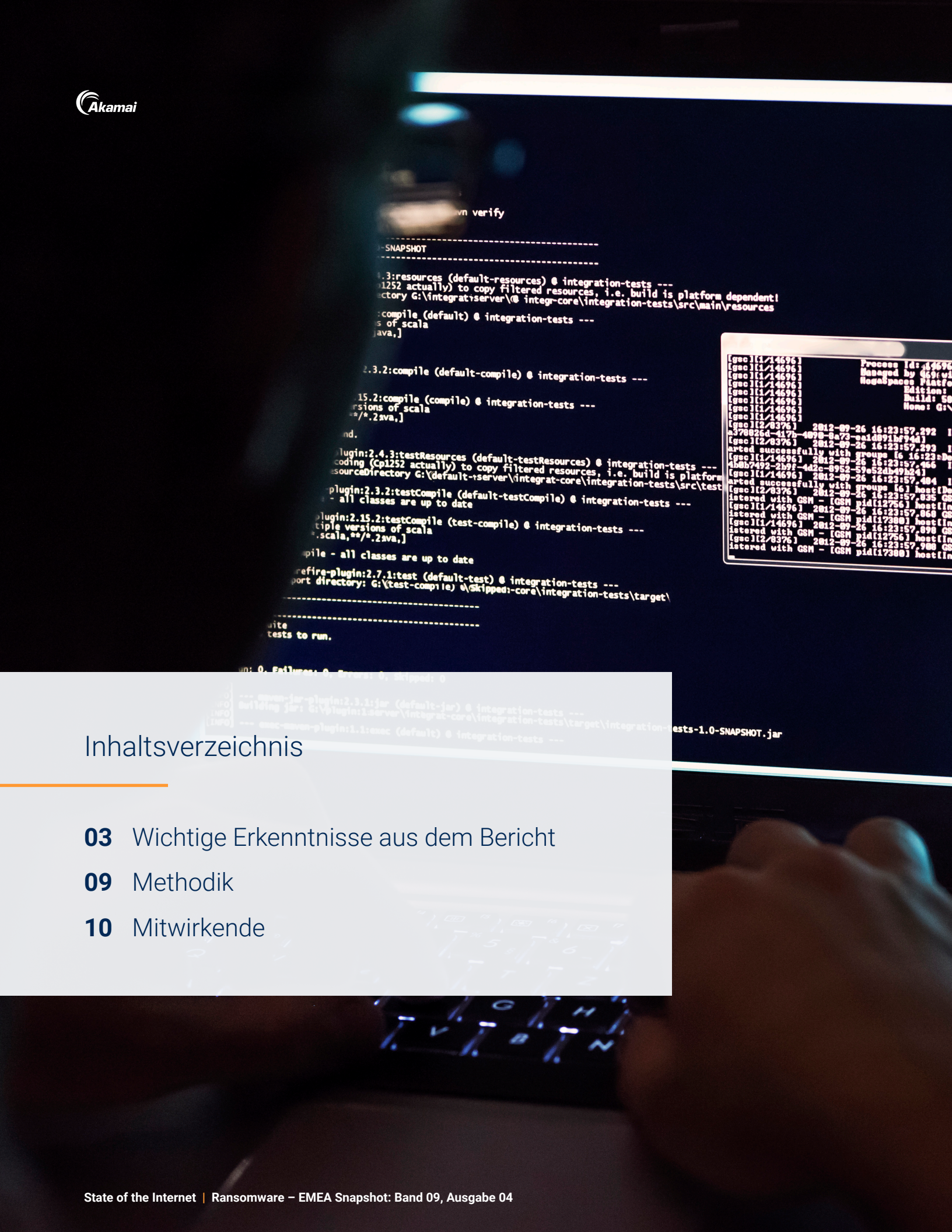
Akamai

„State of the Internet“
Band 09 | Ausgabe 04

Ransomware auf dem Vormarsch

EMEA Snapshot



Inhaltsverzeichnis

Wichtige Erkenntnisse aus dem Bericht

Der EMEA Snapshot ist eine Ergänzung zu unserem größeren SOTI-Bericht zu Ransomware: „Ransomware auf dem Vormarsch: Raffinierte Ausnutzungstechniken und Zero-Day-Angriffe“ (nur in englischer Sprache verfügbar). In diesem Bericht finden Sie detaillierte Analysen der Angriffstrends, Methoden und Techniken von Ransomware-Gruppen, eine Beschreibung der Angriffsphasen und der entsprechenden Lösungen und Empfehlungen zum Schutz Ihres Unternehmens sowie unsere Forschungsmethoden.

Übersicht

Ransomware hat weiterhin verheerende Auswirkungen auf Unternehmen und fordert weitere Opfer, da Angreifer ihre Vorgehensweise ständig weiterentwickeln und verändern, neue Erpressungsmethoden anwenden, eine wachsende Angriffsfläche nutzen und aus Beschränkungen des Budgets für die Sicherheit Kapital schlagen. Die Auswirkungen dieser gefährlichen Trends spiegeln sich in den Ransomware-Gruppen wider, die die Bedrohungslandschaft dominieren, und in ihrem wachsenden Erfolg. In der EMEA-Region zeigt sich dies durch ein Wachstum von 18 % zwischen dem 4. Quartal 2021 und dem 4. Quartal 2022 bei den Unternehmen, die Opfer eines Angriffs geworden sind, wobei die Zahl im Vergleich zwischen dem 1. Quartal 2022 mit dem 1. Quartal 2023 einen Anstieg von 77 % innerhalb eines Jahres aufweist.

In diesem EMEA Snapshot präsentieren wir weitere Erkenntnisse für eine bessere Abwehr und ein besseres Risikomanagement bei diesem wachsenden Problem, darunter:

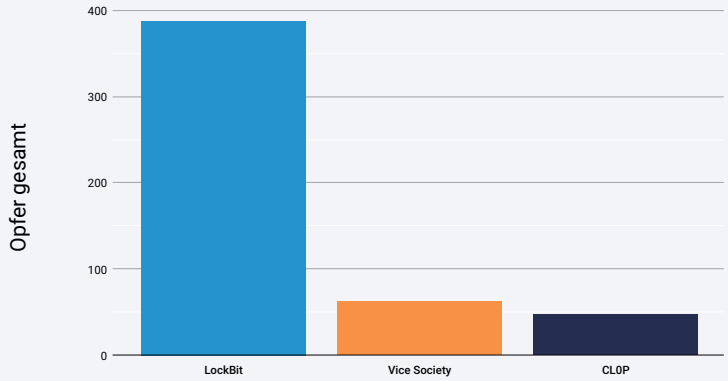
- In der Zeit von Oktober 2021 bis Mai 2023 dominierte LockBit die Ransomware-Szene, wobei CL0P an Bedeutung gewann, indem sie Schwachstellen aggressiv ausnutzte. Eine Veränderung der Angriffstechniken von Phishing hin zu einer zunehmenden Ausnutzung von Zero-Day- und One-Day-Schwachstellen führte zu einer erheblichen Zunahme der Zahl der Opfer.
- Wie auch im Rest der Welt war die Fertigung die Branche mit der höchsten Anzahl an Unternehmen, die Opfer von Ransomware-Angriffen wurden, gefolgt von Unternehmensservices.
- Die Mehrheit der von Ransomware-Angriffen betroffenen Unternehmen waren kleinere Unternehmen mit einem Umsatz von bis zu 50 Millionen US-Dollar. Aber auch die größten Unternehmen wurden angegriffen.

LockBit für meiste Ransomware-Angriffe verantwortlich

Trotz des zunehmenden Bewusstseins für Ransomware und der Fülle an Tools und Best Practices zur Bekämpfung dieser Bedrohung, stieg die Zahl der Unternehmen, die Ransomware-Angriffen zum Opfer fielen, in EMEA zwischen Q4 2021 und Q4 2022 um 18 %. Im Jahresvergleich zwischen Q1 2022 und Q1 2023 wird ein Anstieg von 77 % bei der Anzahl der Opfer verzeichnet. LockBit war zwischen dem 01. Oktober 2021 und dem 31. Mai 2023 für die meisten Angriffe verantwortlich – 45 % davon fanden in der Region EMEA statt. Dies deckt sich mit den Daten in unserem globalen Bericht. In EMEA verdrängt Vice Society jedoch ALPHV als zweitaktivste Gruppe. CL0P ist nach wie vor die drittaktivste Gruppe (EMEA-Abbildung 1).

EMEA: Top 3 der Ransomware-Gruppen nach Anzahl geschädigter Unternehmen

1. Oktober 2021 bis 31. Mai 2023



EMEA-Abb. 1: Der Großteil der Unternehmen, die in der Region EMEA Opfer von Ransomware-Angriffen wurden, wurden von LockBit, Vice Society und CL0P attackiert.

Quartalsanalyse

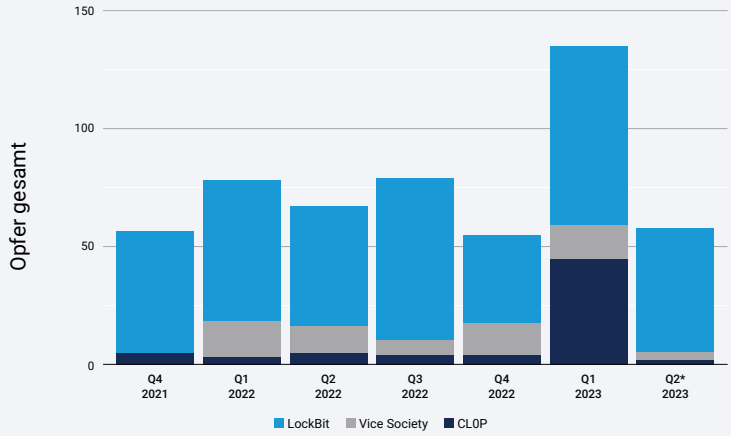
Wenn wir uns die Anzahl der Opfer nach Ransomware-Gruppe ansehen (EMEA-Abbildung 2), dominiert LockBit nach wie vor. Die konstante Präsenz der Vice Society lässt sich vermutlich auf die Tatsache zurückführen, dass das Bildungswesen eine der in EMEA am meisten von Ransomware-Angriffen betroffenen Branchen ist (siehe EMEA-Abbildung 3) und Vice Society als Ransomware-as-a-service unverhältnismäßig stark die Bildungsbranche attackiert. Wie wir auch in den globalen Datentrends sehen können, nehmen Angriffe durch CL0P in der Ransomware-Landschaft in EMEA jedoch zu. Der Anstieg in Q1 2023 kann auf die Ausnutzung einer Vielzahl von Zero-Day-Schwachstellen als Einstiegspunkt zurückgeführt werden. Durch den Wandel der Angriffstechniken in den letzten sechs Monaten – von Phishing hin zu einem rasanten Missbrauch von Schwachstellen – steigen die Opferzahlen. Zum Zeitpunkt dieses Berichts lagen

** Das 2. Quartal 2023 ist kein vollständiges Quartal, da die Daten nur bis 31. Mai 2023 vorliegen.*

jedoch nur unvollständige Daten für Q2 2023* vor. Am 31. Mai 2023 erreichte die Aktivität von CL0P wieder das Niveau von 2022. Auch wenn wir nicht endgültig sagen können, was das Quartal letztendlich für uns bereithalten wird, müssen wir darauf hinweisen, dass CL0P im Juni 2023 die Namen weiterer Firmen veröffentlichte, die in EMEA als Folge der Ausnutzung der MOVEit-Schwachstelle einem Ransomware-Angriff zum Opfer fielen. Wir gehen daher davon aus, dass die Zahl der Opfer noch steigen wird.

EMEA: Top 3 der Ransomware-Gruppen nach Anzahl geschädigter Unternehmen

Vierteljährlich: 1. Oktober 2021 bis 31. Mai 2023



EMEA-Abb. 2: Ein Vergleich der vierteljährlichen Anzahl von Opfern der drei verbreitetsten Ransomware-Gruppen in EMEA: LockBit, Vice Society und CL0P

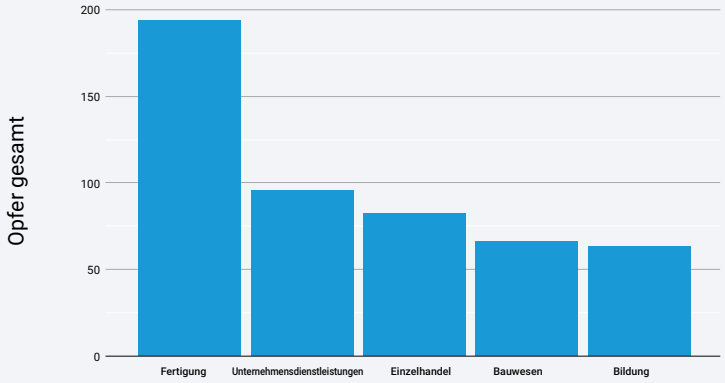
Kritische Branchen in Gefahr

Die fünf kritischen Branchen, die in EMEA am stärksten von Ransomware-Angriffen betroffen sind, sind Fertigung, Unternehmensservices, Einzelhandel, Baugewerbe und Bildungswesen (EMEA-Abbildung 3). Dies entspricht auch dem weltweiten Vergleich und steht im Einklang mit dem globalen Ransomware-Bericht von 2022, in dem Fertigung und Unternehmensservices die vordersten Plätze einnahmen. Zur Zeit dieses Berichts wurden diese Opfer von Conti-Ransomware. Nach dem Verschwinden von Conti übernahm die LockBit-Gruppe deren Stellung. Es zeigt sich zudem eine erhebliche Überschneidung mit den fünf am häufigsten betroffenen Branchen aus unserem vorherigen DNS-Bericht: „Angriffe über die Datenautobahn: Ein detaillierter Blick auf schädlichen DNS-Traffic“. Es besteht eine klare Verbindung zwischen schädlichem „Command and Control“-Traffic (C2) und Ransomware-Angriffen.

** Das 2. Quartal 2023 ist kein vollständiges Quartal, da die Daten nur bis 31. Mai 2023 vorliegen.*

EMEA: Top 5 Branchen nach Zahl der durch Ransomware-Gruppen geschädigten Opfer

1. Oktober 2021 bis 31. Mai 2023



EMEA-Abb. 3: Die Fertigung ist in EMEA die Branche mit der höchsten Anzahl an Unternehmen, die Opfer von Ransomware-Angriffen werden

Es ist auch wichtig zu beachten, dass LockBit die am weitesten verbreitete Ransomware in jeder der vier führenden Branchen in der Region EMEA ist. Auf sie entfallen 45,9 % der Angriffe in der Fertigung, 45,4 % in Unternehmensservices, 45,1 % im Einzelhandel und 53,6 % im Baugewerbe. Das Bildungswesen ist die Ausnahme: in dieser Branche ist Vice Society für die meisten Angriffe verantwortlich (36,5 %) und LockBit für 22,2 % der Angriffe.

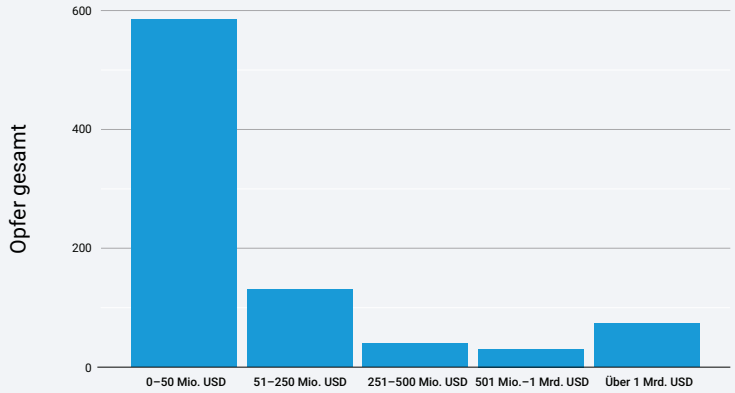
> Jedes Unternehmen ist unabhängig von Größe oder Umsatz dem Risiko von Ransomware-Angriffen ausgesetzt.

Ransomware-Gruppen konzentrieren sich auf den ROI

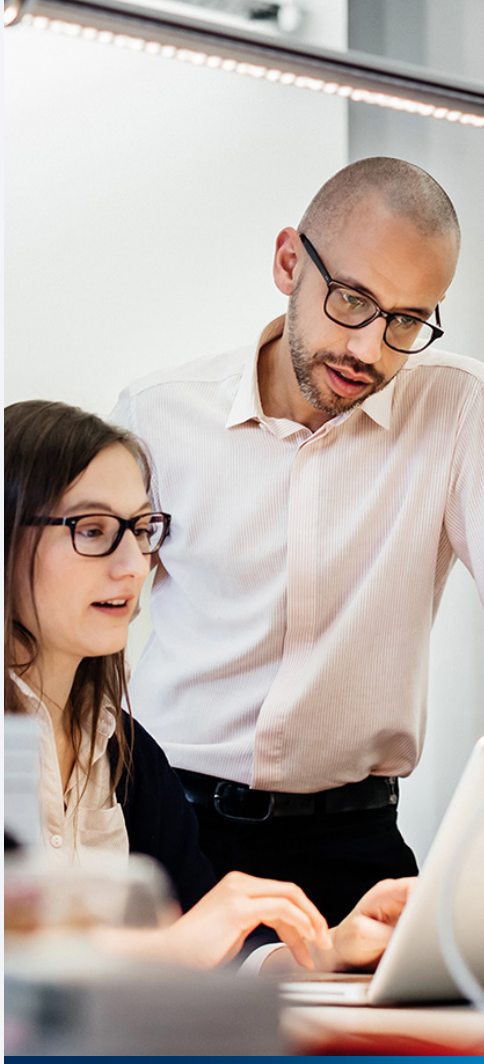
Jedes Unternehmen ist unabhängig von Größe oder Umsatz dem Risiko von Ransomware-Angriffen ausgesetzt. Unsere Daten spiegeln jedoch auch den weltweiten Trend wider – Angreifer starten erfolgreiche Angriffe auf kleinere Unternehmen in EMEA (EMEA-Abbildung 4). Kleinere Unternehmen verfügen möglicherweise über weniger Sicherheitsressourcen, um die Gefahren von Ransomware zu bekämpfen, wodurch sie anfälliger und leichter zu infiltrieren sind. Dennoch sind sie in der Lage, Lösegelder zu zahlen. Allerdings werden auch die größten Unternehmen angegriffen. Studien zeigen, dass die Höhe der Lösegeldforderung auf der Höhe des Umsatzes des betroffenen Unternehmens basiert – je höher der Umsatz, desto höher die Forderung.

EMEA: Anzahl der durch Ransomware-Gruppen geschädigten Opfer nach Umsatz

1. Oktober 2021 bis 31. Mai 2023



EMEA-Abb. 4: Die Mehrheit der Ransomware-Opfer in EMEA sind Unternehmen mit einem Umsatz von bis zu 50 Millionen US-Dollar



Zusammenfassung des EMEA Snapshots

Ransomware hat weiterhin verheerende Auswirkungen auf Unternehmen. Auf weltweiter sowie auf regionaler Ebene bilden Regierungsbehörden eine geschlossene Front, um diese Bedrohung anzugehen, Techniken zu vermitteln und Abwehrspezialisten so beim Schutz ihrer Unternehmen und dem Aufbau von Resilienz zu unterstützen. Die neue Richtlinie über Netz- und Informationssysteme (NIS2) der ENISA – der Agentur der Europäischen Union für Cybersicherheit – zielt darauf ab, die Cybersicherheit in der gesamten EU zu verbessern und umfasst auch neue Aufgaben wie der Einrichtung eines Registers von Schwachstellen. Auch Länder außerhalb der EU führen ihre eigenen Kontrollen ein, wie etwa die National Cybersecurity Authority (NCA) Saudi-Arabiens.

Vor dem Hintergrund der Einführung von Initiativen und Richtlinien zur Stärkung der Cybersicherheitsstandards durch Regierungsbehörden ist es wichtig, dass Sie die Meldepflichten für Ihren Bereich kennen und diese in Ihr Playbook bzw. Ihren Krisenmanagementplan aufnehmen. Zudem müssen Sie sich der Möglichkeiten zur Risikominimierung bewusst sein, die Ihnen durch die Nutzung einer mehrschichtige Sicherheitsarchitektur zur Verfügung stehen.

Weitere Informationen finden Sie im globalen SOTI-Bericht zu Ransomware: „Ransomware auf dem Vormarsch: Raffinierte Ausnutzungstechniken und Zero-Day-Angriffe“.

Methodik

Ransomware-Daten

Die Ransomware-Daten, die in diesem Bericht verwendet wurden, wurden auf den Leak-Websites von etwa 90 verschiedenen Ransomware-Gruppen erfasst. Es ist typisch für diese Gruppen, Details ihrer Angriffe zu veröffentlichen, wie z. B. Zeitstempel, Namen und Domains der Opfer. Dabei ist jedoch zu beachten, dass diese Angaben davon abhängen, was die einzelnen Ransomware-Gruppen veröffentlichen möchten. Ob diese veröffentlichten Angriffe erfolgreich waren, wurde in dieser Studie nicht berücksichtigt.

Diese Untersuchung konzentrierte sich stattdessen auf die gemeldeten Opfer. Für jede Analyse wurde die Anzahl der einzelnen Opfer innerhalb jeder Gruppe gemessen. Diese Daten zu den Opfern wurden mit Daten von ZoomInfo kombiniert, um zusätzliche Details zu jedem Opfer, wie Standort, Umsatzbereich und Branche, zu erhalten.

Alle Daten wurden in einem Zeitraum von 20 Monaten zwischen dem 1. Oktober 2021 und dem 31. Mai 2023 erfasst.

Mitwirkende

Redaktion und Text

Ori David
Badette Tribbey
Charlotte Pelliccia
Lance Rhodes

Prüfung und Fachleute

Moshe Cohen
Shiran Guez
Ophir Harpaz
Reuben Koh
Richard Meeus
Steve Winterfeld
Maxim Zavodchik

Datenanalyse

Chelsea Tuttle

Marketing und Veröffentlichung

Kimberly Gomez
Georgina Morales Hampe
Shivangi Sahu

Weitere „State of the Internet“-Sicherheitsberichte

Lesen Sie vorherige Ausgaben und informieren Sie sich über bevorstehende Veröffentlichungen der renommierten „State of the Internet“-Sicherheitsberichte von Akamai unter **akamai.com/soti**

Weitere Informationen zur Bedrohungsforschung von Akamai

Halten Sie sich unter diesem Link zu neuesten Threat-Intelligence-Analysen, Sicherheitsberichten und Cybersicherheitsforschung auf dem Laufenden: **akamai.com/security-research**

Akamai-Daten aus diesem Bericht

Sehen Sie sich die hochauflösenden Versionen der Diagramme und Grafiken an, auf die in diesem Bericht verwiesen wird. Diese Bilder können kostenlos verwendet und referenziert werden, vorausgesetzt, Akamai wird ordnungsgemäß als Quelle genannt und das Akamai-Logo wird beibehalten. **akamai.com/sotidata**

Weitere Informationen zu Akamai-Lösungen

Weitere Informationen zu Akamai-Lösungen zum Schutz vor Ransomware finden Sie auf unserer Seite zu **Sicherheitslösungen**.

Akamai unterstützt und schützt das digitale Leben. Führende Unternehmen weltweit setzen bei der Erstellung, Bereitstellung und beim Schutz ihrer digitalen Erlebnisse auf Akamai. So unterstützen wir täglich Milliarden von Menschen in ihrem Alltag, bei der Arbeit und in ihrer Freizeit. Akamai Connected Cloud, eine stark verteilte Edge- und Cloud-Plattform, bringt Anwendungen und Erlebnisse näher an die Nutzer und hält Bedrohungen fern. Möchten Sie mehr über die Cloud-Computing-, Sicherheits-, und Inhaltsbereitstellungslösungen von Akamai erfahren? Dann besuchen Sie uns unter akamai.com und akamai.com/blog oder folgen Sie Akamai Technologies auf Twitter und LinkedIn. Veröffentlicht: 08/23.