobilindustrie, das Gesundheitswesen und die Finanzbranche.**

## AUTOMOTIVE

Die Automobilindustrie findet sich – nicht zum ersten Mal – mitten in einer gewaltigen technologischen Revolution wieder. Bahnbrechende technologische Fortschritte ermöglichen die Entwicklung von neuen Fahrzeugtypen, Systemen und Dienstleistungen. Die digitale Transformation bietet hier enorm viele Ansatzmöglichkeiten, allerdings bringt sie auch neue Herausforderungen für die Cybersicherheit mit sich.

Je vernetzter und autonomer die Fahrzeuge werden, desto anfälliger werden sie für Cyberbedrohungen und desto attraktiver sind sie für Angreifer. Die Gefahr beginnt bereits bei den Fertigungssystemen, die immer komplexere Herausforderungen meistern müssen.

In den letzten Jahren war die Automobilindustrie nur selten von groß angelegten und öffentlichkeitswirksamen Bedrohungen betroffen. Die Angreifer konzentrieren sich mittlerweile nicht mehr nur auf die Automobilhersteller, sondern nehmen gleich die gesamte Branche ins Visier. Sie versuchen, die Betriebsabläufe zu stören, sensible Daten zu stehlen und die Lieferketten zu unterbrechen. 2022 konnten wir viel mehr bösartige Akteure beobachten, die es auf die Automobilindustrie abgesehen hatten. Auch die von ihnen verursachten Störungen haben signifikant zugenommen.

Um sich vor solchen Bedrohungen zu schützen, muss die Automobilindustrie zunächst einmal die Risiken kennen, die mit einer starken Vernetzung der Fahrzeuge einhergehen. Erst dann kann sie robuste Cybermaßnahmen zum Schutz der Fahrzeuge und Fahrer implementieren.

### Aktuelle Bedrohungstrends

Charakteristisch für die Automobilindustrie ist die globale Konzeption mit ihren Abhängigkeiten. Weltweit müssen viele Endpunkte überwacht und geschützt werden. Das gilt auch für alle Unternehmen in der Wertschöpfungskette. Angefangen bei denjenigen, die für die Rohmaterialien verantwortlich sind bis hin zu den Autohäusern und Fahrzeugbesitzern. Die digitale Angriffsfläche dieser komplexen Lieferkette ist gewaltig, dennoch muss sie unbedingt gesichert werden, um die Betriebsabläufe aufrechtzuerhalten.

Zwischen dem 1. September und dem 30. November 2022 präsentierte sich uns eine große Bandbreite bei den Angriffen. Angefangen bei einfachem Malspam bis hin zu ausgeklügeltem Spearphishing war alles dabei. Dies zeigt, dass die Automobilindustrie sowohl unter dem Beschuss von Anfängern als auch von erfahrenen Cyberangreifern steht.

### *Downloader*

Malware-Downloader finden sich bei fast allen Arten von Cyberangriffen. Allerdings unterscheiden sie sich bezüglich Aussehen, Dateityp und Raffinesse der Techniken, mit denen sie in Systeme eindringen, mitunter erheblich. Bedrohungsakteure überreden im ersten Schritt ihre Opfer dazu, den Downloader zu installieren. Sobald der Code ausgeführt wird, installieren die Downloader bösartigen Code und Nutzlasten, um weitreichendere Cyberangriffe zu ermöglichen.

GuLoader ist ein Paradebeispiel für einen Downloader, der im Berichtszeitraum bei Angriffen auf die Automobilindustrie zum Einsatz kam. Die Malware wurde 2019 erstmals entdeckt und entwickelt sich seither ständig weiter. GuLoader präsentiert sich zunächst als legitimes digitales Dokument oder ausführbare Datei, bevor es dann gängige Malware herunterlädt.

## *Infostealer*

Die hochkarätigen und besonders geschützten Daten der Automobilindustrie machen die Branche zu einem bevorzugten Ziel für Cyberdiebe. Diese Daten sind häufig wertvoller als die Fahrzeuge selbst.

Malware-Infostealer sind eine Art von bösartigem Code, der Daten aus dem System eines Opfers auskundschaftet und illegal exfiltriert. Diese Daten werden dann entweder monetarisiert und/oder zu taktischen Zwecken verwendet. In Verbindung mit RATs können Infostealer wie Remcos als Commodity-Malware eingesetzt werden. Diese werden oft als Service für andere Bedrohungsakteure verkauft, damit sie Zugang und Kontrolle über fremde Systeme erhalten.

## *Ransomware*

Ransomware sorgt seit Langem für schlaflose Nächte bei Sicherheitsteams. Schließlich ist es kein Geheimnis, dass Ransomware, die auf industrielle Lieferketten abzielt, verheerende Folgen haben kann. In der Automobilindustrie kann ein Ransomware-Angriff auf die Lieferkette die Produktion oder den Vertrieb ganz zum Erliegen bringen. Umsatz- und Reputationsverluste im gesamten Ökosystem wären dann kaum zu verhindern.

Die Ransomware BlackCat ist bei einigen der berüchtigtsten Ransomware-Angriffe 2022 beobachtet worden. BlackCat gibt es als RaaS und wird meist von Gruppen eingesetzt, die finanzielle Motive verfolgen. Die Ransomware hat es vor allem auf Unternehmen in der Fertigungsindustrie abgesehen, insbesondere auf kleinere bis mittlere Unternehmen.

**48 %**

***DER AUTODIEBSTÄHLE BETRAFEN FAHRZEUGE MIT SCHLÜSSELLOSER TECHNOLOGIE.***

BlackCat infiltriert im ersten Schritt eine Umgebung, exfiltriert dann die gefundenen wertvollen Daten und verschlüsselt im nächsten Schritt die verbundenen Systeme.

ALPVH, die Bedrohungsgruppe, die hinter der BlackCat-Ransomware steckt, bevorzugt die doppelte Erpressung. Bei dieser Methode wird ein Teil der abgezogenen Daten auf einer Leak-Site, die gestohlene private und sensible Dokumente hostet, veröffentlicht. Dadurch wächst der Druck auf das betroffene Unternehmen, das Lösegeld zu zahlen, bevor noch wertvollere Daten veröffentlicht oder an Konkurrenten verkauft werden können[16].

## *Dual-Use-Tools*

Dual-Use-Tools bezeichnet legitime Programme, die zwei oder mehr Anwendungsbereiche haben und über Features oder Funktionen verfügen, die auch von Bedrohungsakteuren zweckentfremdet werden können. Häufig spricht man in diesem Zusammenhang auch von „Living off the Land" (LotL). Die Bedrohungsakteure umgehen mithilfe legitimer Tools Sicherheitssysteme und fliegen dadurch unter dem Radar.

Die Nutzung von bösartigem Code ist nicht mehr so beliebt wie früher. Bedrohungsakteure verwenden zunehmend Dual-Use-Tools, um sich in einer Umgebung zu verbreiten, wertvolle Daten zu exfiltrieren oder sogar Malware als legitime Tools zu tarnen. Deshalb sollten Systemadministratoren alle unnötigen Dual-Use-Tools entfernen. Ohne gültige Anwendungsfälle oder eine geschäftliche Rechtfertigung sind sie eine Gefahr.

## *Bedrohungslandschaft in der Automobilindustrie*

Je smarter und vernetzter die modernen Fahrzeuge werden und je mehr softwaredefinierte Fahrzeuge (SDVs) auf dem Markt auftauchen, die Software-Updates für neue Funktionen brauchen, desto größer sind die Chancen für Bedrohungsakteure. Schätzungen zufolge werden 2023 bis zu 775 Millionen vernetzte Fahrzeuge auf den Straßen unterwegs sein[17]. Die Zahl der Angriffsversuche wird höchstwahrscheinlich steigen, da sich die Branche Störungen jeglicher Art bei der Produktion, der Fertigung, dem Versand oder dem Verkauf nicht leisten kann.

In den letzten Jahren kamen die verschiedensten Methoden bei direkten Angriffen auf Fahrzeuge zum Einsatz. Dabei hat sich gezeigt, dass schlüssellose Fahrzeuge besonders anfällig sind.

Die Daten, die der britischen Versicherungsgesellschaft LV= General Insurance vorliegen, beweisen, dass bei 48 Prozent der Autodiebstähle schlüssellose Fahrzeuge betroffen waren[18]. Im Oktober 2022 verkündete Europol die Aushebung eines europäischen Autodiebstahlrings. Die Gruppe hatte sich auf Fahrzeuge mit Keyless-Entry- und Keyless-Start-Systemen konzentriert. Mithilfe von Schadsoftware gelang es ihr, die Fahrzeuge auch ohne physische Schlüsselanhänger zu stehlen[19]. Die Enthüllung erfolgte aus Sicherheitsgründen, nachdem die Schwachstelle gemeldet und gepatcht worden war.

In den letzten fünf Jahren war die Automobilindustrie fast ununterbrochen Cyberangriffen jeglicher Art ausgesetzt. Meist ging es um Datenschutzverletzungen, Ransomware-Attacken oder Angriffe durch Advanced Persistent Threats (APT)-Gruppen. 2022 stieg dann die Zahl der Bedrohungen sprunghaft an. Da eingebettete Technologien immer beliebter werden, wird diese Zahl vermutlich weiter steigen. Bereits 2017 wurde ein Automobilhersteller Opfer der WannaCry-Ransomware[20], die ihn zu einem kurzen Produktionsstopp zwang. 2019 machte die APT32-Gruppe, auch bekannt als OceanLotus, auf sich aufmerksam[21]. Einige Quellen sagen ihr die Unterstützung des vietnamesischen Automobilsektors nach[22]. Dieselbe Gruppe hat auch die Netzwerke anderer Automobilhersteller ins Visier genommen und kompromittiert[23]. Von 2020 bis 2022 nahm die Zahl der Angriffe zu. Meist handelte es sich hierbei um Ransomware-Angriffe. 2022 gab es dann außergewöhnliche Ransomware-Angriffe auf eines der größten europäischen Autohäuser[24], einen niederländischen Spezialfahrzeughersteller[25] und einen amerikanischen Reifenhersteller[26].

Die folgende Abbildung visualisiert die größten Angriffe auf die Automobilindustrie im Jahr 2022 in einer Zeitleiste.

## GRÖSSTE ANGRIFFE AUF DIE AUTOMOBILINDUSTRIE 2022

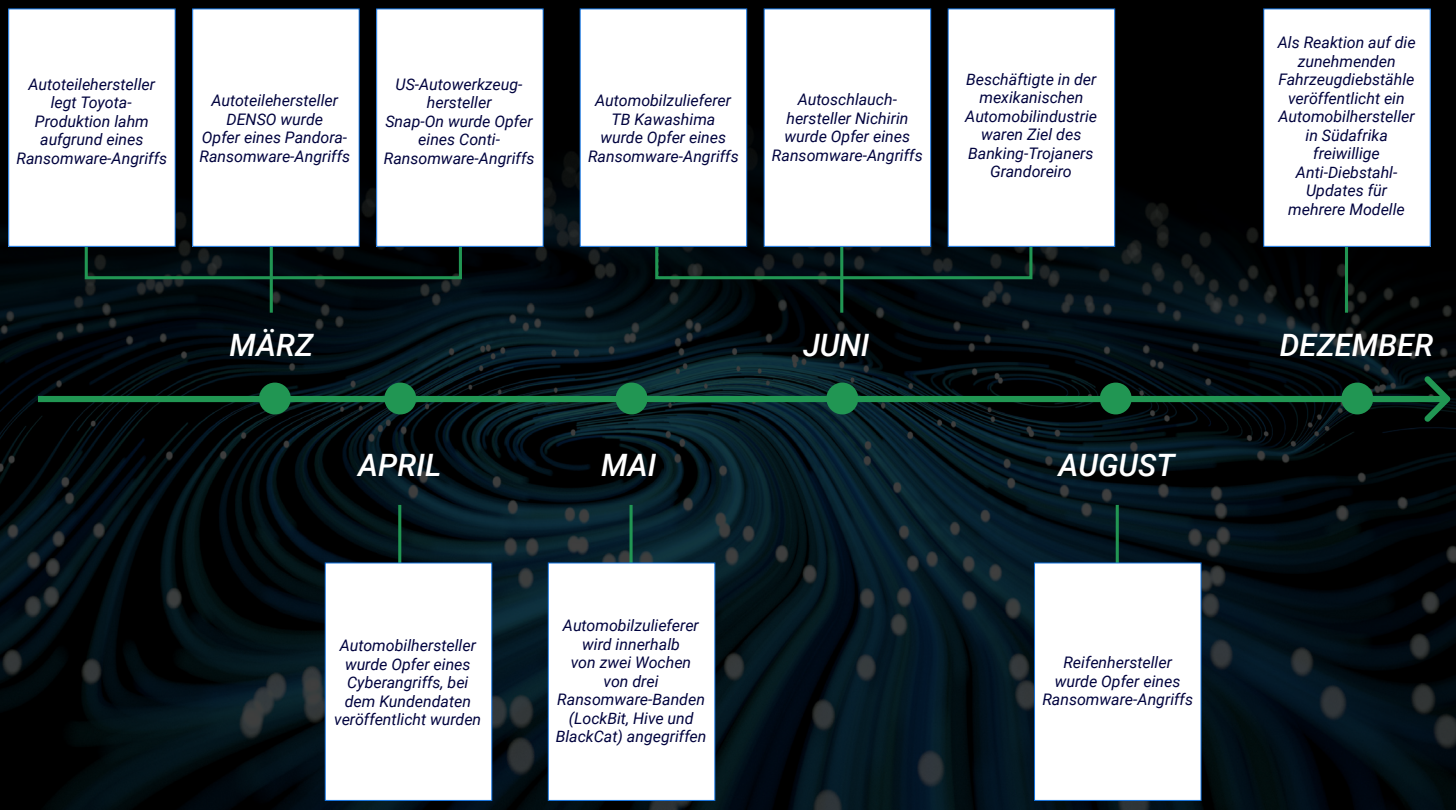



*Abb. 5: Zeitleiste der größten Angriffe auf die Automobilindustrie in 2022.*

## *Angriffe auf die Lieferkette*

Sowohl die Pandemie als auch der russische Einmarsch in der Ukraine haben gezeigt, dass die globalen Lieferketten anfällig sind. Die Automobilindustrie ist nicht immun gegen Verzögerungen, sie kämpft genauso gegen Engpässe und Betriebsunterbrechungen wie andere Branchen auch.

Angesichts der Komplexität setzen viele Unternehmen bei der Lieferkette auf eine Just-in-time-Strategie. Sie glauben, so ihr gewaltiges Ökosystem aus Lieferanten, Ersatzteilen und Herstellern besser aufrechterhalten zu können. Allerdings bieten sie dadurch böswilligen Angreifern eine riesige Angriffsfläche. Denn bei dieser Strategie werden Produkte erst dann hergestellt, wenn sie benötigt werden. Folglich stockt oder verlangsamt sich die Produktion, wenn wichtige Komponenten oder Materialien nicht sofort verfügbar sind. Ein Cyberangriff innerhalb der Lieferkette kann somit die Automobilproduktion abrupt stoppen.

Automobilhersteller selbst sind meist hervorragend gegen externe Bedrohungen geschützt. Böswillige Angreifer versuchen deshalb ihr Glück lieber über Zulieferer, die womöglich über weniger Cybersicherheit verfügen. Im März 2022 führten beispielsweise kompromittierte Dateisysteme bei Kunststoff- und Elektroniklieferanten zu Produktionsverzögerungen bei einem japanischen Automobilhersteller. Schätzungsweise waren 13.000 Fahrzeuge betroffen. Ein Sprecher des Unternehmens gab gegenüber Automotive News Europe an, dass die Lieferkette des Automobilunternehmens 60.000 Unternehmen auf vier Ebenen[27] umfasst. Cyberangriffe bei einer Lieferkette dieser Größenordnung beeinträchtigen auch andere Unternehmen, die Ersatzteile und Materialien dieser Firmen benötigen.

## *Zukunftstrends*

Die verzweigten Lieferketten und komplexen Geschäftsbeziehungen der Automobilindustrie sind ein äußerst attraktives Ziel für Cyberangriffe. Deshalb unternimmt die Branche zahlreiche Schritte, um ihre Sicherheit und Resilienz nachhaltig zu erhöhen. 2022 kündigte RISE, ein schwedisches, staatlich gefördertes Forschungsinstitut, den Launch des RISE Cyber Test Lab for Automotive Cyber Security an. Es soll Europas fortschrittlichstes Zentrum für Cybersicherheit in der Automobilindustrie werden. Laut Planungen sollen die ersten Tests bereits 2023 erfolgen. Zudem empfiehlt die US-Bundesbehörde NHTSA in ihren Cybersecurity Best Practices for the Safety of Modern Vehicles, die 2022 aktualisiert wurden, Fahrzeugherstellern und Zulieferern nachdrücklich, Cyberrisiken über den gesamten Lebenszyklus eines Fahrzeugs hinweg zu schützen, zu erkennen und darauf zu reagieren[28]. Dieser Leitfaden wird durch die globale technische Norm für Cybersicherheit in der Automobilindustrie ISO/SAE 21434 unterstützt.

## *GESUNDHEITSWESEN*

Die Gesundheitsbranche ist immer häufiger Opfer von Cyberangriffen, da Bedrohungsakteure in den vertraulichen Daten und sensiblen Informationen der Gesundheitseinrichtungen ein attraktives Ziel sehen. Vor allem für Gesundheitsdienstleister ist dies eine große Herausforderung, denn ein erfolgreicher Cyberangriff führt nicht selten zum Verlust oder zur Veröffentlichung sensibler Patientendaten. Neben den finanziellen Verlusten können die Angriffe sogar eine ernste Gefahr für Leib und Leben der Patienten darstellen. Allein durch das Ausmaß des Schadens ist das Gesundheitswesen besonders anfällig für Bedrohungen. Weitere Faktoren sind der großflächige Einsatz von Medizintechnik mit einer langen Lebensdauer, die komplexe und oft vernetzte Natur der Gesundheitssysteme sowie die riesigen Mengen an sensiblen Daten, die routinemäßig erfasst und gespeichert werden. Die Branche muss sich daher unbedingt über die Gefahren der aktuellen Cyberbedrohungslandschaft im Klaren sein und sich und ihre Patienten proaktiv vor möglichen Folgen schützen.

Ransomware stellt immer noch die größte Bedrohung für das Gesundheitswesen dar. Denn die Bedrohungsgruppen, die mithilfe von Ransomware das Gesundheitswesen ins Visier nehmen, sind immer noch äußerst aktiv. Dies zeigt auch der Ransomware-Angriff im Oktober 2022 auf CommonSpirit Health, den zweitgrößten US-amerikanischen Gesundheitsdienstleister, bei dem die Daten von mehr als 600.000 Patienten kompromittiert wurden[29]. Zwar haben einige RaaS-Gruppen wie Maze erklärt, dass sie keine Krankenhäuser mehr angreifen wollten. Doch sollte sich niemand auf solche Versprechen verlassen. Denn die Vielzahl der RaaS-Gruppen und die Verbreitung von Partnerschaftsmodellen erschwert die Zuordnung und Verfolgung der Malware. Zumal die Entwickler der Malware nicht zwingend auch die Angriffe durchführen.

Die Telemetriedaten zeigen, dass unsere Cylance Endpoint Security Lösungen im Berichtszeitraum 7.748 einzelne Malware-Samples gestoppt haben, die direkt auf das Gesundheitswesen zielten. Dies entspricht einem Durchschnitt von mehr als 80 einzelnen Malware-Samples pro Tag. Der Trojaner, der am häufigsten eingesetzt wurde, war Qakbot.

# 600.000

***PATIENTENDATEN WURDEN BEIM RANSOMWARE-ANGRIFF AUF COMMONSPIRIT HEALTH IM OKTOBER GESTOHLEN.***

Er treibt seit 2012 sein Unwesen und stellt damit ein nicht unerhebliches Risiko für das Gesundheitswesen dar. 2022 wurde Qakbot hauptsächlich von Gruppen verwendet, die mit der Ransomware Black Basta in Verbindung gebracht werden. Da Emotet nach seiner viermonatigen Abschaltung kaum noch Kampagnen durchgeführt hat und TrickBot sich auf die Verbesserung seiner Bumblebee-Malware zu konzentrieren scheint, nehmen wir an, dass Qakbot derzeit der aktivste Trojaner ist, der seinen RaaS-Affiliates und böswilligen IABs Tür und Tor öffnet.

Auch Meterpreter, eine Metasploit-Nutzlast, die eine interaktive Shell für den Angreifer bereitstellt, und BloodHound konnten wir im Berichtszeitraum beobachten. Wir haben einen Angriff entdeckt, bei dem Meterpreter zusammen mit der Ausführung von SharpHound verwendet wurde, einem Collector für BloodHound, der üblicherweise für seitliche Bewegungen innerhalb eines Netzwerks nach einem Angriff verwendet wird. Die US-Behörde CISA empfiehlt deshalb Netzwerk- und Systemadministratoren die Ausführung von BloodHound, um mögliche Angriffspfade in ihren Umgebungen aufzuspüren[30].

Außerdem haben wir beobachtet, dass TinyNuke den Netwire RAT ausführt. Zwar handelt es sich hierbei ursprünglich um einen Banking-Trojaner mit ähnlichen Funktionen wie ZeuS, doch mittlerweile präsentiert sich TinyNuke als vollwertiger Trojaner, einschließlich VNC-Server-Geräte-Controller und Reverse-SOCKS-Funktionalitäten. TinyNuke wurde auch von der Kimsuky Group[31] eingesetzt und Nordkorea zugeschrieben. Bei der Untersuchung dieses Angriffs haben wir festgestellt, dass TinyNuke Netwire RAT herunterlädt, ausführt und sich mit einer Domain verbindet, die auf DuckDNS gehostet wird, das üblicherweise von RATs verwendet wird.

Die BlackBerry Researcher haben auch einen Fall entdeckt, in dem ein unbekannter Bedrohungsakteur den PlugX RAT eingesetzt hat. Dieser wird üblicherweise von bestimmten nationalstaatlichen Bedrohungsakteuren wie Mustang Panda verwendet. Weitere Informationen dazu finden Sie in unserem öffentlichen Bericht. Damit verdichten sich die Hinweise darauf, dass nicht nur Cyberkriminelle, sondern auch nationalstaatliche Akteure ein starkes Interesse daran haben, die Gesundheitsbranche anzugreifen. Zwar haben wir keine Infostealer wie Redline und Raccoon entdeckt, die explizit auf das Gesundheitswesen zielen, allerdings sind wir auf eine Instanz von GuLoader gestoßen, einem Downloader, der von Cyberkriminellen oft zur Verbreitung von Infostealern verwendet wird.

## FINANZINDUSTRIE

Die Finanzbranche ist seit jeher das Ziel von Cyberkriminellen und nationalstaatlichen Bedrohungsakteuren, die aus Gegenden und Ländern stammen, die unter Finanzsanktionen leiden. Während des 90-tägigen Berichtszeitraums haben unsere Cylance Endpoint Security Lösungen 9.721 einzigartige Malware-Samples gestoppt, die sich gegen Ziele in der Finanzbranche richteten. Der Durchschnitt beträgt damit 108 einzigartige und bösartige Samples pro Tag.

Verschiedene Bedrohungsakteure, nicht nur Cyberkriminelle, sondern auch staatliche Akteure, nutzen kommerzielle Penetrationstests wie Cobalt Strike und andere, um die Zuordnung zwischen bösartigen und legitimen Testaktivitäten zu verwischen.

Diese Verwirrtaktik verschafft den Akteuren mehr Zeit, sich in einem Netzwerk umzusehen, nachdem sie sich Zugang verschafft haben. 2022 wurden wir Zeuge mehrerer Vorfälle, bei denen kommerzielle Software zur Angriffssimulation, wie Cobalt Strike und Pen-Testing-Software wie Metasploit, Mimikatz und Brute Ratel, in Finanzinstituten eingesetzt wurde. Brute Ratel ist ein Tool zur Simulation von Angriffen. Und auch Mimikatz wird häufig sowohl von Kriminellen als auch von Sicherheitsexperten verwendet, um vertrauliche Informationen wie Passwörter und Anmeldedaten aus dem Speicher eines Systems zu extrahieren. Derzeit ist nicht bekannt, ob Mimikatz und Brute Ratel im Rahmen legitimer Pen-Tests oder echter Angriffe eingesetzt wurden.

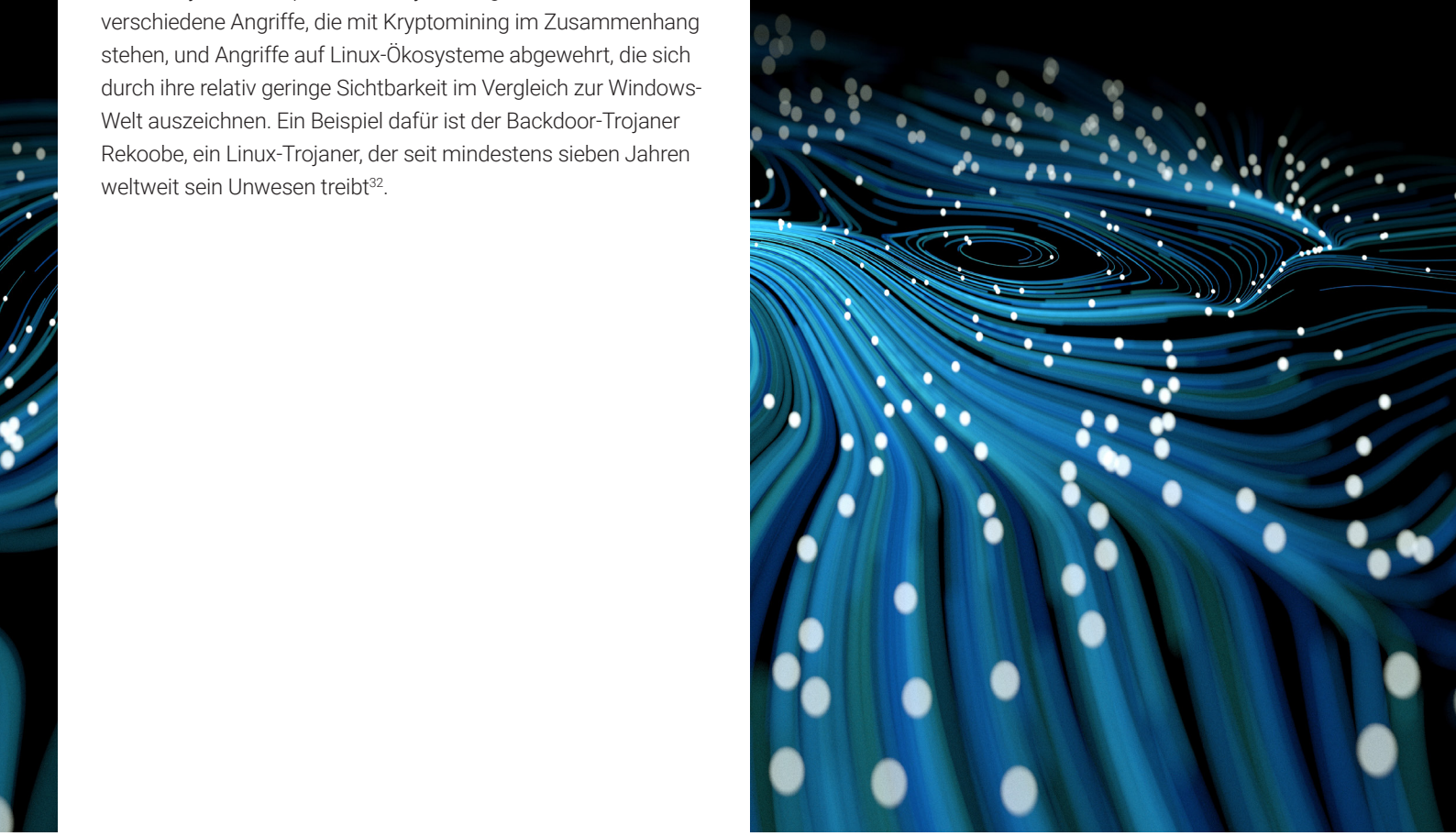
Neben anderen Top-Bedrohungen haben wir auch Initial-Access-Infostealer wie Redline Stealer gestoppt. Es ist allgemein bekannt, dass Tools für den Erstzugang sehr gefragt sind, da sie für Zugang zu Netzwerken sorgen, der dann verkauft werden kann. Viele Bedrohungsakteure, darunter auch die Lapsus$-Gruppe, setzen auf Infostealer, um sich Zugang zu Unternehmen zu verschaffen. Die Lapsus$-Gruppe ist eine internationale Erpressungsgruppe, der zahlreiche Cyberangriffe auf Unternehmen und Regierungsbehörden zugeschrieben werden.

Unsere Cylance Endpoint Security Lösungen haben auch verschiedene Angriffe, die mit Kryptomining im Zusammenhang stehen, und Angriffe auf Linux-Ökosysteme abgewehrt, die sich durch ihre relativ geringe Sichtbarkeit im Vergleich zur Windows-Welt auszeichnen. Ein Beispiel dafür ist der Backdoor-Trojaner Rekoobe, ein Linux-Trojaner, der seit mindestens sieben Jahren weltweit sein Unwesen treibt[32].

***CYLANCE ENDPOINT SECURITY LÖSUNGEN STOPPTEN***

# 9.721

***EINZIGARTIGE MALWARE-SAMPLES, DIE AUF DIE FINANZINDUSTRIE ABZIELTEN.***



# AKTIVSTE BEDROHUNGS-AKTEURE

**Unsere Telemetrie förderte auch die Aktivitäten vieler verschiedener Bedrohungsakteure zutage. Einige der hier aufgeführten Angreifer wurden bereits in den vorangegangenen Abschnitten über bestimmte Angriffsarten oder Branchen erwähnt.**

## TA505

TA505 ist eine sehr aktive und einflussreiche Gruppe von Cyberkriminellen, die die Welt der finanziell motivierten Cyberbedrohungen entscheidend prägt. Zu den bevorzugten Branchen dieser Gruppe gehören weltweit das Bildungs- und Finanzwesen, das Gesundheitswesen, das Gastgewerbe und der Einzelhandel.

Die Gruppe ist dafür bekannt, dass sie Unmengen an bösartigen E-Mails versendet und über ein breites Spektrum an Malware verfügt. Ein deutlicher Hinweis auf starke Verbindungen zu Untergrund-Malware-Netzwerken. Wie schon zuvor verwendet die Gruppe hauptsächlich die Ransomware Locky für ihre Angriffe, allerdings experimentiert sie auch mit anderen Malware-Arten.

Das Toolset von TA505 umfasst Cl0p-Ransomware, den FlawedAmmyy RAT, der auf durchgesickertem Quellcode für eine Version des legitimen Tools Ammyy Admin basierte, und Banking-Trojaner wie Dridex.

## ALPHV

ALPHV ist eine relativ neue und schnell wachsende Gruppe von Cyberkriminellen, die durch innovative Erpressungstaktiken und unkonventionelle Angriffsmethoden auf sich aufmerksam machen. Trotz ihrer relativ kurzen Historie hat die Gruppe einen bedeutenden Einfluss auf ihre Community. Dementsprechend wird sie sich wahrscheinlich weiterentwickeln und ihre Operationen ausweiten[33].

Charakteristisch für ALPHV ist die Verwendung von Rust. Hierbei handelt es sich um eine äußerst leistungsstarke Programmiersprache, mit deren Hilfe Bedrohungsakteure eine Codebasis auf vielen verschiedenen Betriebssystemen verwenden können. Die Gruppe arbeitet mit mehreren LotL-Binärdateien, -Skripten und -Bibliotheken (LOLBins), um ihre Ziele zu erreichen.

Die RasS BlackCat kommt in der letzten Phase der ALPHV-Hacking-Kampagnen zum Einsatz. Zuvor hat sich die Gruppe seitlich innerhalb bestimmter Hosts bewegt und für sie interessante Informationen gesammelt. Erst dann beginnt ALPHV mit der finanziellen Erpressung. Zur Verstärkung der Lösegeldforderung droht die Gruppe sogar mit DDoS-Angriffen. Seit sie BlackCat als RaaS anbietet, hat sich die Hackergruppe dem schnell wachsenden Malware-Trend der doppelten Erpressungsangriffe angeschlossen. Hierbei werden die Daten nicht nur exfiltriert, sondern auch verschlüsselt, um Lösegeld zu erpressen.

Die ALPHV-Gruppe begnügt sich nicht mit einem bestimmten Sektor oder einem bestimmten Land. Da ALPHV die Ransomware BlackCat auch anderen Gruppen zur Verfügung stellt, weist die Existenz der Malware nicht unbedingt auf ALPHV als Angreifer hin. Angriffe mit der BlackCat-Ransomware gab es bisher auf den Einzelhandel, die Finanz- und Fertigungsindustrie, Behörden, den Technologiesektor sowie das Bildungs- und Transportwesen in Ländern wie den USA, Australien, Japan, Italien, Indonesien, Indien und Deutschland[34].

## APT32

Es wird angenommen, dass APT32 seinen Sitz in Vietnam hat und seit ungefähr 2014 bösartige Cyberaktivitäten durchführt. Die Aktionen zielen auf verschiedene private Unternehmen, ausländische Regierungen und Einzelpersonen wie Dissidenten und Journalisten. Geografisch liegt der Schwerpunkt auf südostasiatischen Ländern wie Vietnam, den Philippinen, Laos und Kambodscha. APT32 wendet häufig Taktiken zur strategischen Kompromittierung des Internets an, um Zugang zu den Systemen der Opfer zu erhalten. Diese hochentwickelte Gruppe hat auch schon Verteidigungsorganisationen, Hightech-Unternehmen, das Gesundheitswesen und die Fertigungsindustrie angegriffen.

Das BlackBerry Threat Research and Intelligence Team hat mehrere APT32-Eindringlinge analysiert. Die Gruppe hat eine Reihe von RATs mit der Bezeichnung Ratsnif eingesetzt, um neue Möglichkeiten für Netzwerkangriffe zu schaffen. Wir haben außerdem festgestellt, dass die Gruppe mit Steganografie arbeitet. Bei dieser Technik werden geheime Daten in einer gewöhnlichen, nicht geheimen Datei oder Nachricht versteckt, um eine bösartige Nutzlast in ein PNG-Bild einzubetten.

## APT29 (THE DUKES)

APT29 ist auch als „The Dukes" bekannt. Hierbei handelt es sich um eine gut finanzierte und hochorganisierte Gruppe, die im Verdacht steht, seit mindestens 2008 für die russische Regierung Cyberspionage zu betreiben. Die Gruppe hat es vor allem auf Regierungen und NGOs in Nordamerika und Europa abgesehen, sie hatte aber auch schon Einrichtungen in Asien, Afrika und im Nahen Osten im Visier.

Die Gruppe verwendet häufig Cobalt Strike, Mimikatz und AdFind, ein kostenloses Tool zur Abfrage von Befehlszeilen, das Informationen aus dem Active Directory sammeln kann. Die Gruppe hat zudem zahlreiche benutzerdefinierte Tools entwickelt, zu denen u. a. auch CloudDuke, CozyDuke und FatDuke gehören. Außerdem ist bekannt, dass APT29 auch Schwachstellen in bestimmten Produkten ausnutzt, um auf die Systeme ihrer Opfer zuzugreifen.

## MUSTANG PANDA

Mustang Panda ist eine in China ansässige APT-Gruppe, die sich auf Cyberspionage spezialisiert hat. Die Gruppe wurde 2017 erstmals entdeckt und ist womöglich bereits seit 2014 aktiv[35]. Mustang Panda hat ein breites Spektrum an Unternehmen ins Visier genommen, darunter sind Regierungsbehörden, gemeinnützige Organisationen, religiöse Einrichtungen und NGOs in Ländern auf der ganzen Welt. Der Schwerpunkt liegt auf den USA, Europa, der Mongolei, Myanmar, Pakistan und Vietnam.

Die Gruppe nutzt häufig China Chopper und PlugX für ihre Operationen. PlugX ist ein modularer RAT, der so konfiguriert werden kann, dass er sowohl HTTP als auch DNS für Command-and-Control (C2)-Aktivitäten nutzt. China Chopper ist eine bösartige Software, die auf Webservern gehostet wird und unbefugten Zugriff auf das Netzwerk eines Unternehmens ermöglicht, ohne dass ein infiziertes Gerät mit einem entfernten C2-Server kommunizieren muss.

Das BlackBerry Threat Research and Intelligence Team hat jüngst Aktivitäten entdeckt, bei denen Mustang Panda das weltweite Interesse am Ukrainekrieg nutzt, um Ziele in Europa und im asiatisch-pazifischen Raum anzugreifen.

## TA542

Es wird vermutet, dass die kriminelle TA542-Gruppe eine wichtige Rolle bei der Entwicklung der Emotet-Malware gespielt hat. Diese Malware wurde erstmals Mitte 2014 entdeckt und teilt bestimmte Merkmale mit dem Banking-Trojaner Bugat, der auch als Feodo bekannt ist. Zudem wurde sie um einen RSA-Schlüsselaustausch für die C2-Kommunikation und einen modularen Aufbau erweitert. TA542 folgt nicht den typischen Verhaltensmustern cyberkrimineller Organisationen. Sie ziehen Angriffe in kurzer Zeit durch und legen dann eine mehrmonatige Pause ein. Danach tauchen sie meist mit einer neuen Version auf oder probieren eine Malware-Variante aus. Zu den bevorzugten Branchen der TA542-Kampagnen gehören das Bildungs- und Finanzwesen, der Einzelhandel und das Gesundheitswesen.

# GÄNGIGE MITRE-TECHNIKEN

Das BlackBerry Threat Research and Intelligence Team nutzt mehrere MITRE-Techniken, Ereignisanalysen und Telemetriedaten, um Bedrohungen zu analysieren. Die MITRE-Techniken, die wir im Berichtszeitraum verwendet haben, finden Sie in der folgenden Tabelle. Eine vollständige Liste der vom BlackBerry Team verwendeten MITRE-Techniken finden Sie im MITRE ATT&CK® Navigator Layer.

## TABELLE 1: GÄNGIGE MITRE-TECHNIKEN UND -TAKTIKEN

| MITRE-Techniken | Technik-ID | Taktik |
|---|---|---|
| System Information Discovery | T1082 | Discovery |
| Process Injection | T1055 | Defense evasion |
| Virtualization/Sandbox Evasion | T1497 | Defense evasion |
| Remote System Discovery | T1018 | Discovery |
| Masquerading | T1036 | Defense evasion |
| Application Layer Protocol | T1071 | Command-and-control |
| Software Packing | T1027.002 | Defense evasion |
| Security Software Discovery | T1518.001 | Discovery |
| Process Discovery | T1057 | Discovery |
| Disable or Modify Tools | T1562.001 | Defense evasion |
| Application Window Discovery | T1010 | Discovery |
| Windows Management Instrumentation | T1047 | Execution |
| Query Registry | T1012 | Discovery |
| Obfuscated Files or Information | T1027 | Defense evasion |
| Modify Registry | T1112 | Defense evasion |
| File and Directory Discovery | T1083 | Discovery |
| Encrypted Channel | T1573 | Command-and-control |
| Command and Scripting Interpreter | T1059 | Execution |
| Rundll32 | T1218.011 | Defense evasion |
| Regsvr32 | T1218.010 | Defense evasion |

Die meisten der hier aufgeführten Techniken stehen im Zusammenhang mit Umgehungs- und Entdeckungstaktiken. Im Allgemeinen werden diese Taktiken und verwandte Techniken bei der Nachuntersuchung einer Infektion aufgedeckt. Die Anwendung dieser Techniken erfordert Kenntnisse über die zuvor identifizierten Eindringlinge. Hier finden Sie Verhaltensbeispiele für die fünf häufigsten Techniken.

## *VERHALTENSBEISPIELE FÜR GÄNGIGE TECHNIKEN*

Die folgende Tabelle beschreibt die Verhaltensweisen, die mit den gängigsten MITRE-Techniken verbunden sind.

### *TABELLE 2: VERHALTENSMUSTER FÜR GÄNGIGE TECHNIKEN*

| Technik | Verhalten |
|---|---|
| System Information Discovery - T1082 | > wmic csproduct get UUID<br>> query user<br>> tasklist \| findstr “dll”<br>> systeminfo >> output<br>> date /t |
| Process Injection - T1055 | > dllhost.exe<br>> rundll32.exe<br>> explorer.exe<br>> MSBuild.exe |
| Virtualization/Sandbox Evasion - T1497 | > timeout 5000<br>> Start-Sleep -s 100<br>> Registrierungen von VMWare und VirtualBox prüfen |
| Remote System Discovery - T1018 | > net group /domain admins<br>> nltest /domain_trusts /alltrusts<br>> net view /all |
| Masquerading - T1036 | > Dateiname der Malware in einen legitim klingenden Dateinamen umbenennen<br>> .jpg-Erweiterung für Binärdateien verwenden<br>> Geplante Aufgaben mit legitimen Namen wie win32times und anderen verwenden |

## MITRE D3FEND ABWEHRMASSNAHMEN

Durch die Kenntnis gängiger Abwehrmaßnahmen können Unternehmen ihre Verteidigungsstrategien verbessern und feststellen, ob die Sichtbarkeit angemessen ist und ob Erkennungstechniken vorhanden sind. Abwehrmaßnahmen können auf Vorfällen im Betriebssystem basieren wie z. B. Prozessereignissen, die im System auftreten oder auf Dateiereignissen wie sie beim Erstellen, Ändern oder Löschen von Dateien vorkommen.

Eine vollständige Liste von Angriffstechniken und den zugehörigen Abwehrmaßnahmen finden Sie in unserem GitHub Repository. Wir empfehlen Ihnen, nur die Abwehrmaßnahmen auszuwählen, die Sie vollständig implementieren können und die den Anforderungen Ihres Unternehmens am besten entsprechen.

***FÜR EINE VOLLSTÄNDIGE LISTE DER ANGRIFFSTECHNIKEN SOWIE DER ZUGEHÖRIGEN ABWEHRMASSNAHMEN BESUCHEN SIE BITTE DAS BLACKBERRY GITHUB REPOSITORY.***

# BEKANNTESTE ANGRIFFE

Zwischen dem 1. September und dem 30. November 2022 hat das BlackBerry Threat Research and Intelligence Team die weltweite Cyberbedrohungslage beobachtet, Trends aufgedeckt, Informationen recherchiert und veröffentlicht. Die Weltwirtschaft muss sich noch immer von den Folgen der Corona-Pandemie erholen. Außerdem sorgen die aktuellen geopolitischen Ereignisse in Osteuropa für Unsicherheit und die Ost-West-Beziehungen leiden darunter. Diese Faktoren bilden einen Boden für Bedrohungsakteure, die sowohl politisch als auch finanziell motiviert sind.

In diesem Quartal wurden APT-Gruppen mit staatlicher Beteiligung, finanziell motivierte Ransomware-Banden und viele andere Bedrohungsakteure aller Größen, Fähigkeiten und Motivationen bei der Durchführung verschiedener Kampagnen beobachtet. Hier finden Sie eine Auswahl der folgenreichsten Angriffe in der globalen Landschaft und unsere eigenen wichtigsten Funde im Laufe des Quartals.

## DJVU: SELTSAM VERTRAUTE RANSOMWARE

Die Ransomware DJVU tarnt sich als legitimer Dienst oder als legitime Anwendung und wird oft mit Täuschungsdateien verbunden, um harmlos zu erscheinen. DJVU ist eine Weiterentwicklung der berüchtigten STOP-Ransomware und hat seit 2018, dem Jahr ihrer Entstehung, viele Entwicklungen durchlebt. Die Ransomware verwendet für ihre Verschlüsselungsroutine die kryptografische Stromchiffre Salsa20.

Nach der Durchführung zahlreicher Anti-Analyse- und Anti-Sandbox-Prüfungen, die sie zur Bestätigung braucht, dass sie auf einem echten System ausgeführt wird, verschlüsselt die Malware mehrere Dateitypen. Erst dann schickt sie eine Lösegeldforderung mit Anweisungen an ihre Opfer. Durch das Hinzufügen von Ransomware Downloader-Funktionen zur Vorverschlüsselung wurde die Ransomware noch bösartiger.

In diesem Quartal hat DJVU offenbar mit den Bedrohungsgruppen zusammengearbeitet, die hinter der Arkei-Variante Vidar Stealer und Redline Stealer stecken, um die Möglichkeiten der Bedrohungsakteure auszubauen und noch mehr von den Opfern zu profitieren.

## *MUSTANG PANDA MISSBRAUCHT LEGITIME APPS, UM OPFER IN MYANMAR ANZUGREIFEN*

Anfang Oktober haben wir die Ergebnisse einer mehrmonatigen Verfolgung der APT-Gruppe Mustang Panda veröffentlicht. Diese Gruppe, die auch als Bronze President, Red Delta und Honeymyte bekannt ist, wird öffentlich China zugeschrieben.

Im Berichtszeitraum haben wir auch eine Kampagne aufgedeckt, die auf Myanmar abzielt. Die Kampagne präsentierte sich als populäre myanmarische Nachrichtenmedien und zielte auf mehrere Einrichtungen, darunter auch ein staatliches VPN-Portal. Der Infektionsvektor in dieser Kampagne bestand aus Phishing-Ködern mit bösartigen Anhängen. Diese sollten die User dazu verleiten, sie auszuführen, damit die Angreifer im System Fuß fassen konnten.

Die Ausführungskette enthielt mehrere Komponenten, darunter ein legitimes, gutartiges Dienstprogramm, das für das Hijacking der DLL-Suchreihenfolge anfällig ist, sowie einen bösartigen DLL-Loader und eine verschlüsselte DAT-Nutzlast. Nachdem der bösartige DLL-Loader als Sideload ausgeführt wurde, wird eine PlugX-Nutzlast in den Speicher geladen. Der Infektionsvektor, die Ausführungskette, die Verwendung von PlugX und die allgemeinen TTPs entsprechen einer gängigen Kampagnenmethodik von Mustang Panda.

## *BIANLIAN RANSOMWARE VERSCHLÜSSELT DATEIEN IN EINEM WIMPERNSCHLAG*

BianLian ist eine extrem schnell agierende Ransomware, die in der Programmiersprache GoLang geschrieben wurde. In diesem Whitepaper haben wir die aktuelle Zunahme der bösartigen Nutzung von seltenen Sprachen wie GoLang prognostiziert. Bedrohungsakteure kennen das Potenzial dieser Sprachen und nutzen es zur Erstellung von Malware, insbesondere von maßgeschneiderter Ransomware. GoLang bietet einen besonders soliden Support für simultane Aktionen, die Angriffe beschleunigen. So können mehrere bösartige Funktionen unabhängig voneinander zur gleichen Zeit ausgeführt werden.

BianLian ist eine relativ neue Bedrohung, die auf die verschiedensten Branchen zielt. Die Gruppe, die hinter dieser Malware steckt, scheint rein finanziell motiviert zu sein. Die BianLian-Angriffe konnten bis Ende 2022 beobachtet werden. Die Gruppe scheint die Systeme und Netzwerke, auf die sie zugreifen kann, stark auszunutzen. Ihren Aktionen geht die manuelle Infiltration der Systeme voraus. Hat die Gruppe einmal Zugang, nutzt sie LOLBins zur Erkundung der Netzwerke und Systeme. Nach der Erkundung setzt sie ihre Ransomware ein, um Kapital aus ihrer Aktion zu schlagen.

## *UNBEKANNTER ROMCOM-BEDROHUNGSAKTEUR FÄLSCHT BELIEBTE APPS UND GREIFT JETZT DAS UKRAINISCHE MILITÄR AN*

Im Oktober entdeckte BlackBerry den bisher unbekannten RomCom RAT, der auf ukrainische Militäreinrichtungen abzielt. Derselbe Bedrohungsakteur war dafür bekannt, gefälschte Versionen des beliebten Advanced IP Scanners einzusetzen, bevor er seine Bemühungen auf PDF Filler, eine weitere beliebte Anwendung, verlagerte und diese Exploits möglicherweise selbst entwickelt hat.

Der RAT RomCom versucht, die Kontrolle über die anvisierten Geräte zu übernehmen. Der erste Infektionsvektor, den wir beobachtet haben, war eine E-Mail mit einem eingebetteten Link zu einem gefälschten ukrainischen Dokument namens Наказ_309.pdf (Order_309.pdf auf Englisch), das den Downloader der nächsten Stufe auslöste.

Im Berichtszeitraum zeigte sich, dass dieser Bedrohungsakteur auch aktiv neue Techniken entwickelte, um Opfer auf der ganzen Welt anzugreifen.

## BEDROHUNGSAKTEUR HINTER ROMCOM NUTZT BELIEBTE SOFTWARE-MARKEN, UM DER UKRAINE UND POTENZIELL AUCH GROSSBRITANNIEN ZU SCHADEN

Nach zahlreichen Angriffen auf die Ukraine startete dieselbe Gruppe neue Angriffskampagnen, die andere beliebte Software-Marken zweckentfremdeten. Das BlackBerry Threat Research and Intelligence Team entdeckte die Kampagnen bei ihrer Analyse von Netzwerk-Artefakten, die bei unseren früheren Untersuchungen zum RomCom RAT führten.

Unsere Researcher fanden heraus, dass sich der Bedrohungsakteur in seinen Kampagnen als SolarWinds Network Performance Monitor, KeePass Open Source Password Manager und PDF Reader Pro ausgab. Die Kampagnen nutzten diese legitimen Produkte als Fassade und entwarfen gefälschte Websites, um die Opfer zum Herunterladen der Remcos RAT-Malware zu verleiten. Der RomCom-Bedrohungsakteur setzt auch weiterhin neue Kampagnen ein, die sich gegen die Ukraine richten. Und mit seiner jüngsten Angriffsreihe weitet er seine Ziele scheinbar auf andere englischsprachige Ziele in der ganzen Welt aus.

## RANSOMWARE ARCRYPTER BREITET SICH VON LATEINAMERIKA AUF DIE GANZE WELT AUS

Das BlackBerry Threat Investigation Team hat 2022 die ARCrypter Ransomware-Familie das ganze Jahr über beobachtet. Im August wurde eine unbekannte Variante gefunden, die wir ARCrypter genannt haben. Sie zielte auf lateinamerikanische Institutionen. Beispielsweise wurde INVIMA, das nationale Institut für Lebensmittel- und Arzneimittelüberwachung in Kolumbien, im Oktober aufgrund eines gemeldeten Cyberangriffs vorübergehend heruntergefahren[36].

Im Rahmen unseres Threat Huntings hat BlackBerry weitere bemerkenswerte Muster für diese Ransomware identifiziert. Der Zeitrahmen des Angriffs und der Inhalt der Lösegeldforderung, in der INVIMA erwähnt wird, weisen darauf hin, dass mit hoher Wahrscheinlichkeit die ARCrypter-Ransomware bei dem INVIMA-Cyberangriff verwendet wurde. Durch weitere Nachforschungen konnten wir zwei Dateisätze aufdecken: einen zusätzlichen Malware-Dropper und ein Dateiverschlüsselungsprogramm.

***DIE GLOBALE REICHWEITER DER KAMPAGNEN ZEIGT, DASS DIE MUSTANG-PANDA-GRUPPE ÜBER***

# UMFANGREICHE

***RESSOURCEN UND FÄHIGKEITEN VERFÜGT. WIR GEHEN DAVON AUS, DASS DIES NICHT IHR LETZTER ANGRIFF WAR.***

### MUSTANG PANDA NUTZT DEN UKRAINEKRIEG FÜR ANGRIFFE AUF ZIELE IN EUROPA UND IM ASIATISCH-PAZIFISCHEN RAUM

Im Dezember wurde durch unser kontinuierliches Monitoring eine Mustang-Panda-Kampagne aufgedeckt, die sich gegen Einrichtungen in mehreren Ländern und verschiedenen Kontinenten richtete.

Diese Kampagne nutzte thematische Köder mit aktuellem geopolitischen Bezug wie beispielsweise „Political Guidance for the New EU Approach Towards Russia.rar". Der Köder enthielt ein gefälschtes Dokument und eine LNK-Datei, die derselben Namenskonvention folgte wie die RAR-Datei des Köders. Zu den zusätzlichen Komponenten gehörten legitime Dienstprogramme, die anfällig sind für die Entführung von DLL-Suchaufträgen sowie bösartige DLL-Loader und DAT-Nutzlasten. Die Gruppe hatte ähnliche Komponenten bereits früher verwendet.

Ziel der Ausführungskette ist es, eine PlugX-Nutzlast in den Speicher des Hostsystems einzuschleusen, um vollständigen Remote-Zugriff auf das kompromittierte System zu erlangen.

Der Kern der Ausführungskette und die TTPs dieser Kampagne waren bereits bekannt, wurden für diese Angriffe aber leicht modifiziert. Entscheidend war eine Änderung im Ausführungsablauf. Anstelle von EnumThreadWindows wurde die Funktion EnumSystemCodePagesW für die Ausführung des Shellcodes verwendet. Diese kleine Änderung erforderte Anpassungen der Abwehrmaßnahmen, um einen möglichst effektiven Schutz zu gewährleisten.

Durch Auslagern eines eindeutigen Domain-SSL-Zertifikats konnten wir 15 zusätzliche IP-Adressen aufdecken. Fünf davon waren C2-Server der Mustang-Panda-Gruppe, die ähnliche Dateien, die derselben Angriffskette und denselben TTPs entsprechen, an zusätzliche Standorte und Opfer weiterleiten.

Die globale Reichweite der Kampagnen deutet darauf hin, dass die Gruppe über umfangreiche Ressourcen und Fähigkeiten verfügt. Wir gehen davon aus, dass dies nicht ihr letzter Angriff war.

## WEITERE ATTACKEN

### EMOTET

Emotet ist eine ausgeklügelte und sich ständig weiterentwickelnde Malware-Familie, auch bekannt als Heodo oder Geodo. Sie erschien im November 2022 wieder auf der Bildfläche und wird der kriminellen TA542-Gruppe zugeschrieben. Seit ihrer Entstehung 2014 hat sie sich vielfach weiterentwickelt[37].

Emotet wird meist als infiziertes Microsoft® Excel® Dokument via E-Mail verschickt. Die Opfer sollen diesen Anhang öffnen und dabei die Pop-up-Sicherheitswarnungen ignorieren. Was ein schwerer Fehler ist. Denn unmittelbar nach dem Öffnen der gefälschten Datei beginnt die Malware mit dem Download. Ist die Malware installiert, kann sie zahlreiche Funktionen ausführen. Darunter auch das Ablegen und Verteilen zusätzlicher Malware.

### CRYWIPER

Anfang Dezember wurden Einzelheiten über CryWiper bekannt, einen neuen Wiper, der bislang speziell russische Ziele im Visier hatte. Dazu gehörten auch verschiedene Gerichtsgebäude und Bürgermeisterbüros[38].

Auf den ersten Blick verhält sich CryWiper wie eine typische Ransomware. Sie fügt die Erweiterung .CRY an die Dateinamen an und hinterlässt über README.txt eine Lösegeldforderung mit Hinweisen zur Zahlung und Wiederherstellung. Doch der erste Eindruck täuscht. In Wirklichkeit zerstört CryWiper – wie andere Wiper auch – die Dateien auf den Zielsystemen unwiederbringlich, inklusive aller Schattendateien. Eine Wiederherstellung ist damit unmöglich. Unabhängig davon, ob Lösegeld gezahlt wurde oder nicht.

CryWiper nutzt für die vollständige Zerstörung der Dateien den Pseudozufallszahlengenerator (PRNG) Mersenne Vortex. Dadurch werden die ursprünglichen Inhalte der Datei überschrieben und vernichtet.

# SCHLUSSFOLGERUNGEN UND VORSCHAU FÜR Q1 2023

**Nicht nur der Berichtszeitraum, sondern das gesamte Jahr 2022 hat wichtige Cybersecurity-Trends zutage gefördert, die sich wahrscheinlich auch 2023 und darüber hinaus fortsetzen werden. Einer davon ist die wachsende Zahl der politisch motivierten Bedrohungsakteure. Ihre Aktionen reichen von Fehl- und Falschinformationen auf Fake-News-Websites, die Verfolgung von Journalisten und Dissidenten bis hin zu direkten Angriffen auf Regierungs- und Militäreinrichtungen.**

Die Bedrohungsakteure nutzen dabei sowohl neue Tools und Techniken als auch Modifizierungen bestehender Tools, um eine Entdeckung zu vermeiden. Die Zunahme gezielter Angriffe auf die Automobilindustrie, das Gesundheits- und Finanzwesen verdeutlicht einmal mehr, dass diese Branchen besonders gefährdet sind und daher auch besonderen Schutz benötigen.

Um Ihr Unternehmen vor Malware und Cyberangriffen zu schützen, müssen Sie die Tools und Motive der Bedrohungsakteure kennen. Dieses Wissen liefert Ihnen kontextbezogene, vorausschauende und umsetzbare Informationen über Cyberbedrohungen, mit denen Sie die Auswirkungen von Bedrohungen auf Ihr Unternehmen verringern können.

## LESSONS LEARNED/ERKENNTNISSE

- Bedrohungsakteure haben verstärkt Einzelpersonen und Institutionen im Visier. Denn neben Geld spielen auch gesamtwirtschaftliche, geopolitische und gesellschaftliche Gründe eine entscheidende Rolle bei der Auswahl der Opfer. Darauf müssen sich die Verteidiger einstellen und dies proaktiv bei ihrer Cybersicherheit berücksichtigen.
- Bei der Entwicklung neuer Malware werden zunehmend weniger verbreitete oder exotische Programmiersprachen wie GoLang und Rust verwendet. Darauf müssen sich die Threat Hunter einstellen und lernen, wie sich dies auf die Angriffe auswirkt. In Zukunft könnten mehr Angriffe auf Linux und macOS erfolgen, da GoLang plattformübergreifende Kodierung unterstützt.
- Nationalstaatliche Akteure nutzen verstärkt Ransomware. Das liegt am breiteren Zugang zu diesen Tools und an der Verfügbarkeit von Ransomware-as-a-Service. Damit können auch technisch unerfahrene Gruppen schwere Vorfälle auslösen. So geschehen im letzten Jahr.
- Die Automobilindustrie war 2022 überdurchschnittlich häufig Opfer von Cyberangriffen. Die Kompromittierung großer Hersteller und Zulieferer führte zum Stillstand zahlreicher Produktionslinien. Diese Entwicklung wird sich 2023 wahrscheinlich fortsetzen.
- Angriffe auf die Lieferkette durch die Ausnutzung legitimierter Apps lassen sich reduzieren. Und zwar durch die Implementierung von Zero-Trust-Richtlinien, die eine kontinuierliche Authentifizierung und Autorisierung für den Zugriff auf Netzwerke und Anwendungen erfordern.

## VORSCHAU AUF DAS 1. QUARTAL 2023

- Zu den zentralen Merkmalen des russischen Überfalls auf die Ukraine gehören Cyberangriffe gegen die militärische und zivile Infrastruktur. Solange der Krieg andauert, werden wir wahrscheinlich noch weitere solcher Cyberangriffe beobachten können.
- Auch Ransomware-Attacken auf Krankenhäuser und medizinische Einrichtungen werden sich fortsetzen. Schwerpunktmäßig in Ländern, die die Ukraine unterstützen oder fördern.
- Die kritische Infrastruktur wird ebenfalls weiterhin zu den Opfern von Cyberattacken gehören. KI wird dabei zunehmend genutzt für die Automatisierung, aber auch für die Entwicklung von Deepfake-Angriffen.
- Angriffe auf europäische Finanzinstitutionen wird es auch weiterhin geben. So wie im September 2022 auf das britische Fintech-Unternehmen Revolut und seine App, bei dem mehr als 50.000 Datensätze von Kunden gestohlen wurden.
- In Nord- und Südamerika erwarten wir eine explosionsartige Zunahme von Spyware-Angriffen auf Mobilgeräte. Speziell Bedrohungsakteure in Brasilien werden ihre Trojaner-Angriffe auf Banken von Desktops auf Mobilgeräte verlagern und damit Opfer in Lateinamerika angreifen. Bereits im Dezember 2022 wurde die Banking-Malware BrasDex[39] entdeckt, die sich noch auf Ziele in Brasilien konzentriert wie beispielsweise PIX, ein Bezahlsystem vergleichbar mit Zelle in den USA.
- Angriffe auf Linux-Systeme könnten nach wie vor unter dem Radar fliegen. Insbesondere solche, die Systeme virtualisieren, Ransomware einschleusen und Backdoors auf Zielsystemen installieren.
- Wir erwarten mehr gezielte Attacken auf Cloud-Infrastrukturen in allen Branchen. Der Grund dafür ist, dass Bedrohungsakteure noch mehr über die Unternehmen erfahren wollen, die sie angreifen.

# RESSOURCEN

Folgende BlackBerry Threat Research and Intelligence Ressourcen sind verfügbar.

## ÖFFENTLICHE INDICATORS OF COMPROMISE (IOCS)

Das BlackBerry Threat Research and Intelligence Team veröffentlicht die Indicators of Compromise (IoCs) der analysierten Kampagnen in unserem öffentlichen GitHub Repository. Alle IoCs und andere umsetzbare Informationen aus unseren Threat Reports, Blogs und Whitepaper (wie YARA oder Sigma Rules) finden Sie im BlackBerry Threat Research & Intelligence Team Public GitHub.

## ÖFFENLICHE REGELN

Das BlackBerry Threat Research and Intelligence Team hat YARA-Regeln verfasst, um viele der in diesem Report besprochenen Bedrohungen zu identifizieren. Sie finden unsere öffentlich verfügbaren YARA-Regeln hier.

## GÄNGIGE MITRE-TECHNIKEN

Das BlackBerry Threat Research and Intelligence Team stützt sich auf mehrere MITRE-Techniken, Ereignisanalyse und Telemetrie zur Analyse von Bedrohungen. Eine vollständige Liste der MITRE-Techniken befindet sich im MITRE ATT&CK Navigator Layer, der vom BlackBerry Team erstellt wurde.

## MITRE D3FEND ABWEHRMASSNAHMEN

Eine vollständige Liste von Angriffstechniken und zugehörigen Abwehrmaßnahmen finden Sie im Blogs and Reports Bereich unseres GitHub Repository.

# QUELLEN


1 https://www.uber.com/newsroom/security-update/

2 https://www.computerworld.com/article/3604601/macs-reach-23-share-in-us-enterprises-idc-confirms.html

3 https://www.developer.com/news/90-of-the-public-cloud-runs-on-linux/

4 https://sysdig.com/blog/malware-analysis-shellbot-sysdig/

5 https://threatpost.com/sysrv-k-botnet-targets-windows-linux/179646/

6 https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-22947

7 https://yoroi.company/research/outlaw-is-back-a-new-crypto-botnet-targets-european-organizations/

8 https://sandflysecurity.com/blog/log4j-kinsing-linux-malware-in-the-wild/

9 https://cve.mitre.org/cgi-bin/cvename.cgi?name=cve-2021-44228

10 https://cyware.com/news/kinsing-operators-target-weblogic-servers-and-docker-apis-for-cryptomining-5ce39d4b

11 https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-14882

12 https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-26134

13 https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-2725

14 https://twitter.com/MsftSecIntel/status/1542281836742729733

15 https://www.statista.com/statistics/272698/global-market-share-held-by-mobile-operating-systems-since-2009

16 https://www.reuters.com/business/autos-transportation/continental-investigates-cyberattack-after-report-says-data-up-sale-2022-11-15/

17 https://www.juniperresearch.com/press/in-vehicle-commerce-opportunities-exceed-775mn

18 https://www.lv.com/insurance/press/keyless-technology-drives-rise-in-theft-over-past-four-years

19 https://www.europol.europa.eu/media-press/newsroom/news/31-arrested-for-stealing-cars-hacking-keyless-tech

20 https://www.bbc.com/news/uk-england-39906534

21 https://attack.mitre.org/groups/G0050/

22 https://resources.infosecinstitute.com/topic/biggest-data-breaches-of-2019-so-far/

23 https://www.zdnet.com/article/bmw-and-hyundai-hacked-by-vietnamese-hackers-report-claims/

24 https://www.zdnet.com/article/europes-biggest-car-dealer-hit-with-ransomware-attack/

25 https://www.broshuis.com/news/ransomware-attack

26 https://www.reuters.com/business/autos-transportation/japans-bridgestone-reports-ransomware-attack-us-subsidiary-2022-03-18/

27 https://europe.autonews.com/automakers/toyota-suspend-output-japan-after-supplier-hit-cyberattack

28 https://www.nhtsa.gov/press-releases/nhtsa-updates-cybersecurity-best-practices-new-vehicles

29 https://www.bleepingcomputer.com/news/security/commonspirit-health-ransomware-attack-exposed-data-of-623-000-patients/

30 https://www.cisa.gov/emergency-directive-21-02

31 https://asec.ahnlab.com/en/27346/

32 https://malpedia.caad.fkie.fraunhofer.de/details/elf.rekoobe

33 https://www.computerweekly.com/news/252525240/ALPHV-BlackCat-ransomware-family-becoming-more-dangerous

34 https://www.securitymagazine.com/articles/97489-blackcat-alphv-ransomware-breaches-60-organizations

35 https://attack.mitre.org/groups/G0129/

36 https://twitter.com/invimacolombia/status/1577455552954712064?s=20&t=JYJsQ6PFhxBv3YHim_PQrw

37 https://malpedia.caad.fkie.fraunhofer.de/actor/mummy_spider

38 https://www.bleepingcomputer.com/news/security/new-crywiper-data-wiper-targets-russian-courts-mayor-s-offices/

39 https://thehackernews.com/2022/12/beware-cybercriminals-launch-new.html

BlackBerry | Cybersecurity

***Über BlackBerry:*** 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 215 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.***



**Ausgabe Januar 2023**