Ransomware-Report 2025 von ThreatLabz



© 2025 Zscaler, Inc. Alle Rechte vorbehalten.

Inhaltsverzeichnis



Kurzfassung 3

Die wichtigsten Ergebnisse im Überblick 4

Bedrohungslage durch Ransomware: Wichtige Trends und Angriffsziele 6

- Ransomware-Angriffe erreichen neuen Höchststand 6
- Starker Aufwärtstrend bei Datenexfiltrationen 7
- Am stärksten betroffene Branchen 9
- Globale und regionale Hotspots 11
- Aktivste Ransomware-Gruppen in den Jahren 2024/25 14
- Neue Ransomware-Gruppen 15
- Wichtige Schwachstellen, die bei Ransomware-Kampagnen ausgenutzt werden 16

Ransomware-Vorfälle in den Schlagzeilen 17

- Black Basta nutzt ChatGPT für kriminelle Aktivitäten 17
- Das Ransomware-Playbook für mehrstufige Angriffe18 18
- RaaS-Mechanismen bei Dark-Web-Datenleck aufgedeckt 20
- Das Gesundheitswesen im Visier von Ransomware-Akteuren 22
- Die Wende im Kampf gegen Ransomware 23

Die 5 gefährlichsten Ransomware-Gruppen 2025/26 24

- 1. Dark Angels 24
- 2. Clop/ClOp 25
- 3. DragonForce 26
- 4. Akira 26
- 5. Interlock 27

Ransomware-Archiv von ThreatLabz 28

Prognosen für 2026 29

Zero Trust + KI: Die Zscaler-Lösung zum Schutz vor Ransomware 31

Checkliste zur Ransomware-Prävention 33

Forschungsmethodik 35

- Über ThreatLabZ 35
- Über Zscaler 35

© 2025 Zscaler, Inc. Alle Rechte vorbehalten.

Kurzfassung

Ransomware ist seit langem eine Konstante in der Bedrohungslandschaft — doch die Techniken und Taktiken der Angreifer ändern sich ständig. Heutige Kampagnen sind stärker zielgerichtet, automatisiert und effizienter, was teilweise auf den zunehmenden Einsatz generativer KI zurückzuführen ist, die alle Schritte von Phishing-Ködern bis hin zur Entwicklung von Malware verbessert und beschleunigt. Diese Entwicklung hat zu einem deutlichen Anstieg der Ransomware-Aktivitäten und -Auswirkungen geführt.

Von April 2024 bis April 2025 blockierte die Zscaler-Cloud mehr Ransomware-Angriffe als in jedem anderen Jahr zuvor — insgesamt 10,8 Millionen. Dies entspricht einem Anstieg um 145,9 % im Vergleich zum Vorjahr. Gleichzeitig stieg die Anzahl der Unternehmen, die auf Ransomware-Leak-Websites gelistet waren, um 70,1 %. Dies unterstreicht eine allgemeine Verlagerung hin zu erpresserischen Angriffen. Heutige Kampagnen sind hochfrequent und darauf ausgelegt, eine maximale Wirkung zu erzielen, oft ohne dass eine Verschlüsselung erforderlich ist. Immer mehr Ransomware-Betreiber verzichten gänzlich auf Verschlüsselung und bevorzugen stattdessen reine Datenerpressung. Diese Entwicklung spiegelt sich in einem Anstieg des Datenexfiltrationsvolumens um 92,7 % im vergangenen Jahr wider.

Selbst bei spektakulären Angriffsinitiativen wie Operation Endgame zeigen Ransomware-Gruppen keine Anzeichen einer Verlangsamung. Wenn überhaupt, könnten Störungen die Neuerfindung vorantreiben. Während des Analysezeitraums für diesen Bericht sind 34 neue Ransomware-Gruppen aufgetaucht. Inzwischen kletterten etablierte Gruppen wie DragonForce, Akira und Clop an die Spitze der Aktivitätscharts und demonstrierten damit die Resilienz ausgereifter Ransomware-Operationen.

Der Ransomware-Report 2025 von Zscaler ThreatLabz geht tiefer auf diese Entwicklungen und Erkenntnisse ein und behandelt die am stärksten betroffenen Sektoren und Regionen, zu beobachtende Ransomware-Gruppen, neuartige Angriffsmethoden und umsetzbare Anleitungen für Verteidiger. Erfahren Sie, wie ThreatLabz über die Bedrohungsverfolgung hinaus eine aktive Rolle beim Schutz von Unternehmen weltweit spielt — von der Entwicklung benutzerdefinierter Tools zur Wiederherstellung nach Ransomware-Angriffen bis hin zur Beteiligung an globalen Bemühungen zur Aufdeckung und Störung groß angelegter Malware- und Ransomware-Ökosysteme.

© 2025 Zscaler, Inc. Alle Rechte vorbehalten.

Die wichtigsten Ergebnisse im Überblick

Die von der Zscaler-Cloud blockierten Ransomware-Versuche stiegen im Vergleich zum Vorjahr (April 2024—April 2025) um 145,9 % und stellten damit den stärksten Anstieg seit drei Jahren dar.

Das Volumen der exfiltrierten Daten der zehn größten Ransomware-Familien stieg im Vergleich zum Vorjahr um 92,7 % auf 238,5 Terabyte (TB) gestohlene Daten, was auf eine allgemeine Verlagerung hin zu Datendiebstahl als primäre Erpressungstaktik hindeutet.

Die Zahl der Erpressungsfälle in der Öffentlichkeit stieg laut einer Analyse von Dataleak-Websites um 70,1 %. Dies zeigt, dass die Gefahr eines Reputationsschadens oder regulatorischer Konsequenzen oft größer ist als die bloße Verschlüsselung.

Die am stärksten betroffenen Branchen waren Fertigung, Technologie und Gesundheitswesen. Im Öl- und Gassektor kam es zu einem Anstieg der Angriffe um 935,3 %.

© 2025 Zscaler, Inc. Alle Rechte vorbehalten.

Die USA bleiben das weltweit am stärksten betroffene Ziel, auf das 50,8 % aller Angriffe entfallen, gefolgt von Kanada, dem Vereinigten Königreich, Deutschland und Indien.

Generative KI wird für Akteure, die hinter Ransomware-Angriffen stecken, zu einem Wirkungsmultiplikator, da sie dabei hilft, schnell Phishing-Köder zu erstellen, Schadcode zu schreiben, die Datenextraktion zu automatisieren und vieles mehr.

RansomHub (833), Akira (520) und Clop (488) erwiesen sich als die aktivsten Ransomware-Familien und waren gemeinsam für die Mehrheit der Angriffe verantwortlich.

Vishing (sprachbasiertes Phishing) wird zunehmend in Ransomware-Angriffe integriert.

ThreatLabz hat während des Analysezeitraums 34 neue aktive Ransomware-Gruppen identifiziert, sodass sich die Gesamtzahl der seit Beginn unserer Untersuchung beobachteten Ransomware-Gruppen auf 425 erhöht.

Trotz zunehmender Ransomware-Aktivitäten haben koordinierte Strafverfolgungsmaßnahmen — unterstützt von Branchenexperten wie Zscaler ThreatLabz — bedeutende Fortschritte bei der Störung wichtiger Ransomware-Infrastrukturen erzielt, wie die Operation Endgame zeigt.

© 2025 Zscaler, Inc. Alle Rechte vorbehalten.

Bedrohungslage durch Ransomware: Wichtige Trends und Angriffsziele

Während schlagzeilenträchtige Sicherheitsverletzungen das globale Ausmaß von Ransomware veranschaulichen, lassen sich die wertvollsten Erkenntnisse aus der Analyse der Zielmuster und operativen Verhaltensweisen gewinnen, die die Bedrohungsakteure in ihren Kampagnen anwenden.

In diesem Abschnitt wird untersucht, wo Ransomware die größten Auswirkungen hat (nach Branche und Region) und welche Ransomware-Gruppen am aktivsten sind. Außerdem wird die Entstehung neuer Gruppen im letzten Jahr beleuchtet.

Ransomware-Angriffe erreichen neuen Höchststand

Das stetige Wachstum der Ransomware-Aktivitäten ist nicht mehr überraschend. Die aktuellen Daten zeigen wieder einen dramatischen Anstieg des Angriffsvolumens: Die Zahl der versuchten Ransomware-Angriffe in der Zscaler-Cloud ist im Vergleich zum Vorjahr um 145,9 % gestiegen — und seit 2021 um das Sechsfache. Dieser Anstieg spiegelt mehr als nur ein höheres Volumen wider; er signalisiert eine Verlagerung hin zu schnelleren, gezielteren Kampagnen, die auf Umgebungen mit hohem Schadenspotenzial abzielen.

Sicherheitsteams sind mit den Taktiken von Ransomware zwar weitgehend vertraut. Die zunehmende Verbreitung, Präzision und operative Effizienz der jüngsten Kampagnen deutet jedoch auf eine Weiterentwicklung hin, die teilweise durch GenAI vorangetrieben wird, die die Entwicklung von Ransomware zu einem ausgefeilteren und skalierbareren Geschäftsmodell für Cyberkriminelle beschleunigt.

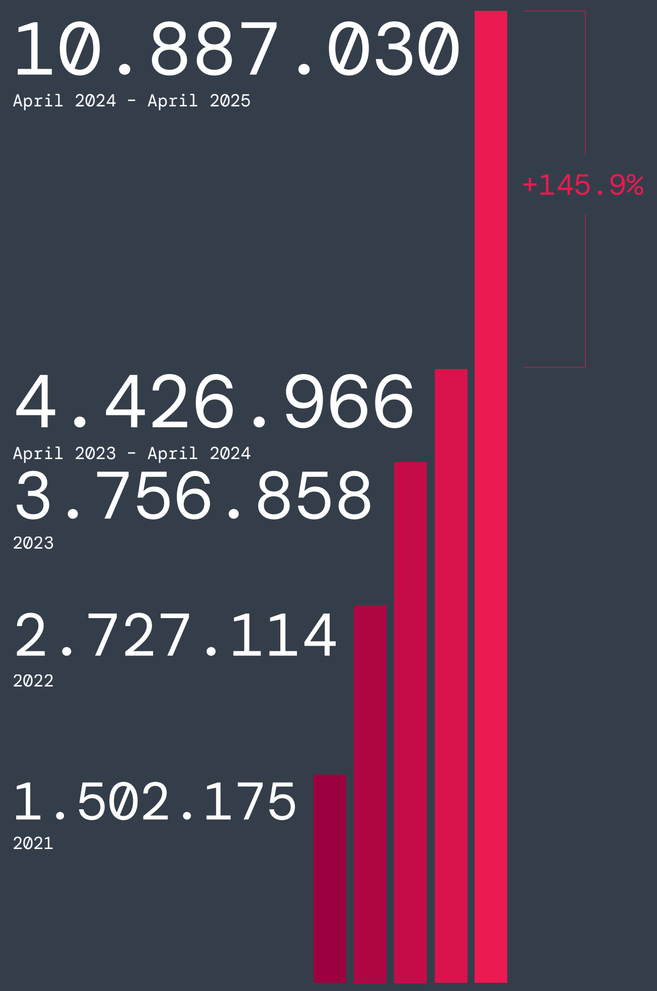


Abb.1: Von Zscaler jährlich blockierte Ransomware-Angriffe



© 2025 Zscaler, Inc. Alle Rechte vorbehalten.



Starker Aufwärtstrend bei Datenexfiltrationen

Im letzten Jahr haben Ransomware-Gruppen den Datendiebstahl von einer Nebenhandlung zum Hauptereignis gemacht. Immer häufiger ist die Verschlüsselung allein nicht mehr das Endziel. Bedrohungsakteure exfiltrieren riesige Datenmengen, um den Druck zu verstärken und die Risiken für die Opfer zu erhöhen.

Ein Anstieg der Datenexfiltrationen in letzter Zeit spiegelt diesen Trend wider. Die Analyse von ThreatLabz zeigt, dass das Gesamtvolumen der gestohlenen Daten bei den zehn größten Ransomware-Gruppen im Vergleich zum Vorjahr zugenommen hat. Das Gesamtvolumen der von diesen Gruppen exfiltrierten Daten stieg um 92,7 %, von 123,8 TB (April 2023—März 2024) auf 238,5 TB (April 2024—März 2025). Nicht berücksichtigt wurde ein einzelner Verstoß im Zeitraum 2023—2024, bei dem 100 TB an Daten exfiltriert wurden — die größte Exfiltration, die im gesamten Datensatz beobachtet wurde —, was die jährliche Gesamtsumme stark verzerrt. Durch Entfernen dieses statistischen Ausreißers wird ein genauerer Überblick über allgemeinere Trends bei Datendiebstahlaktivitäten möglich.

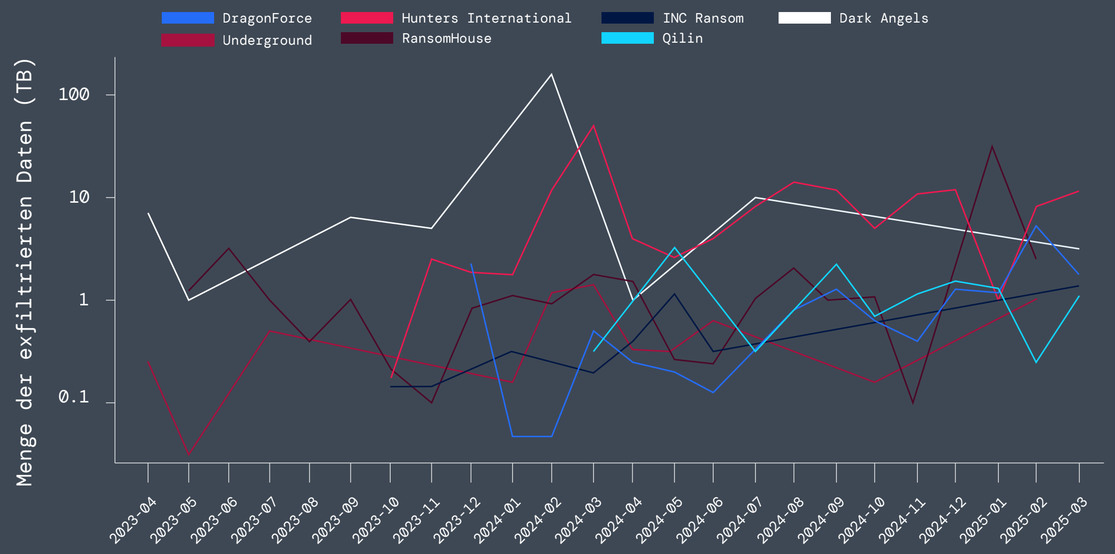


Abb. 2: Datenexfiltration durch die größten Ransomware-Gruppen

- **Hunters International** erhöhte die Gesamtzahl der gestohlenen Daten im Vergleich zum Vorjahr um 224,3 % von 37,7 TB auf 122,1 TB. Der durchschnittliche Datenverlust pro Opfer stieg ebenfalls von etwa 300 GB auf 359 GB, was einem Anstieg von 19,6 % pro Opfer entspricht. Der nächste Abschnitt („Verlagerung zur reinen Datenerpressung“) untersucht, wie die Gruppe beschloss, vollständig auf die Dateiverschlüsselung zu verzichten.
- **DragonForce** verzeichnete den größten prozentualen Anstieg des gesamten Exfiltrationsvolumens, nämlich um 382,6 % von 4,2 TB auf 20,3 TB. Obwohl der Mittelwert mit einem leichten Rückgang weitgehend stabil blieb, deutet der Anstieg des Gesamtvolumens darauf hin, dass die Gruppe mehr Opfer kompromittiert hat.
- **Dark Angels** hatte den höchsten durchschnittlichen Schaden pro Opfer: ein Anstieg um 132,6 % von 2,15 TB auf 5 TB. Dies steht im Einklang mit der anhaltenden Konzentration der Gruppe auf große, prominente Ziele, obwohl es insgesamt weniger Vorfälle gab.
- **RansomHub** hat im Vergleich zum Vorjahr 86,2 % mehr Daten exfiltriert, insgesamt 22,4 TB von April 2024 bis März 2025. Der durchschnittliche Datenverlust der Gruppe pro Opfer hat sich von 50 GB auf 118 GB mehr als verdoppelt.
- **RansomHouse** teigerte das gestohlene Datenvolumen im Vergleich zum Vorjahr um 83,1 % von 17,2 TB auf 31,6 TB. Der durchschnittliche Datenverlust pro Opfer stieg ebenfalls von 425 GB auf 500 GB.

© 2025 Zscaler, Inc. Alle Rechte vorbehalten.

Verlagerung zur reinen Datenerpressung

Im Ransomware-Report 2024 untersuchte Zscaler ThreatLabz, wie sich die Hive-Ransomware-Gruppe im Oktober 2023 in Hunters International umbenannte, nachdem im Rahmen eines vom FBI geführten Einsatzes Anfang des Jahres die Infrastruktur der Gruppe beschlagnahmt worden war. Seit der Gründung von Hunters International ist die Gruppe sehr aktiv und konzentriert sich stark auf Datendiebstahl statt auf Verschlüsselung. Insgesamt hat die Gruppe seit ihrer Gründung fast 160 TB an Daten gestohlen. Jedes Opfer von Hunters International verlor durchschnittlich 698 GB, der mittlere Datenverlust lag bei 317 GB. Abbildung 3 zeigt die Menge der seit der Gründung der Gruppe pro Monat gestohlenen Daten.

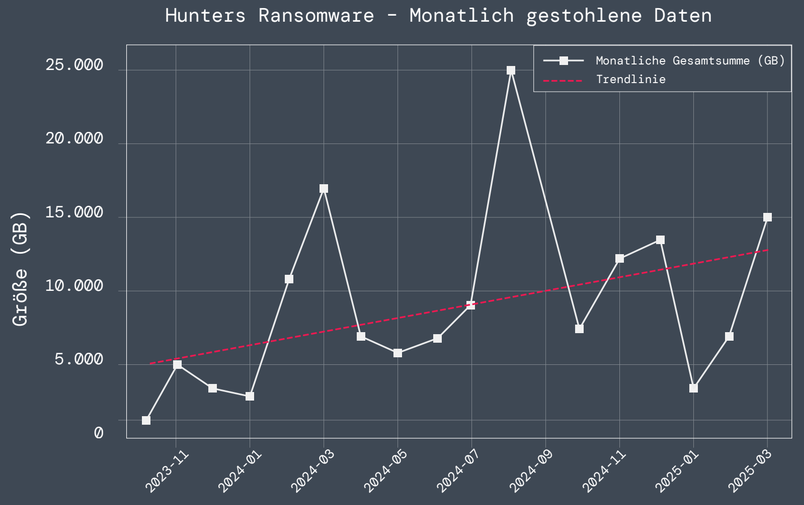


Abb. 3: Datenmenge (in GB), die pro Monat von Hunters International gestohlen wurde

Im Mai 2025 tauchte unter dem Namen World Leaks eine neue Gruppe auf, die Angriffe startete, ohne Ransomware einzusetzen, sondern sich stattdessen ausschließlich auf die Erpressung mit gestohlenen Daten konzentrierte. Die Website von World Leaks weist optisch und programmatisch Ähnlichkeiten mit Hunters International auf (siehe Abbildung 4), was darauf hindeutet, dass hinter beiden wahrscheinlich dieselbe Gruppe steckt.

Seit World Leaks im Mai 2025 mit ihren Angriffen begann, hat die Gruppe mehr als 25 TB an Daten gestohlen. Die Statistiken zum Datendiebstahl ähneln stark denen von Hunters International. Jedes Opfer verliert durchschnittlich 769 GB, der Mittelwert liegt bei 452 GB.

Übrigens gab Hunters International am 3. Juli 2025 über eine Nachricht auf ihrer Leak-Website bekannt, die Gruppe würde ihren Betrieb einstellen und kostenlose Entschlüsselungstools bereitstellen (siehe Abbildung 5).

Dieser Wechsel von der Dateiverschlüsselung zum Datendiebstahl ist nicht beispiellos. Auch andere Gruppen wie BianLian und Clop haben sich von Ransomware abgewandt und setzen nun verstärkt auf Datenerpressung. Dieser Trend wird später in diesem Report noch genauer untersucht.

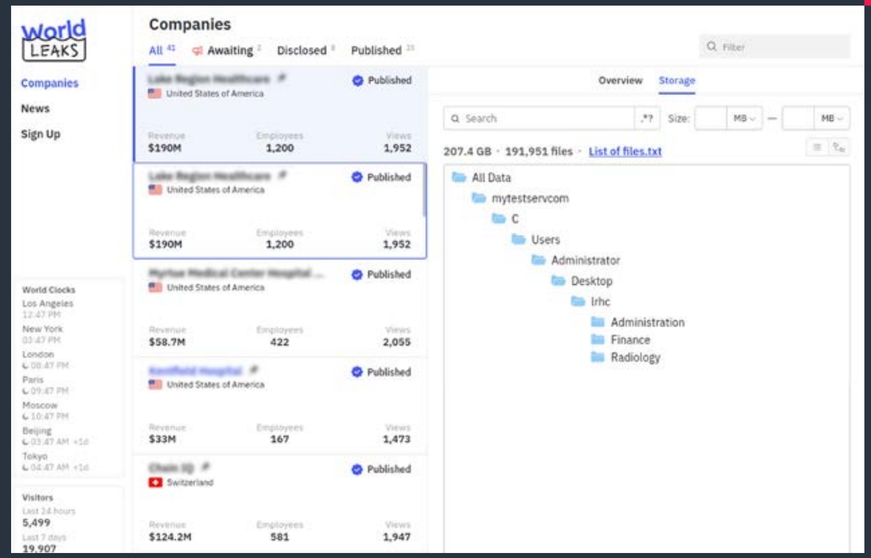


Abb. 4: Website der Ransomware-Gruppe World Leaks

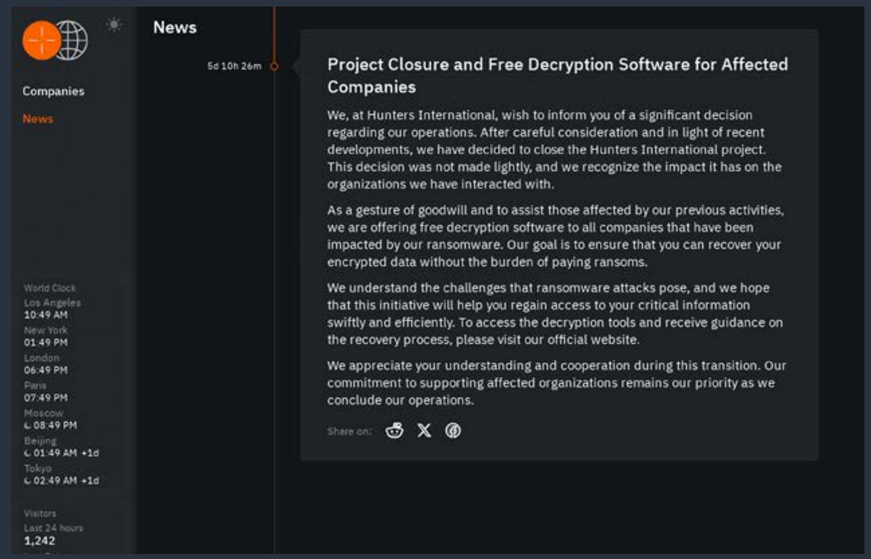


Abb. 5: Mitteilung über die Betriebseinstellung von Hunters International

© 2025 Zscaler, Inc. Alle Rechte vorbehalten.

Am stärksten betroffene Branchen

Die Angreifer konzentrierten sich weiterhin auf Branchen, in denen der Zahlungsdruck am höchsten ist — sei es aufgrund möglicher Betriebsstörungen, der Vertraulichkeit gestohlener Daten und der damit verbundenen potenziellen Reputationsschäden oder der rechtlichen Risiken.

Abbildung 6 zeigt die Anzahl der Ransomware-Vorfälle pro Branche basierend auf Daten von Leak-Websites und bietet eine Momentaufnahme bestätigter Angriffe, bei denen Bedrohungsakteure Daten exfiltrierten und Erpressungsdruck ausübten. Die am häufigsten angegriffenen Sektoren waren nach wie vor die Fertigung, die Technologie und das Gesundheitswesen.

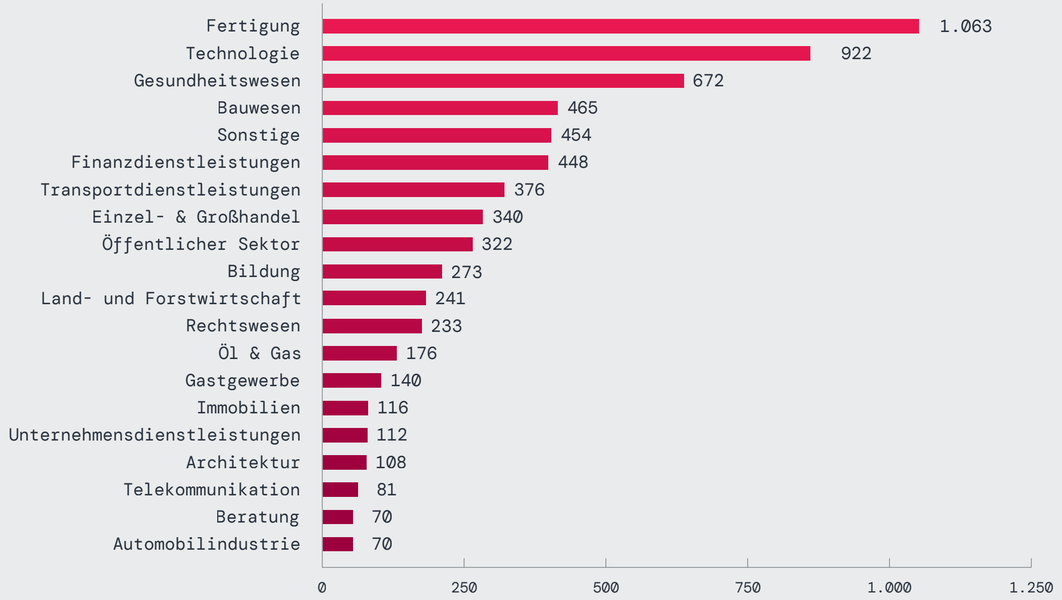


Abb. 6: Ransomware-Angriffe nach Branchen basierend auf Dataleak-Websites (Top 20 Branchen)



© 2025 Zscaler, Inc. Alle Rechte vorbehalten.

Trends im Jahresvergleich

Abbildung 7 zeigt die prozentualen Veränderungen der Ransomware-Angriffe im Jahresvergleich nach Branchen.

Ransomware-Angriffe auf den Öl- und Gassektor haben im Vergleich zum Vorjahr um mehr als 900 % zugenommen. Dies ist wahrscheinlich auf eine Kombination aus zunehmender Automatisierung — von Bohrinseln bis hin zu Pipelines —, die die Angriffsfläche vergrößert, und veralteten Sicherheitspraktiken zurückzuführen. Im Jahr 2025 warnte die Cybersecurity and Infrastructure Security Agency (CISA)[1], dass selbst „unerfahrene" Bedrohungsakteure Schwachstellen in industriellen Steuerungssystemen (ICS) und SCADA-Technologien ausnutzen, die für den Betrieb in der Öl- und Gasindustrie unerlässlich sind.

Auch im Agrarsektor kam es zu einem sprunghaften Anstieg der Ransomware-Angriffe um 677,4 %. Landwirtschaftliche Betriebe werden zunehmend digitalisiert (Stichwort intelligente Traktoren und IoT-fähige Sensoren), ohne entsprechende Sicherheitsvorkehrungen umzusetzen. Dennoch gibt es Anzeichen für Fortschritte und die Erkenntnis, dass landwirtschaftliche Systeme heute bevorzugte Ziele für Ransomware sind: John Deere schrieb 2025 einen Hackathon aus, bei dem Studierende aufgefordert wurden, Schwachstellen in den intelligenten Traktoren des führenden Landmaschinen-Herstellers aufzudecken.[2]

Das Gesundheitswesen zählt nach wie vor zu den am häufigsten und konsequentesten angegriffenen Bereichen. Die Angriffe haben dort gegenüber dem Vorjahr um 115,4 % zugenommen. Laut einem Bericht des HIPAA Journal[3] haben Forschende der Michigan State University, der Yale University und der Johns Hopkins University erausgefunden, dass Ransomware mittlerweile zu den Hauptursachen für Datenschutzverstöße im Gesundheitswesen zählen. Dieses Risiko wurde für mehrere große Gesundheitsorganisationen, die von Ransomware-Angriffen betroffen waren, die der auf **unserer einschlägigen Watchlist** vertretenen Interlock-Gruppe zugeschrieben werden, schmerzhafte Realität. Einzelheiten erfahren Sie im Abschnitt **„Das Gesundheitswesen im Visier von Ransomware-Akteuren"**.

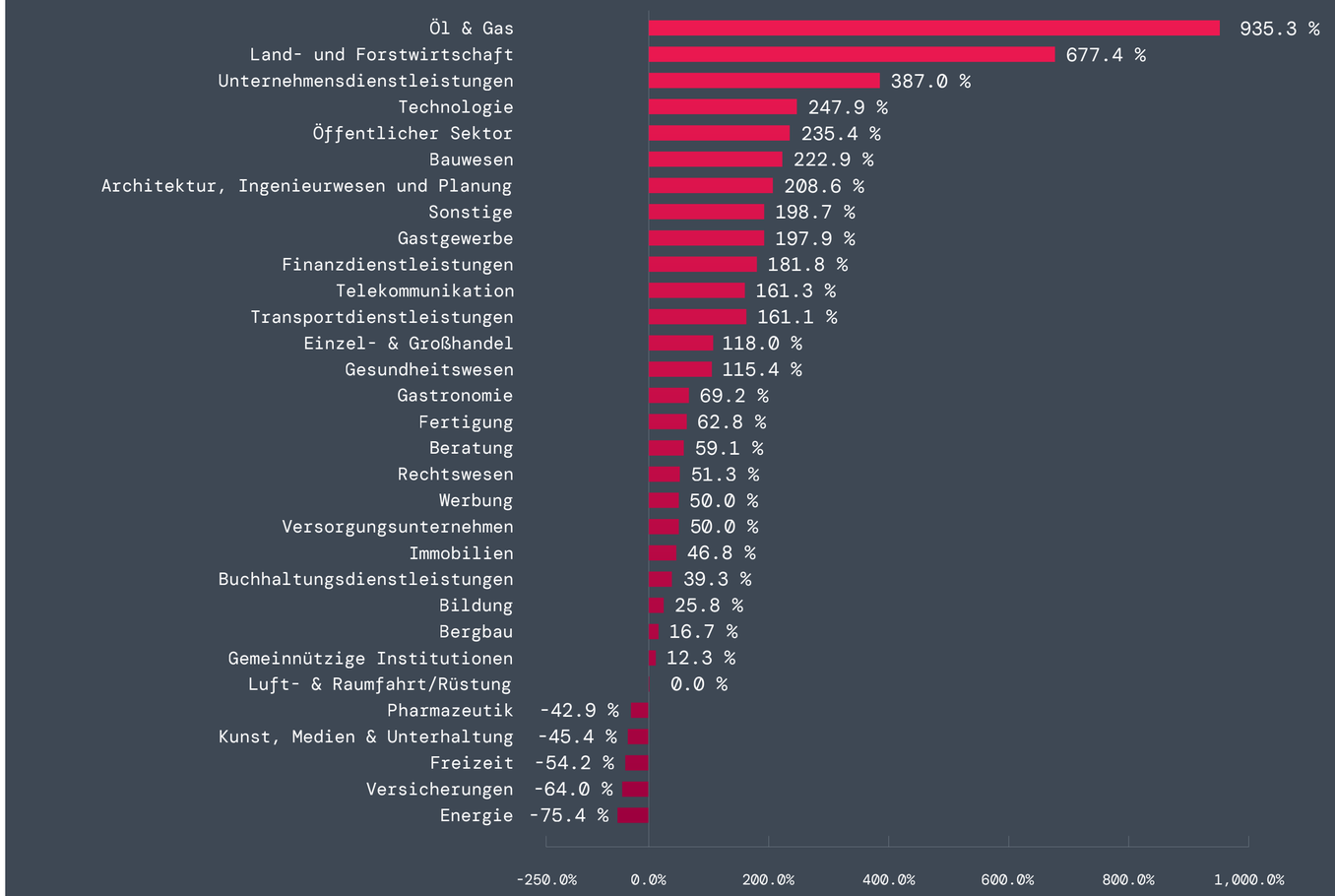


Abb. 7: Prozentuale Veränderung der Ransomware-Erpressungsangriffe im Vergleich zum Vorjahr nach Branchen
(Branchen mit weniger als 10 gemeldeten Angriffen im letztjährigen Datensatz wurden ausgeschlossen, um ein Überbewerten des Wachstums aufgrund eines niedrigen Ausgangswerts zu vermeiden)

[1] CISA, Unsophisticated Cyber Actor(s) Targeting Operational Technology, 6. Mai 2025.
[2] Axios, John Deere invites students to hack tractors, 24. Juni 2025.
[3] The HIPAA Journal, Study Explores Extent of Hacking and Ransomware Attacks in Healthcare, 16. Mai 2025.

© 2025 Zscaler, Inc. Alle Rechte vorbehalten.

Globale und regionale Hotspots

Daten von Leak-Websites zeigen eine eindeutige geografische Konzentration: Ein Großteil der Angriffe richtet sich gegen Unternehmen in den USA (50,8 %), weit vor Ländern wie Kanada (5,2 %) und Großbritannien (4,6 %). Dies verdeutlicht, dass Bedrohungsakteure weiterhin digital konzentrierte Volkswirtschaften mit hohem BSP priorisieren. Abbildung 8 zeigt eine Aufschlüsselung der 15 am häufigsten betroffenen Länder nach dem Anteil der auf Dataleak-Websites dokumentierte Ransomware-Angriffe.



Abb. 8: Top-15-Länder nach Anteil der Ransomware-Angriffe

© 2025 Zscaler, Inc. Alle Rechte vorbehalten.

Trends im Jahresvergleich

Die Auswirkungen von Ransomware fallen von Region zu Region sehr unterschiedlich aus. Wenn man weiß, wo sich die Angriffe beschleunigen, kann man zuverlässiger vorhersagen, wo die Bedrohungsakteure wahrscheinlich als nächstes zuschlagen werden, und regionsspezifische Abwehrstrategien entwickeln.

GLOBALE TOP 15: MASSIVE SPITZEN IN DEN USA

Ransomware-Angriffe nahmen weltweit stark zu. Die 15 Länder mit den meisten Ransomware-Angriffen verzeichneten Zuwächse im zwei- und dreistelligen Prozentbereich (siehe Abbildung 9). Die Zahl der Angriffe in den USA hat sich mit 3.671 mehr als verdoppelt und übertrifft damit die Gesamtzahl der übrigen 15 am häufigsten betroffenen Länder. Der Anstieg in Kanada um 194,5 % unterstreicht die Expansion der Bedrohungsakteure in Nordamerika, wobei der Fokus zunehmend auf anfälligen Sektoren liegt. Laut des National Cyber Threat Assessment 2025—2026 des Canadian Centre for Cyber Security ist Ransomware die größte Bedrohung der kritischen Infrastruktur des Landes durch Cyberkriminalität. Verwiesen wird dabei auf die zunehmenden Angriffe auf Unternehmen im Gesundheitswesen, der Industrie und dem öffentlichen Sektor.[4]

Land	Ransomware-Angriffe (Report 2024)	Ransomware-Angriffe (Report 2025)	Prozentuale Veränderung
USA	1.821	3.671	101,6 %
Kanada	128	377	194,5 %
Vereinigtes Königreich	216	333	54,2 %
Deutschland	149	260	74,5 %
Indien	60	199	231,7 %
Italien	118	181	53,4 %
Frankreich	119	159	33,6 %
Australien	73	152	108,2 %
Brasilien	57	149	161,4 %
Spanien	62	134	116,1 %
Japan	42	75	78,6 %
Mexiko	57	74	29,8 %
Schweiz	43	60	39,5 %
Belgien	34	59	73,5 %
Israel	11	59	436,4 %

Abb. 9: Jahresvergleich der Ransomware-Angriffe nach Ländern



[4] Canadian Centre for Cyber Security, National Cyber Threat Assessment 2025–2026, abgerufen am 14. Juli 2025.

© 2025 Zscaler, Inc. Alle Rechte vorbehalten.

EMEA: ZUNEHMENDE ANGRIFFE IN EUROPA UND DARÜBER HINAUS

In der Region Europa, Naher Osten und Afrika (EMEA) kam es zu einem flächendeckenden Anstieg der Ransomware-Aktivitäten, wie in Abbildung 10 dargestellt. Bemerkenswerte Spitzen im Vergleich zum Vorjahr wurden in großen Volkswirtschaften wie Spanien (+116,1 %) und Deutschland (+74,5 %) sowie kleineren Märkten wie Belgien (+73,5 %) beobachtet. In Israel kam es zu einem starken relativen Anstieg um 436,4 % (gegenüber einem vergleichsweise niedrigen Ausgangswert), der wahrscheinlich auf wachsende geopolitische Spannungen und eine Zunahme staatlich organisierter Ransomware-Operationen zurückzuführen ist.

Land	Ransomware-Angriffe (Report 2024)	Ransomware-Angriffe (Report 2025)	Prozentuale Veränderung
Vereinigtes Königreich	216	333	54,2 %
Deutschland	149	260	74,5 %
Italien	118	181	53,4 %
Frankreich	119	159	33,6 %
Spanien	62	134	116,1 %
Schweiz	43	60	39,5 %
Belgien	34	59	73,5 %
Israel	11	59	436,4 %
Vereinigte Arabische Emirate	21	52	147,6 %
Niederlande	50	52	4 %

Abb. 10: Jahresvergleich der Ransomware-Angriffe nach Ländern in der EMEA-Region

APAC: EXPLOSIVES WACHSTUM IN SCHWELLEN- UND ETABLIERTEN MÄRKTEN

Die Region Asien-Pazifik (APAC) verzeichnete einige der weltweit höchsten Zuwächse im Vergleich zum Vorjahr. Wie Abbildung 11 zeigt, haben Ransomware-Akteure ihre Präsenz in einer Region ausgeweitet, die durch eine rasante digitale Transformation und sehr unterschiedliche Cyber-Reifegrade gekennzeichnet ist. Die Auswirkungen waren im gesamten APAC-Raum spürbar, von regionalen Technologie- und Logistikzentren wie Singapur (+237,5 %) und Taiwan (+147,1 %) bis hin zu großen Volkswirtschaften wie China (+186,7 %) und Indien (+231,7 %).

Land	Ransomware-Angriffe (Report 2024)	Ransomware-Angriffe (Report 2025)	Prozentuale Veränderung
Indien	60	199	231,7 %
Australien	73	153	109,6 %
Japan	42	75	78,6 %
Singapur	16	54	237,5 %
Indonesien	23	43	86,9 %
China	15	43	186,7 %
Taiwan	17	42	147,1 %
Thailand	25	32	28 %
Malaysia	20	27	35 %
Hongkong	7	23	228,6 %

Abb. 11: Jahresvergleich der Ransomware-Angriffe nach Ländern in der APAC-Region

© 2025 Zscaler, Inc. Alle Rechte vorbehalten.

Aktivste Ransomware-Gruppen in den Jahren 2024/25

Mehrere äußerst aktive Gruppen dominierten weiterhin das Ransomware-Ökosystem, allen voran RansomHub, die mit 833 öffentlich bekannten Opfern die höchste Opferzahl verzeichnete. Damit war die Gruppe gemessen an den gemeldeten Aktivitäten im letzten Jahr die produktivste Ransomware-Gruppe. Interessanterweise beschloss die Gruppe, ihre Aktivitäten einzustellen, und verschwand im April 2025.

Sowohl Akira als auch Clop sind seit letztem Jahr in der Rangliste der Ransomware-Angriffe aufgestiegen. Akira, der 520 Opfer zugeschrieben werden, hat ihren Einflussbereich durch zahlreiche Partner und Erstzugangsbroker stetig erweitert. Clop, bekannt für seinen Fokus auf Supply-Chain-Angriffe, liegt mit 488 Opfern dicht dahinter. Dies unterstreicht die Strategie des Unternehmens, zur Maximierung ihrer Wirkung gängige Softwareanwendungen von Drittanbietern ins Visier zu nehmen.

Abbildung 12 zeigt die Ransomware-Gruppen mit den meisten Opfern im letzten Jahr.

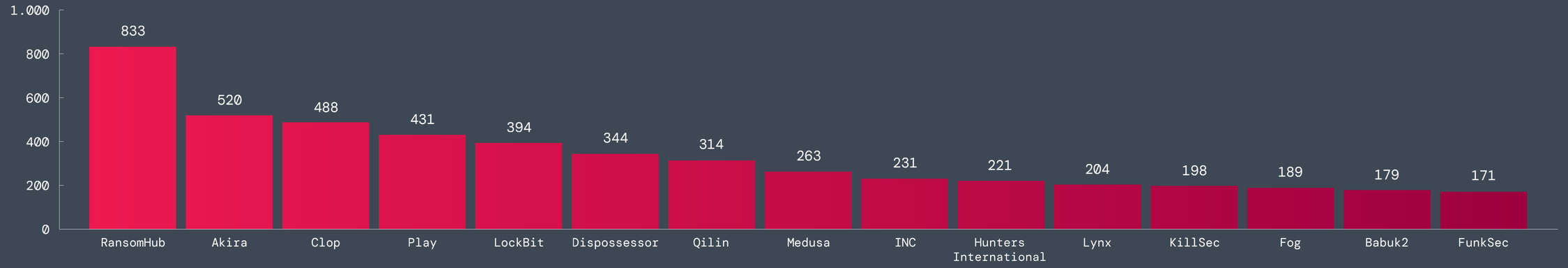


Abb. 12: Auf Dataleak-Websites gemeldete Ransomware-Angriffe

© 2025 Zscaler, Inc. Alle Rechte vorbehalten.

Neue Ransomware-Gruppen

Die Ransomware-Landschaft verändert sich ständig: Altbekannte Gruppen verschwinden und neue Gruppen tauchen auf. Dabei kann es sich um eine strategische Umbenennung zur Umgehung von Sanktionen handeln oder um den Versuch einer neuen Gruppe, eine Lücke zu füllen, die andere hinterlassen haben. Unabhängig davon wechseln Mitglieder ehemaliger Ransomware-Gruppen regelmäßig zu neuen Akteuren und wenden dabei ihre etablierten Angriffsmethoden an. Die Zeitleiste in Abbildung 13 zeigt Ransomware-Gruppen, die zwischen April 2024 und April 2025 aktiv wurden und begannen, Daten auf Leak-Websites zu veröffentlichen.

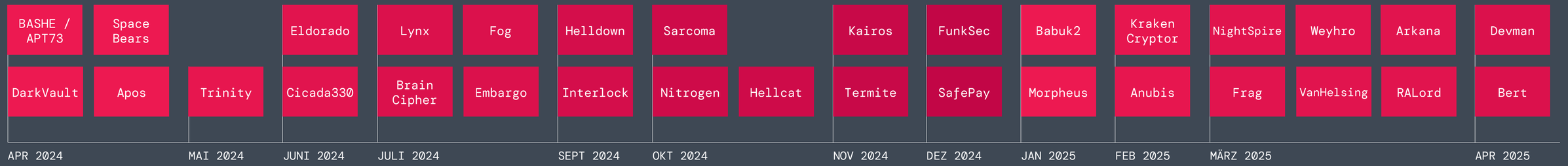


Abb. 13: Neue Ransomware-Gruppen mit Dataleak-Websites



© 2025 Zscaler, Inc. Alle Rechte vorbehalten.

Wichtige Schwachstellen, die bei Ransomware-Kampagnen ausgenutzt werden

Ransomware-Gruppen nutzen zunehmend Schwachstellen in kritischen Unternehmenstechnologien aus, um wirkungsvolle Angriffe auszuführen. Durch die Ausnutzung dieser Schwachstellen können Angreifer sich lateral bewegen, vertrauliche Informationen stehlen und Ransomware in Netzwerkumgebungen verbreiten. Fast alle dieser Schwachstellen können leicht ausgenutzt werden, da es sich um internetbasierte Anwendungen handelt, die durch einfache Scantechniken entdeckt werden können. Zu den wichtigsten Zielen zählen VPNs, Backup-Systeme, Hypervisoren, Remote-Access-Tools und Dateiübertragungsanwendungen — Technologien, die in Unternehmen weit verbreitet und für den Betrieb unerlässlich sind.

VPNs
Schwachstellen in virtuellen privaten Netzwerken (VPN) bieten Angreifern in der Regel direkten Zugriff auf das interne Netzwerk eines Unternehmens und ermöglichen es Bedrohungsakteuren, Aufklärungsarbeit zu leisten, sich lateral zu bewegen und kritische Systeme zu kompromittieren, um Daten zu stehlen und Ransomware einzusetzen.

Beispiele für diese Schwachstellen sind **CVE-2024-55591** (betrifft FortiProxy SSL VPN-Geräte) und **CVE-2024-40766** (betrifft SonicWall SSL VPN-Geräte).

Backup-Lösungen:
Backup- und Replikationstechnologien sind zu zentralen Angriffsvektoren für Ransomware-Betreiber geworden. Schwachstellen in diesen Systemen ermöglichen direkten Zugriff, um Daten zu stehlen und Backup-Lösungen vor der Dateiverschlüsselung zu deaktivieren.

Ein Beispiel für eine Sicherheitslücke, die von Ransomware-Bedrohern ausgenutzt wurde, ist **CVE-2023-27532** (Veeam Backup & Replikation).

Virtualisierungssoftware:
Hypervisoren wie VMware ESXi konzentrieren Workloads und sind daher ein wertvolles Ziel für Ransomware. Exploits gegen ESXi können ganze virtualisierte Umgebungen gefährden.

Beispielsweise ermöglicht die Sicherheitslücke **CVE-2024-37085** Angreifern, die ESX-Admins-Gruppe zu manipulieren, um die Kontrolle über einen Server zu erlangen. In den letzten Jahren haben Ransomware-Gruppen zudem zunehmend benutzerdefinierte Ransomware-Builds entwickelt, die ausschließlich der Verschlüsselung von Dateien in ESXi-Umgebungen dienen.

Tools für den Remotezugriff:
RMM-Tools (Remote Monitoring and Management) sind in IT-Umgebungen von Unternehmen für die Verwaltung von Endgeräten und Infrastruktur unverzichtbar. Sie sind jedoch auch häufig Ziel von Ransomware-Gruppen, insbesondere wenn die zugrunde liegende Software anfällig ist.

Beispiele für diese Schwachstellen sind **CVE-2024-57726**, CVE-2024-57727 und **CVE-2024-57728**(SimpleHelp RMM), die es Akteuren, die Ransomware-Angriffe begehen, ermöglicht haben, sich Zugriff auf Unternehmensumgebungen zu verschaffen.

File-Transfer-Anwendungen:
Unternehmen nutzen File-Transfer-Anwendungen, um Dateien effizient zwischen internen Systemen und externen Geschäftspartnern, Lieferanten oder Kunden auszutauschen. Bei Zugriff auf das Internet können jedoch Schwachstellen in der zugrunde liegenden Anwendung ausgenutzt werden, um auf Unternehmensdaten zuzugreifen. Diese Anwendungsgruppe war das Hauptziel der Clop-Ransomware-Gruppe, die wir später in diesem Report näher erläutern.

Allein im letzten Jahr nutzte die Gruppe mehrere Zero-Day-Schwachstellen in Dateiübertragungsanwendungen (**CVE-2024-50623** und **CVE-2024-55956**), um Daten von Hunderten von Unternehmen zu stehlen.

Absicherung anfälliger Systeme

Im Kampf gegen die Ransomware-Kampagnen, die durch diese Schwachstellen begünstigt werden, müssen Unternehmen einen mehrschichtigen Sicherheitsansatz verfolgen:

1. **Patchen als Priorität:** Beschleunigen Sie die Fehlerbehebung für Edge-Services — Firewalls, VPNs und Backup-Systeme.
2. **Segmentierung und Zero Trust:** Blockieren Sie laterale Bewegungen, indem Sie die Segmentierung von Einzelverbindungen zwischen Usern und Anwendungen, die Verwaltung des Gerätestatus, strenge Zugriffskontrollen und die Überwachung von Konten mit Sonderberechtigungen erzwingen.
3. **Erweiterter Bedrohungsschutz mit Zero-Day-Abdeckung:** Nutzen Sie Inline-Sandboxing und Isolationstechnologien, um Zero-Day-Exploits zu verhindern. Führen Sie eine TLS-Inspektion durch, um schädliche Payloads zu blockieren, und wenden Sie DLP-Kontrollen (Data Loss Prevention) an, um Datenexfiltration zu verhindern.

Durch das proaktive Schließen dieser Sicherheitslücken können Unternehmen die Fähigkeit der Ransomware-Akteure, Schwachstellen auszunutzen, verringern und ihre Resilienz deutlich stärken.

© 2025 Zscaler, Inc. Alle Rechte vorbehalten.

Ransomware-Vorfälle in den Schlagzeilen

Black Basta nutzt ChatGPT für kriminelle Aktivitäten

Im Februar 2025 wurden zahlreiche Nachrichten vom internen Matrix-Chatserver der Black Basta-Ransomware-Gruppe online geleakt, was Forschern einen direkten Einblick in die Aktivitäten der Gruppe ermöglichte. Diese Chats, die sich über den Zeitraum von September 2023 bis September 2024 erstreckten, gaben Aufschluss über die interne Struktur, Angriffsstrategien und Prozesse der Gruppe. Vor allem enthüllen sie, wie Black Basta ChatGPT nutzt. Laut dem ThreatLabz-Report 2025 zur KI-Sicherheit dominiert ChatGPT die KI-Landschaft und ist für rund 45 % aller KI-bezogenen Transaktionen verantwortlich.

Aufgrund der großen Beliebtheit und weiten Verbreitung von ChatGPT in der KI-Landschaft untersuchte ThreatLabz, wie Black Basta ChatGPT in seine Routinevorgänge integriert.

Unsere Erkenntnisse zeigen, dass die Ransomware-Gruppe ChatGPT auf verschiedene Weise einsetzt:

- **Umschreiben von Code:** In den Chat-Protokollen wird ausdrücklich die Verwendung von ChatGPT zum Umschreiben von Skripten in Python erwähnt.
- **Integration in allgemeine Arbeitsabläufe:** Die Gruppe gibt an, neben Internetressourcen teilweise auch auf ChatGPT zurückzugreifen, was auf eine Integration in ihre allgemeinen Arbeitsabläufe hindeutet. Darüber hinaus zeigen die Chatprotokolle, dass sich die Mitglieder gegenseitig zur Problemlösung mit ChatGPT anspornen.
- **Interesse an KI-Modellen ohne rechtliche Einschränkungen:** Die Diskussion über WormGPT spiegelt ein Interesse an der Erforschung unzensierter KI-Tools wider, die möglicherweise Funktionen bieten, die nicht durch die in ChatGPT integrierten rechtlichen und ethischen Regeln eingeschränkt sind.

Russisch	Deutsch	Was bedeutet das?
щас попижу с chat gpt	Jetzt werde ich chatten mit ChatGPT	Zeigt, dass Black-Basta-Mitglieder ChatGPT verwenden bei technischen Aufgaben.
чату gpt задайте вопрос *он поможет вам*	Fragen Sie ChatGPT die Frage Er wird Ihnen helfen.	Zeigt, dass Black Basta ChatGPT zur Problemlösung verwendet und es anderen in der Gruppe ebenfalls empfiehlt.
что они подразумевают под тем что все что ты писал надо переписать на питон ? *надо тз и какие функции, а я скажу возможно это или нет* *попробуй переписать чатом gpt*	Was soll das heißen: Muss alles in Python umgeschrieben werden? Die Anforderungen und welche Funktionen sind benötigt - lassen Sie es mich wissen, und Ich entscheide dann, ob es möglich ist oder nicht. Versuche, es mit ChatGPT umzuschreiben.	Hebt hervor, wie Black Basta ist Nutzung der Funktionen von ChatGPT, um beim Umschreiben von Skripten in Python, möglicherweise als Zeitersparnis und/oder Ausgleich für schwache Python-Programmierkenntnisse.
на половину инет, на половину chatgpt	Das ist zur Hälfte internetbasiert und zur Hälfte ChatGPT.	Zeigt, dass Black-Basta-Mitglieder einen hybriden Ansatz verfolgen bei Angriffen, bei denen ChatGPT eine bedeutende Rolle neben Internetquellen spielem.
бля найти бы доступ в WormGPT *без цензуры chatGPT который*	Ich will wissen, wie ich Zugriff auf WormGPT erhalte. unzensierter ChatGPT welche	Zeigt Black Bastas Interesse daran, von ChatGPT auf weniger ethische Tools wie WormGPT umzusteigen. Deutet an, dass sie ChatGPT ausgiebig genutzt haben und vertraut sind mit seinen Einschränkungen.

© 2025 Zscaler, Inc. Alle Rechte vorbehalten.

Das Ransomware-Playbook für mehrstufige Angriffe18

Es wurde eine Abkehr von den Erstzugriffsbrokern beobachtet, die groß angelegte Spam-Kampagnen als ersten Infektionsvektor verwenden. Stattdessen wurden in den letzten zwei Jahren gezieltere Angriffe erfolgreich eingesetzt, wobei die in Abbildung 14 dargestellte Methodik zum Einsatz kam.

Die hinter diesen Angriffen stehenden Bedrohungsakteure führen zunächst mithilfe von Websites wie ZoomInfo eine Erkundung durch, um Kontaktinformationen über Mitarbeiter eines Zielunternehmens zu erwerben. Über Websites wie LinkedIn können zusätzliche Mitarbeiterinformationen abgerufen werden, sodass Bedrohungsakteure gezielt Mitarbeiter identifizieren können, als die sie sich zu Angriffszwecken ausgeben können, insbesondere Mitarbeiter der IT-Abteilung des Unternehmens. Bestimmte Mitarbeiter mit Berechtigungen für den Zugriff auf vertrauliche Daten (normalerweise in den Bereichen Personalwesen, Lohnbuchhaltung und Finanzen) sind häufige Angriffsziele.

Nachdem die Kontaktangaben des Opfers erlangt wurden, beginnt der Angriff mit „Spam-Bombing“, um den Posteingang des Opfers zu überfluten. Anschließend ruft der Bedrohungsakteur diesen Mitarbeiter an (mit den zuvor erhaltenen Informationen) und gibt sich als Fachkraft aus der IT-Abteilung des Unternehmens aus — ein klassisches Beispiel für Vishing (Voice Phishing). Die Anrufer werden passend zum imitierten IT-Mitarbeiter (männlich, weiblich, Muttersprachler oder nicht) ausgewählt. Der Bedrohungsakteur informiert das Opfer, dass er aus der IT-Abteilung des Unternehmens anrufe und ihm bei der „Aktualisierung seines Spamfilters“ helfen wolle, und fordert Fernzugriff über ein RMM-Tool wie Microsoft Teams, Quick Assist, Team Viewer, AnyDesk usw. an. Wenn das Opfer auf die List hereinfällt, führt der Bedrohungsakteur eine Reihe von Aktionen aus, um eine Backdoor auf dem System des Opfers zu installieren und gleichzeitig genügend Glaubwürdigkeit zu vermitteln, dass die Spamfilter des Opfers „aktualisiert“ wurden. Abbildung 15 zeigt eine echte Website, die von einem Ransomware-Erstzugriffsbroker betrieben wird, der diese Masche verwendet.

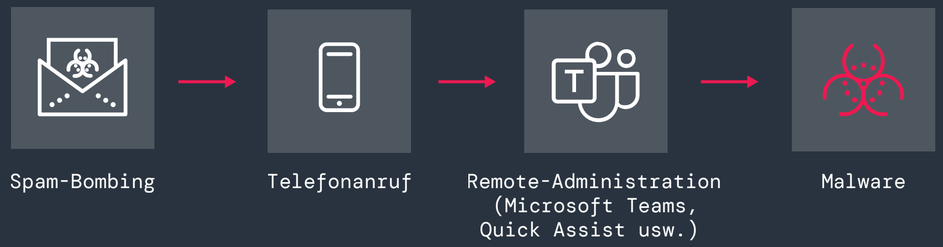


Abb. 14: Methodik eines mehrstufigen Ransomware-Angriffs



Abb. 15: Die gefälschte „Filter-Update“-Website eines Ransomware-Erstzugriffsbrokers

© 2025 Zscaler, Inc. Alle Rechte vorbehalten.

Diese Websites, die häufig auf Azure oder Amazon Web Services gehostet werden, sind täuschend einfach, können jedoch zahlreiche Techniken einsetzen, die speziell dafür entwickelt wurden, Antiviren- und Malware-Sandboxen zu umgehen: Ein solches detailorientiertes Vorgehen kann folgende Maßnahmen umfassen:

- Bei den Filter-Packs-Links handelt es sich eigentlich um ein mehrteiliges ZIP-Archiv (aufgeteilt in zwei Teile, z. B. kbxxxxxxx), das mit einem Passcode verschlüsselt ist.
- Mit der/den Schaltfläche(n) „Updates herunterladen“ werden PowerShell- oder Windows-Shell-Befehle in die Zwischenablage des Opfers kopiert, wo sie dann ausgeführt werden. Diese Befehle fordern den Bedrohungsakteur zur Eingabe des Passcodes für das ZIP-Archiv auf. Darüber hinaus legen die Befehle Registrierungswerte mit den Befehls- und Steuerungsinformationen der Malware-Payload fest. Daher funktioniert die ausführbare Malware in einer Sandbox-Umgebung mit diesem vorherigen Initialisierungsschritt nicht ordnungsgemäß.
- Nachdem das ZIP-Archiv entschlüsselt und dekomprimiert wurde, wird eine legitime ausführbare Datei (z. B. Microsoft OneDrive) genutzt, um eine schädliche Payload per DLL-Sideload zu entschlüsseln und bereitzustellen.

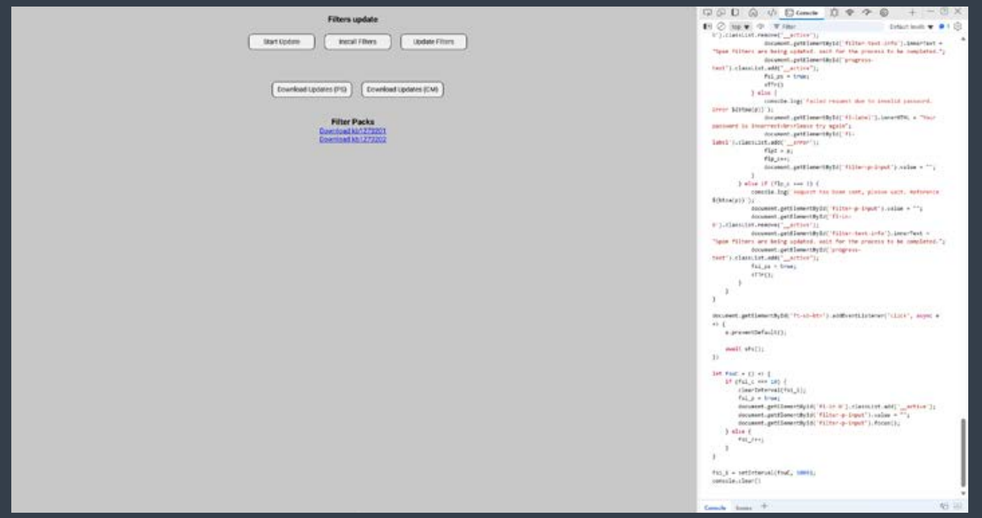


Abb. 16: Zugriff auf die Konsole auf dem Endgerät eines Opfers

Die oberen drei Schaltflächen dienen dazu, das Microsoft 365-Passwort des Opfers zu stehlen. Beim Anklicken kopiert jede Schaltfläche JavaScript-Inhalte in die Zwischenablage des Opfers. Der Bedrohungsakteur öffnet dann die Entwicklertools des Webbrowsers, um auf die Konsole zuzugreifen, wie in Abbildung 16 gezeigt.

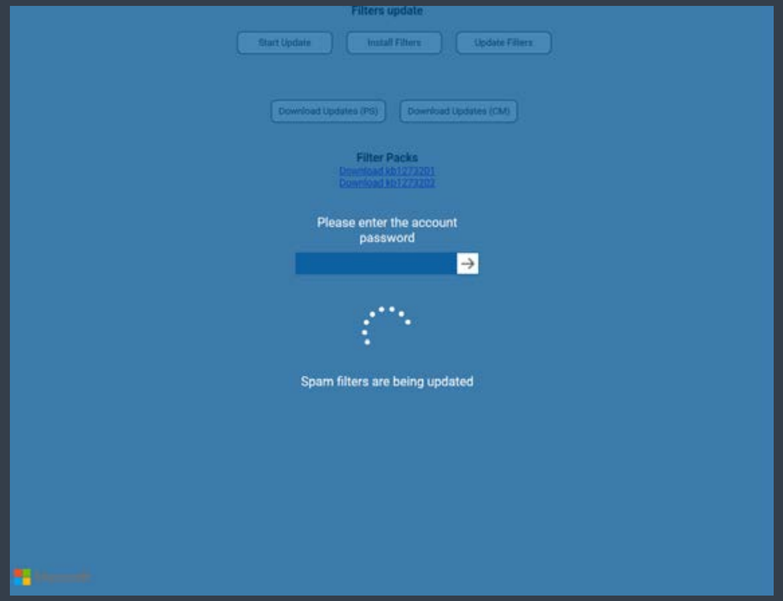


Abb. 17: Ein gefälschtes Passwort-Eingabefeld

Der JavaScript-Inhalt aus der Zwischenablage wird dann in die Konsole eingefügt und ausgeführt. Dabei wird ein Overlay angezeigt, das das Opfer zur Eingabe seines Passworts auffordert (siehe Abbildung 17).

Nachdem das Konto-Passwort des Opfers gestohlen und die Malware-Backdoor installiert wurde, versucht der Bedrohungsakteur, sich innerhalb der Unternehmensumgebung lateral zu bewegen, um Daten zu stehlen und Ransomware auszuliefern. Diese neue Art gezielter Ransomware-Angriffe ist häufig erfolgreich und viele Opfer fallen auf diese Maschen herein.

© 2025 Zscaler, Inc. Alle Rechte vorbehalten.

RaaS-Mechanismen bei Dark-Web-Datenleck aufgedeckt

Im Mai 2025 wurde in den Partner- und Admin-Panels von LockBit ein Link zum Herunterladen der Datenbank der Gruppe eingeblendet (siehe Abbildung 18).

Die geleakte MySQL-Datenbank bietet Forschern, darunter ThreatLabz, einen detaillierten Einblick in die internen Abläufe von LockBit nach einem **internationalen Großeinsatz der Strafverfolgungsbehörden** namens Operation Cronos im Februar 2024, in dessen Folge Anklage gegen den Anführer der Gruppe erhoben wurde. Selbst nach der Zerschlagung **erholte sich LockBit innerhalb weniger Tage** und startete über eine neue Dataleak-Website neue Angriffe. Die geleakte Datenbank enthält die Aktivitäten der Gruppe rund um die **Veröffentlichung von LockBit 4.0** vom 18. Dezember 2024 bis zum 29. April 2025. Die Informationen enthüllen die Namen von 75 Partnern, 4.423 Lösegeld-Chatnachrichten und rund 60.000 Bitcoin-Wallet-Adressen. 54 der 75 Partner erstellten LockBit-Ransomware-Builds für 246 Opfer in 156 Unternehmen. Jeder Partner wurde mit einer bestimmten Vertrauensstufe gekennzeichnet, wie in Abbildung 19 dargestellt.



Abb. 18: LockBit-Admin-Panel mit Link zum Herunterladen der Datenbank

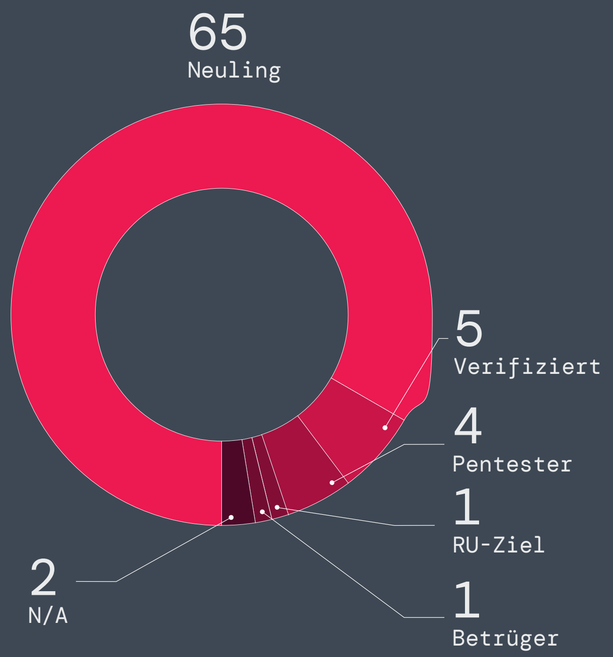


Abbildung 19: Anzahl der LockBit-Partner nach „Vertrauensstufe“

Es gab 35 Partner mit pausiertem Status, vermutlich diejenigen, die inaktiv oder suspendiert waren. Interessanterweise wechselte ein Partner mit dem Namen BaleyBeach nach der Schließung des Konkurrenten RansomHub (auf den wir später noch eingehen werden) zu LockBit. Unten sehen Sie eine Chat-Nachricht, die dieser Partner an ein Opfer gesendet hat.

> “We were affiliates of RansomHub, now RansomHub closed, we movede [sic] here. So existing companies (including yours) which we had to deal with still have chance [sic] to prevent their data leak. (Wir waren Partner von RansomHub, nach der Auflösung von RansomHub sind wir hierher umgezogen. Bestehende Unternehmen (einschließlich Ihres), mit denen wir zu tun hatten, haben also immer noch eine Chance, die Offenlegung von Daten zu verhindern.)”

© 2025 Zscaler, Inc. Alle Rechte vorbehalten.

Abbildung 20 zeigt die Anzahl der LockBit-Builds, die von den Partnern mit den meisten Builds generiert wurden.

Weder dem Administrator noch den Matrix777-Usern wurden Vertrauensstufen zugewiesen, und sie waren mit derselben TOX-ID registriert, was darauf hindeutet, dass es sich wahrscheinlich um dieselbe Person handelt.

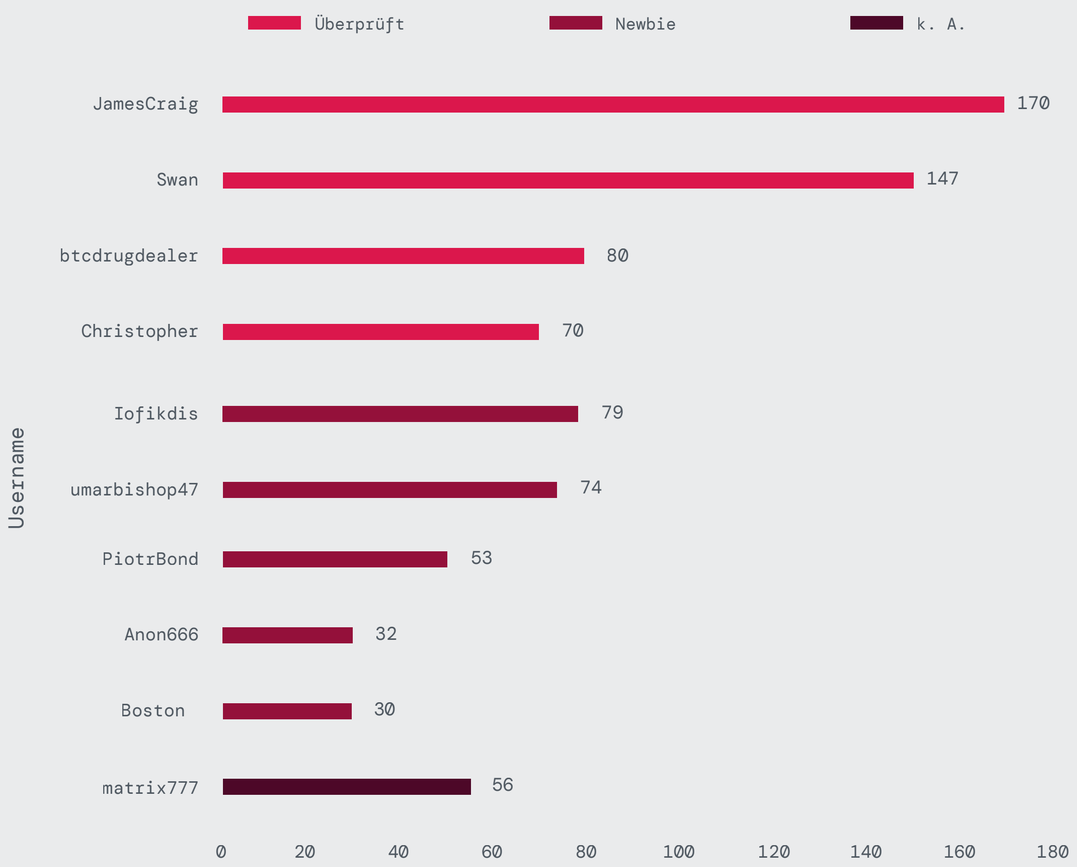


Abb. 20: Anzahl der LockBit-Builds pro Partner

Insgesamt beteiligten sich 208 Opfer an Lösegeld-Chats und 20 zahlten ein Lösegeld. Wie in Abbildung 21 dargestellt, erhielten in diesem Zeitraum von fast sechs Monaten nur 10 LockBit-Partner Lösegeldzahlungen.

In einem Fall* erklärte sich ein Opfer zur Zahlung von 2 Mio. USD an den LockBit-Partner Swan bereit. Die Chat-Protokolle endeten jedoch, kurz bevor die Informationen zur Zahlung bereitgestellt wurden. Wir können jedoch davon ausgehen, dass die Zahlung tatsächlich über eine andere Bitcoin-Wallet in der Datenbank erfolgte, die von der LockBit-Gruppe kontrolliert wird, die für dieses Opfer eine Provision von 20 % erhielt. So verdienten zwei Partner, Swan und Christopher, über 100.000 USD. Insgesamt verdienten alle LockBit-Partner zusammen 2.334.615 USD (1.867.692 USD nach Provisionen) an Lösegeldzahlungen. Die LockBit-Gruppe erhielt 20 % dieses Betrags, das entspricht etwa 466.923 USD. Diese Lösegeldzahlungen sind weitaus niedriger als die vieler führender Ransomware-Gruppen, die häufig Zahlungen in Millionenhöhe erhalten. Somit deutet diese geleakte LockBit-Datenbank darauf hin, dass die Störung im Februar 2024 die Gruppe erheblich geschwächt hat.

Username	Erhaltene Zahlungen (Schätzwert in USD)	Anzahl der Opfer, die Lösegeld gezahlt haben	Gesamtzahl der Opfer-Chats
Swan	2.021.000 USD*	2*	17
Christopher	231.015 USD	8	44
umarbishop47	40.000 USD	1	10
PiotrBond	13.000 USD	2	16
ArrynBaird	10.000 USD	1	5
Iofikdis	6.000 USD	1	12
RiccardoBond	4.400 USD	1	4
Brown	3.600 USD	1	5
JamesCraig	3.600 USD	2	17
btcdrugdealer	2.000 USD	1	6

Abb. 21: Von LockBit-Partnern erhaltene Lösegeldzahlungen

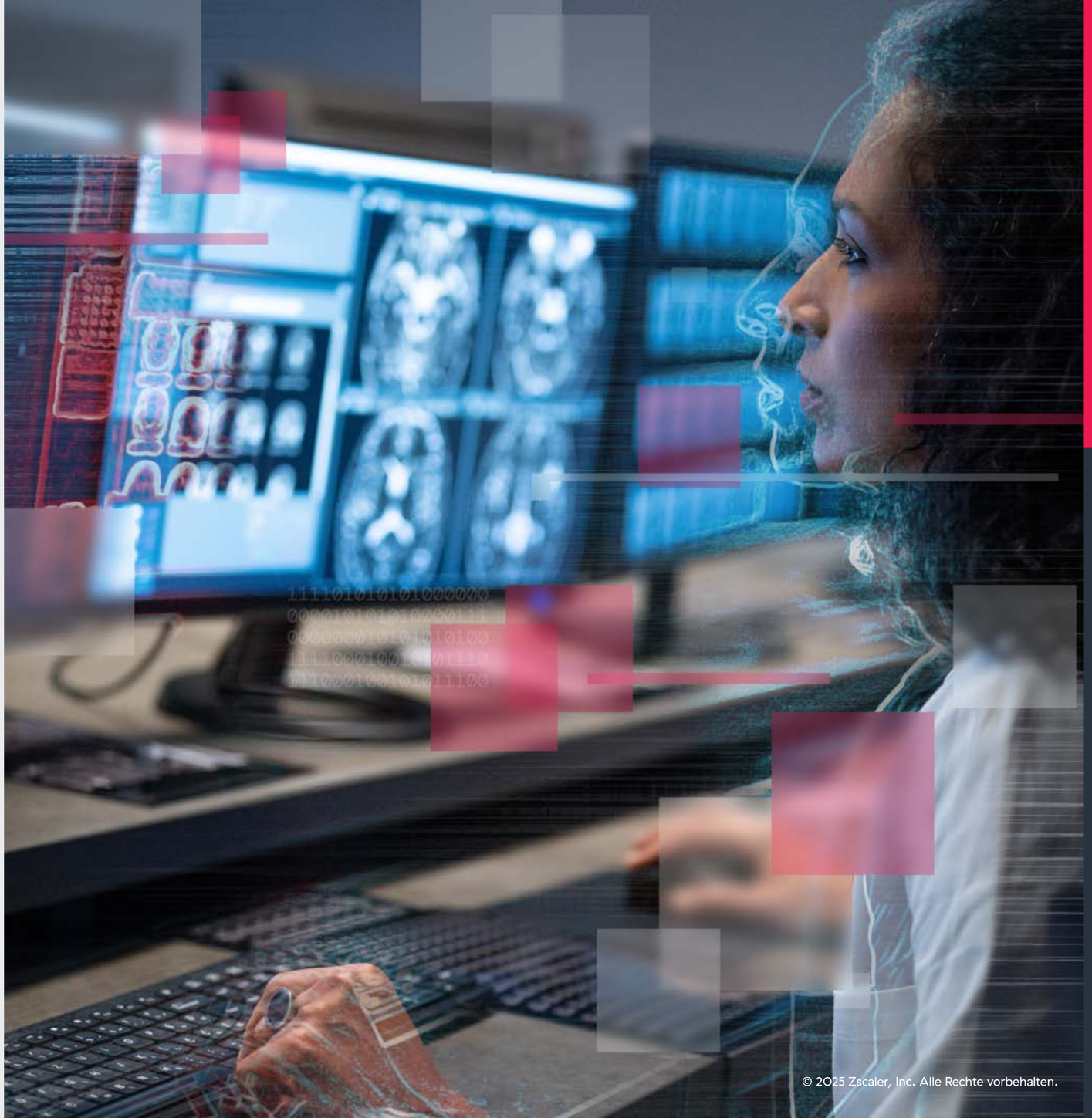
© 2025 Zscaler, Inc. Alle Rechte vorbehalten.

Das Gesundheitswesen im Visier von Ransomware-Akteuren

Ransomware-Angriffe auf den Gesundheitssektor weisen einen Trend hin zu einem neuen Muster auf: erst Daten exfiltrieren, dann Betriebsabläufe stören. Für Bedrohungsakteure zählt Datendiebstahl heute zu den wichtigsten Druckmitteln. Da Gesundheitseinrichtungen über riesige Bestände an geschützten Gesundheitsdaten verfügen, sind sie für Ransomware-Betreiber, die den Druck maximieren wollen, zu lukrativen Zielen geworden. Da das Vertrauen der Patienten im Gesundheitswesen von entscheidender Bedeutung ist, kann ein öffentlicher Verstoß ebenso schädlich sein wie Ausfallzeiten.

Weltweit verzeichnete der Gesundheitssektor im Vergleich zum Vorjahr einen deutlichen Anstieg von Ransomware-Angriffen. Diese Angriffe kombinierten häufig die Exfiltration großer Datenmengen mit Verschlüsselung, was die Institutionen mit operativem Chaos, finanziellen Verlusten und Reputationsschäden zurückließ. Im Jahr 2024 meldete das Office for Civil Rights (OCR) des US-Gesundheitsministeriums 725 Sicherheitsverstöße mit 500 oder mehr betroffenen Personen. Rund 275 Millionen Gesundheitsdaten wurden offengelegt.[5]

Ransomware im Gesundheitswesen zielt nicht mehr bloß auf Betriebsunterbrechungen ab. Es geht um Erpressung — und die beginnt mit Daten. Durch den Diebstahl und die Offenlegung von Millionen von Datensätzen können Ransomware-Betreiber den Druck auf Opfer im Gesundheitswesen verdoppeln. Aktuelle Daten zu verschiedenen Ransomware-Gruppen unterstreichen einen kritischen Trend: Das Ausmaß des Datendiebstahls nimmt rapide zu. Zu den Gruppen, die diese Entwicklung vorantreiben, gehört Interlock, die im Abschnitt **„Die 5 gefährlichsten Ransomware-Gruppen 2025/26“** vorgestellt wird.



[5] The HIPAA Journal, 2024 **Healthcare Data Breach Report**, 30. Januar 2025.

© 2025 Zscaler, Inc. Alle Rechte vorbehalten.

Die Wende im Kampf gegen Ransomware

Trotz der deutlichen Zunahme von Ransomware-Angriffen im letzten Jahr gibt es im Kampf gegen Ransomware Erfolge zu vermelden. Die Zusammenarbeit zwischen globalen Strafverfolgungsbehörden und Forschern aus der Privatwirtschaft hat sich bei der Zerschlagung einiger Schlüsselelemente von Ransomware-Operationen und der Unterstützung der Opfer bei der Wiederherstellung als wirksam erwiesen.

Beispielsweise entdeckte ThreatLabz Anfang 2025 eine Schwachstelle in RansomHub, die die Entschlüsselung von Dateien ohne Zahlung eines Lösegelds ermöglichte. Aufbauend auf dieser Entdeckung entwickelte das ThreatLabz-Team *DecryptHub* (siehe Abbildung 22), ein spezialisiertes Portal zur Unterstützung von Unternehmen, die von den Ransomware-Angriffen von RansomHub betroffen sind.

Das ThreatLabz DecryptHub-Portal half Dutzenden von betroffenen Unternehmen, Dateien wiederherzustellen, und ersparte ihnen so potenziell Millionen von Dollar an Lösegeldzahlungen.

Vor ihrer Einstellung im April 2025 zählte RansomHub zu den größten und aktivsten Ransomware-Gruppen. Viele der mit der Gruppe verbundenen Unternehmen waren zuvor mit der inzwischen aufgelösten Ransomware-Operation BlackCat verbunden. Ähnlich wie BlackCat verwendete RansomHub die Programmiersprache Rust, um Ransomware für zahlreiche Architekturen zu entwickeln und zu plattformübergreifend zu kompilieren, darunter:

- Windows (x86, x64, ARM, ARM64)
- FreeBSD (x64)
- Linux (x86, x64, ARM, ARM64, ARMv5, ARMv5-64, ARMv6, ARMv6-64, ARMv7, ARMv7-64)
- ESXi (x64)

Ein weiterer bemerkenswerter Erfolg aus dem vergangenen Jahr ist der groß angelegte Strafverfolgungseinsatz mit dem Codenamen **Operation Endgame**, der in Abstimmung mit Branchenpartnern, darunter Zscaler, durchgeführt wurde (siehe Abbildung 23).

Operation Endgame ist eine globale Initiative zur Zerschlagung cyberkrimineller Organisationen und des Malware-Ökosystems, das Ransomware-Angriffe ermöglicht. Der jüngste Erfolg war die Zerschlagung von **DanaBot**, einer leistungsstarken modularen Malware-Gruppe, die eine Malware-as-a-Service-Plattform (MaaS) mit Verbindungen zu verschiedenen Ransomware-Gruppen betrieb. Dies knüpft an eine Reihe von Erfolgen im Jahr 2024 an, als Operation Endgame bekannte Malware-Familien wie **SmokeLoader**, IcedID, SystemBC, Pikabot und Bumblebee ins Visier nahm.

Zscaler ThreatLabz unterstützt Operation Endgame seit zwei Jahren und stellt wichtige Ressourcen und Informationen zur Verfügung, um Malware-Kampagnen zu identifizieren, kriminelle Infrastrukturen zu zerschlagen und Cyberkriminelle zu entlarven. ThreatLabz hat außerdem kostenlose Tools über **GitHub** veröffentlicht, mit denen Infektionen erkannt und behoben werden können. Dies unterstreicht die Bedeutung der Zusammenarbeit im Kampf gegen Ransomware.



Abb. 22: Das Opferportal DecryptHub

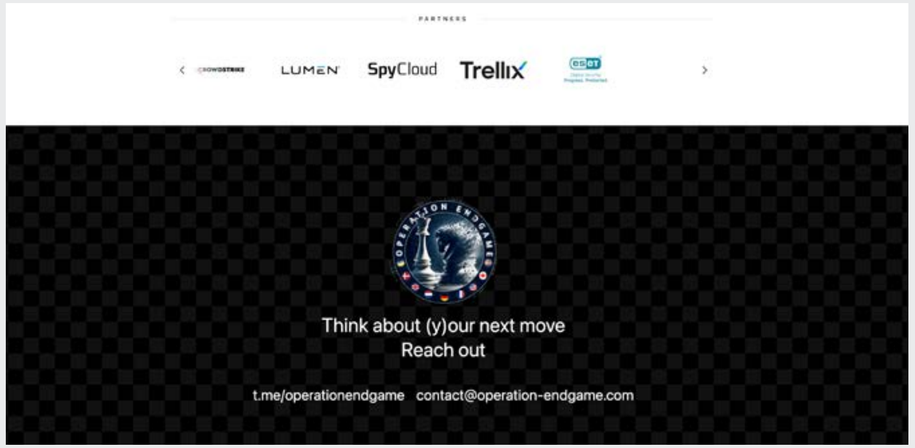


Abb. 23: Kontaktdaten von Operation Endgame

©2025 Zscaler, Inc. All rights reserved.

Die 5 gefährlichsten Ransomware-Gruppen 2025/26

1. Dark Angels

Die Ransomware-Gruppe Dark Angels ist seit April 2022 aktiv und zählt zu den derzeit erfolgreichsten Ransomware-Akteuren. Die Gruppe ist für ihre äußerst lukrativen Angriffe bekannt geworden und verzeichnete eine Lösegeldzahlung in Rekordhöhe von 75 Millionen USD, die ThreatLabz 2024 aufdeckte. Die Gruppe hebt sich aus mehreren Gründen von der Masse ab. Im Gegensatz zu anderen Bedrohungsgruppen lagern die Dark Angels ihre Angriffe nicht an Drittanbieter (z. B. Erstzugriffsbroker) aus. Die Anzahl der von den Dark Angels gestarteten Angriffe ist begrenzt und konzentriert sich auf große Organisationen. Dark Angels exfiltriert riesige Datenmengen von Opfern, im Durchschnitt 9,6 TB und im Median 2,35 TB. Die Gruppe entscheidet dann, ob sie Ransomware einsetzt und die Daten einer Organisation verschlüsselt. Um Schlagzeilen zu vermeiden und unter dem Radar zu bleiben, bemüht sich Dark Angels nach Möglichkeit, Unternehmen nicht mit Ransomware zu schwächen.

Die Gruppe veröffentlicht gestohlene Opferdaten auf einer Website namens Dunghill Leak und einem Telegram-Kanal, auf denen die Dark Angels nicht erwähnt werden, wahrscheinlich teilweise, um eine Zuordnung der Angriffe zu vermeiden.

Dark Angels infiltriert Unternehmensnetzwerke mithilfe verschiedener Techniken, darunter Phishing-E-Mails und öffentlich zugängliche Anwendungen, die Schwachstellen wie CVE-2023-22069 enthalten. Die Gruppe scannt kompromittierte Netzwerke und nutzt Microsoft-Active-Directory-Umgebungen aus. Die primären Ziele sind Benutzer mit Domänenadministrator-Berechtigungen, um laterale Bewegungen und den Zugriff auf die Domänencontroller der Organisation zu erleichtern.

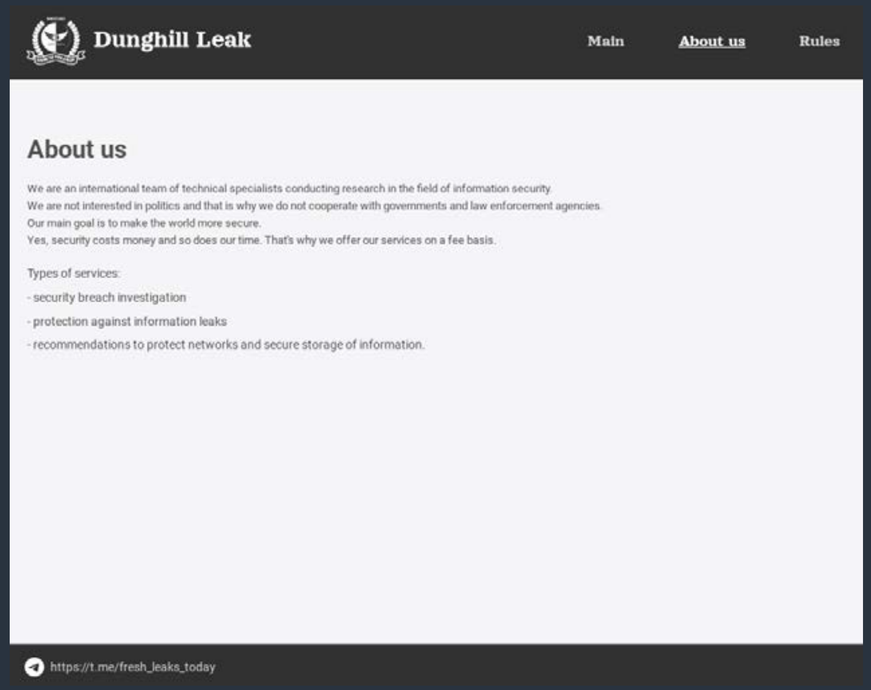


Abb. 24: Dunghill-Leak-Website der Dark Angels-Gruppe

Interessanterweise hat Dark Angels keine eigene Ransomware entwickelt. Stattdessen verlässt sich die Gruppe auf benutzerdefinierte Builds von Ransomware-Familien von Drittanbietern, darunter Babuk, Read the Manual (RTM) Locker und eine Variante von RagnarLocker. Dark Angels zielt auf Dateien unter Windows, Linux, ARM und ESXi zur Dateiverschlüsselung ab.



© 2025 Zscaler, Inc. Alle Rechte vorbehalten.

2. Clop/Cl0p

Clop, auch bekannt als ClOp, ist eine Ransomware-Gruppe, die seit 2019 aktiv ist. Clop hat sich weitgehend von der Dateiverschlüsselung abgewandt und konzentriert sich stattdessen auf Datenerpressung über Supply-Chain-Angriffe, die Zero-Day-Schwachstellen ausnutzen, insbesondere in gängigen webbasierten File-Transfer-Plattformen. Diese ermöglichen es den Angreifern, auf vertrauliche Daten von Hunderten oder sogar Tausenden von Unternehmen zugleich zuzugreifen und diese zu stehlen. Zu den File-Transfer-Anwendungen, die als erste ausgenutzt wurden, zählte die Legacy-FTA von Acellion im Dezember 2020. Sie wies zahlreiche Schwachstellen (CVE-2021-2710, CVE-2021-27102, CVE-2021-27103 und CVE-2021-27104) auf, die Clop ausnutzte, um eine speziell entwickelte Webshell bereitzustellen und Daten von Dutzenden von Unternehmen zu stehlen. Im Juli 2021 nutzte Clop die Sicherheitslücke CVE-2021-35211 in den **Anwendungen Serv-U Managed File Transfer und Serv-U Secure FTP**. In diesen Fällen nutzte Clop die Schwachstelle aus, um sich Zugriff auf die internen Netzwerke von Unternehmen zu verschaffen, was zur Datenexfiltration und Dateiverschlüsselung führte.

Anfang 2023 führte Clop einen weiteren Supply-Chain-Angriff durch, der auf die Managed File Transfer (MFT)-Anwendung von GoAnywhere abzielte. Dieser Angriff nutzte CVE-2023-0669 aus und ermöglichte so die Ausführung von Remotecode ohne Authentifizierung sowie Datendiebstahl. Clop nutzte die Zero-Day-Schwachstelle, um **Daten von über 100 Unternehmen zu stehlen**. Im Mai 2023, nur wenige Monate nach dem MFT-Vorfall bei GoAnywhere, nutzte Clop eine Zero-Day-SQL-Injection-Schwachstelle (**CVE-2023-34362**) in der MOVEit Transfer-Anwendung, um Daten von Unternehmen zu stehlen, die über internetfähige Instanzen verfügten. Dies war einer der bis dahin größten Ransomware-Supply-Chain-Angriffe, der über 2.500 Organisationen betraf und zum Verlust personenbezogener Daten von **Millionen von Menschen** führte. Clop kündigte diesen Angriff auf seiner Dataleak-Website an, wie in Abbildung 25 dargestellt.



DEAR COMPANIES.

CLOP IS ONE OF TOP ORGANIZATION OFFER PENETRATION TESTING SERVICE AFTER THE FACT.

THIS IS ANNOUNCEMENT TO EDUCATE COMPANIES WHO USE PROGRESS MOVEIT PRODUCT THAT CHANCE IS THAT WE DOWNLOAD ALOT OF YOUR DATA AS PART OF EXCEPTIONAL EXPLOIT. WE ARE THE ONLY ONE WHO PERFORM SUCH ATTACK AND RELAX BECAUSE YOUR DATA IS SAFE.

WE ARE TO PROCEED AS FOLLOW AND YOU SHOULD PAY ATTENTION TO AVOID EXTRAORDINARY MEASURES TO IMPACT YOU COMPANY.

IMPORTANT! WE DO NOT WISH TO SPEAK TO MEDIA OR RESEARCHERS. LEAVE.

STEP 1 - IF YOU HAD MOVEIT SOFTWARE CONTINUE TO STEP 2 ELSE LEAVE.
STEP 2 - EMAIL OUR TEAM UNLOCK@GOTO-PAY.COM OR SUPPORT@IN2PAY.COM
STEP 3 - OUR TEAM WILL EMAIL YOU WITH DEDICATED CHAT URL OVER TOR

WE HAVE INFORMATION ON HUNDREDS OF COMPANIES SO OUR DISCUSSION WILL WORK VERY SIMPLE.

STEP 1 - IF WE DO NOT HEAR FROM YOU UNTIL JUNE 14 2023 WE WILL POST YOUR NAME ON THIS PAGE
STEP 2 - IF YOU RECEIVE CHAT URL GO THERE AND INTRODUCE YOU
STEP 3 - OUR TEAM WILL PROVIDE 10% PROOF OF DATA WE HAVE AND PRICE TO DELETE
STEP 4 - YOU MAY ASK FOR 2-3 FILES RANDOM AS PROOF WE ARE NOT LYING
STEP 5 - YOU HAVE 3 DAY TO DISCUSS PRICE AND IF NO AGREEMENT YOU CUSTOM PAGE WILL BE CREATED
STEP 6 - AFTER 7 DAYS ALL YOU DATA WILL START TO BE PUBLICATION
STEP 7 - YOU CHAT WILL CLOSE AFTER 10 NOT PRODUCTIVE DAY AND DATA WILL BE PUBLISH

WHAT WARRANTY? OUR TEAM HAS BEEN AROUND FOR MANY YEARS. WE HAVE NOT EVEN ONE TIME NOT DO AS WE PROMISE. WHEN WE SAY DATA IS DELETE IT IS CAUSE WE SHOW VIDEO PROOF. WE HAVE NO USE FOR FEW MEASLE DOLLARS TO DECEIVE YOU.

CALL TODAY BEFORE YOUR COMPANY NAME IS PUBLISH HERE.

FRIENDLY CLOP.

PS. IF YOU ARE A GOVERNMENT, CITY OR POLICE SERVICE DO NOT WORRY, WE ERASED ALL YOUR DATA. YOU DO NOT NEED TO CONTACT US. WE HAVE NO INTEREST TO EXPOSE SUCH INFORMATION.

Abb. 25: Bekanntgabe des Exploits der MOVEit-Sicherheitslücke CVE-2023-34362

Die jüngsten groß angelegten Supply-Chain-Angriffe von Clop ereigneten sich im Oktober 2024. Dabei wurden zwei Schwachstellen (CVE-2024-50623 und CVE-2024-55956) in den File-Transfer-Anwendungen Harmony, VLTrader und LexiCom von Cleo ausgenutzt. Diese Schwachstellen ermöglichten es einem nicht authentifizierten User, **beliebige Bash- oder PowerShell-Befehle zu importieren und auszuführen**. Clop nutzte diese Schwachstellen erneut, um Daten von Unternehmen zu stehlen, die im Internet exponierte File-Transfer-Anwendungen von Cleo einsetzten. Ein Beispiel für eine Lösegeldforderung von Clop an ein Opfer dieser Cleo-Angriffe wurde von ThreatLabz erfasst und ist hier verfügbar.

Die Angriffe von Clop sind von erheblicher Tragweite, da einige Opfer mehrfach von der Gruppe angegriffen wurden. So identifizierte ThreatLabz ein Opfer des MOVEit-Angriffs von Clop, das bereits ein Lösegeld in Höhe von 1 Mio. USD gezahlt hatte und später dem Cleo-Angriff der Gruppe zum Opfer fiel.

© 2025 Zscaler, Inc. Alle Rechte vorbehalten.

3. DragonForce

DragonForce entstand im Dezember 2023 als RaaS-Gruppe. Frühe Versionen der Ransomware von DragonForce nutzten den durchgesickerten LockBit-Builder. Später entwickelte die Gruppe ihre eigene Ransomware auf Basis des geleakten Conti-Quellcodes. Anfang 2025 kündigte DragonForce in einem Cybercrime-Forum und auf seiner Nachrichten-Website ein neues kartellartiges Geschäftsmodell an (siehe Abbildung 26).

Dieses neue Modell ermöglicht es Ransomware-Partnern, die Infrastruktur, Tools und Services der Gruppe für ihre eigenen Angriffe zu nutzen, mit einem Gewinnbeteiligungsprogramm im Verhältnis 80/20. Die mit der Gruppe verbundenen Unternehmen haben mehr als 30 TB an Daten gestohlen, wobei jedes Opfer im Durchschnitt etwa 156 GB verlor, im Median waren es 72 GB.

DragonForce erhielt relativ wenig Aufmerksamkeit, bis die Gruppe im April 2025 ihre „Fusion“ mit RansomHub ankündigte, einer der damals größten und aktivsten Ransomware-Gruppen. RansomHub bestritt die Behauptung und beschuldigte Mitglieder von DragonForce, ihre Infrastruktur gestört und ihre Website gehackt zu haben. Fest steht, dass RansomHub den Betrieb einstellte und viele der mit der Gruppe verbundenen Unternehmen zu DragonForce wechselten. Zu diesen Partnern gehört Scattered Spider (auch bekannt als „The Com“), das mithilfe verschiedener Social-Engineering-Techniken Angriffe in erheblichem Ausmaß auf große Unternehmen durchgeführt hat und dabei gezielt IT-Abteilungen angegriffen hat, um die Multifaktor-Authentifizierung (MFA) zu umgehen. Scattered Spider soll hinter den DragonForce-Angriffen stecken, die im April und Mai 2025 mehrere britische Einzelhändler ins Visier nahmen.

4. Akira

Seit ihrem Auftauchen im April 2023 hat sich Akira als eine der aktivsten Ransomware-Gruppen etabliert. Die ersten Versionen von Akira basierten auf dem durchgesickerten Conti-Quellcode. Später entwickelte die Gruppe eine Rust-basierte Ransomware namens Megazord. Die Gruppe gab Megazord jedoch zugunsten der C/C++ basierte Variante, die nun für ESXi-Versionen 6 und 7 sowie Windows x86 und x64 kompiliert ist. Die neueste Variante verwendet die GNU Multiple Precision Arithmetic Library (GMP) für die RSA-Verschlüsselung anstelle der nativen Windows-APIs früherer Versionen. Interessanterweise verwendete Black Basta zuvor dieselbe GMP-Bibliothek für die asymmetrische Verschlüsselung in seiner Ransomware (vor der Migration auf die Crypto++ Bibliothek).

Die mit Akira verbundenen Unternehmen konzentrieren sich weiterhin in erster Linie auf die Dateiverschlüsselung und nicht auf den Diebstahl großer Datenmengen. Das Volumen der Datenexfiltration durch Akira-Partner ist im Durchschnitt geringer als bei vielen anderen Ransomware-Gruppen, die einzelnen Opfern Daten im Terabyte-Bereich oder mehr stehlen. Tatsächlich betrugen die durchschnittlichen und mittleren Datendiebstahlvolumina auf der Dataleak-Website von Akira (siehe Abbildung 27) 44,87 GB bzw. 14,33 GB. Der größte Datendiebstahl belief sich auf etwa 370 GB und war damit weitaus kleiner als bei vielen der größten Ransomware-Familien. Obwohl Akira keinen Schwerpunkt auf Datendiebstahl legt, gibt es eine beträchtliche Zahl von Opfern und insgesamt ist die Gruppe für Datenverluste von über 13 TB verantwortlich.

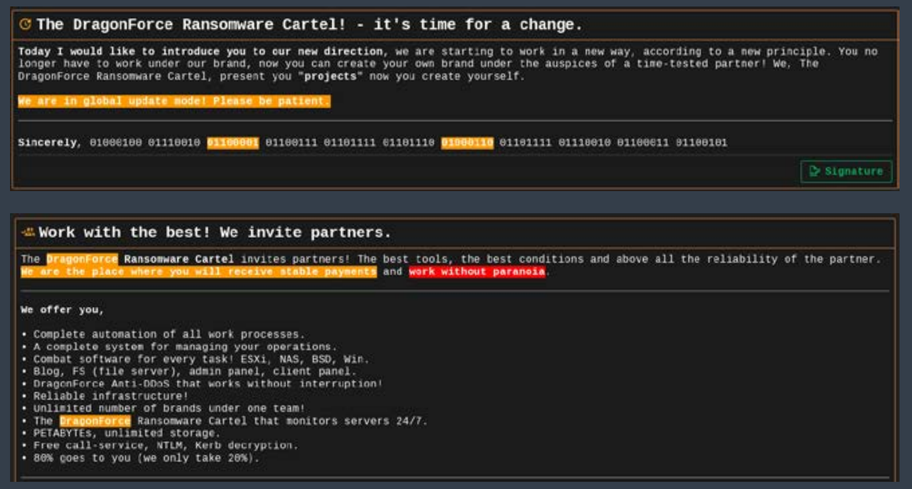


Abb. 26: Bekanntgabe des „Kartell“-Modells von DragonForce



Abb. 27: Dataleak-Website der Akira-Gruppe

© 2025 Zscaler, Inc. Alle Rechte vorbehalten.

5. Interlock

Interlock ist eine neuere Ransomware-Gruppe, die seit mindestens September 2024 Angriffe durchführt und bisher rund 50 Unternehmen kompromittiert hat. Die Angriffe von Interlock erstrecken sich über verschiedene Sektoren, darunter Gesundheitswesen, Bildung, Finanzen, Regierung und Fertigung. Die beiden erstgenannten Sektoren wurden von Interlock besonders hart getroffen. Diese gezielte Angriffsstrategie ist wahrscheinlich auf die ausgeprägte Kenntnis der Gruppe über Compliance-Rahmenwerke wie DSGVO, HIPAA, CCPA, NYDFS und GLBA zurückzuführen. Interlock versucht, diese Vorschriften auszunutzen, um die Opfer zur Zahlung eines Lösegelds zu drängen. Tatsächlich werden in den **Lösegeldforderungen** von Interlock ausdrücklich die finanziellen Strafen für solche Verstöße genannt.

Die Gruppe hat Ransomware-Varianten für Windows, Linux und FreeBSD entwickelt. Bemerkenswert daran ist lediglich, dass spezielle Builds für FreeBSD eher ungewöhnlich sind. Da jedoch viele große Unternehmen FreeBSD zum Betreiben kritischer Serverinfrastrukturen verwenden, ist dies nicht überraschend und wird auch weiterhin ein Ziel bleiben.

Ähnlich wie Dark Angels stiehlt Interlock große Datenmengen von Unternehmen. In einem Fall stahl Interlock mehr als 11 TB Daten von einem einzigen Opfer. Ein weiteres Opfer im Gesundheitswesen verlor mehr als 5 TB Daten und zahlte über 2,5 Mio. USD Lösegeld. Insgesamt hat die Gruppe allein in den letzten neun Monaten mehr als 73,5 TB an Daten gestohlen. Im Durchschnitt verlor jedes Opfer 1,6 TB an Daten, wobei der mittlere Verlust bei etwa 700 GB lag.

Der Abschnitt „Über uns“ auf der Dataleak-Website von Interlock, der in Abbildung 28 dargestellt ist, verdeutlicht die Haltung der Gruppe gegenüber den Opfern. Interlock macht „Leichtsinn“ und „Fahrlässigkeit“ der Opfer als Hauptursache für die erfolgreichen Ransomware-Angriffe der Gruppe verantwortlich.

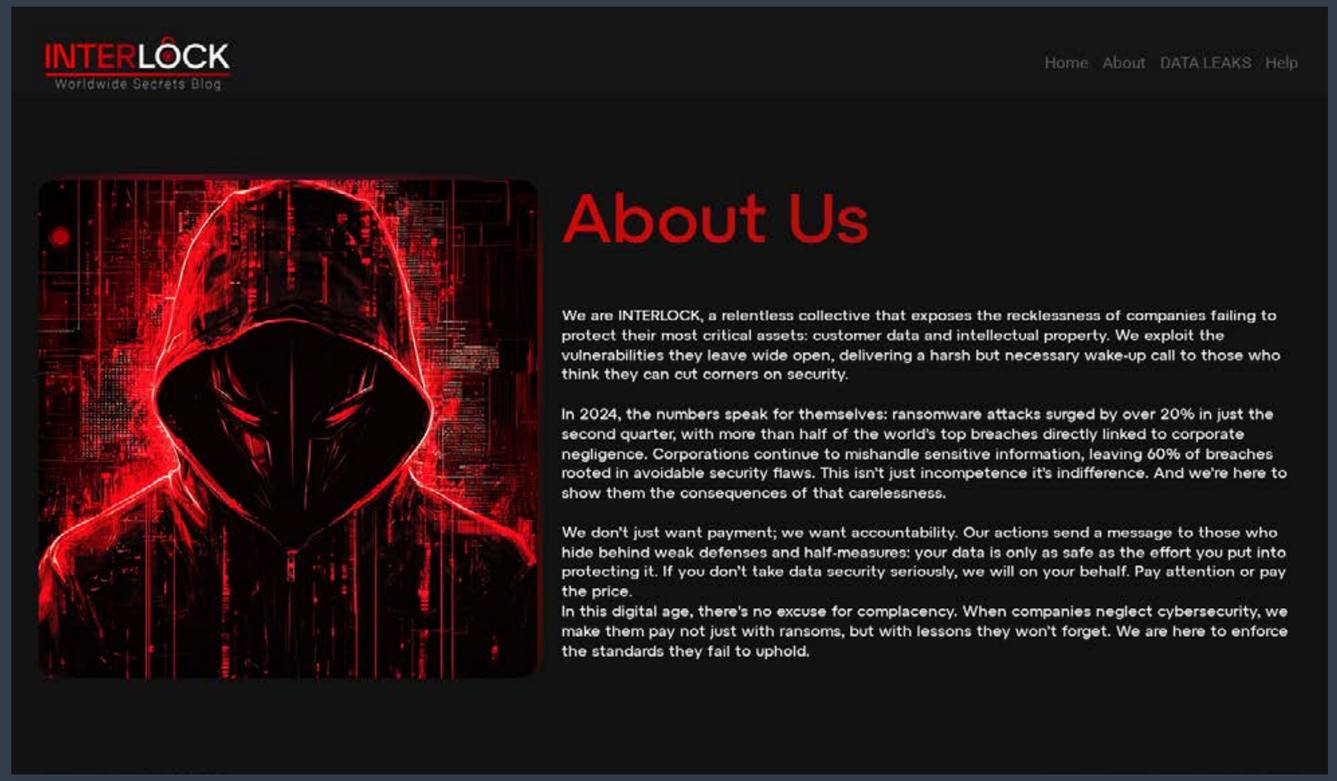


Abb. 28: „Über uns“-Seite der Interlock-Gruppe

© 2025 Zscaler, Inc. Alle Rechte vorbehalten.

Ransomware-Archiv von ThreatLabz

Zscaler ThreatLabz pflegt ein **öffentliches GitHub-Repository**, in dem zum Zeitpunkt der Erstellung dieses Artikels im vergangenen Jahr 73 neue Lösegeldforderungen von Ransomware-Gruppen hinzugefügt wurden, sodass sich die Gesamtzahl auf 1.018 erhöht. Dieses Archiv kann hilfreich sein, um Ransomware-Gruppen im Laufe der Zeit zu verfolgen, einschließlich ihrer Dataleak-Websites und Verhandlungstaktiken. Darüber hinaus können mithilfe stilometrischer Analysen Ransomware-Gruppen identifiziert werden, die sich umbenennen.



© 2025 Zscaler, Inc. Alle Rechte vorbehalten.



Prognosen für 2026

1. Ransomware-Gruppen werden GenAI als Waffe für skalierbare, mehrphasige Erpressungskampagnen einsetzen.

Generative KI wird zunehmend zur Kerninfrastruktur für Ransomware-Operationen. Geleakte Nachrichten der Black Basta-Gruppe enthüllen, wie Ransomware-Bedrohungsakteure bereits Tools wie ChatGPT verwenden, um Phishing-Köder und gefälschte Dokumente zu generieren, Malware zu debuggen und umzuschreiben und Deepfake-Inhalte zu erstellen. In Zukunft ist davon auszugehen, dass dieses Modell durch Ransomware-Operationen erweitert wird — mit enormen Möglichkeiten, einschließlich der Verwendung von LLMs zur Analyse und Zusammenfassung gestohlener vertraulicher Daten. Da Unternehmen zudem immer mehr Daten für KI-Trainingszwecke sammeln, werden diese Daten zu lukrativen Zielen für Ransomware-Gruppen.

2. Ransomware-Gruppen werden weiterhin mehrstufige Social-Engineering-Angriffe durchführen.

Ransomware-Betreiber werden ihre gezielten Angriffe verdoppeln und Massen-Spam-Kampagnen durch hochpräzises Social Engineering ersetzen. Mithilfe von Plattformen wie LinkedIn und ZoomInfo ermitteln sie Mitarbeiter mit erweiterten Zugriffsberechtigungen, überfluten Posteingänge mit Spam und geben sich dann per Telefonanruf als IT-Mitarbeiter aus, um sich Zugriff zu verschaffen.

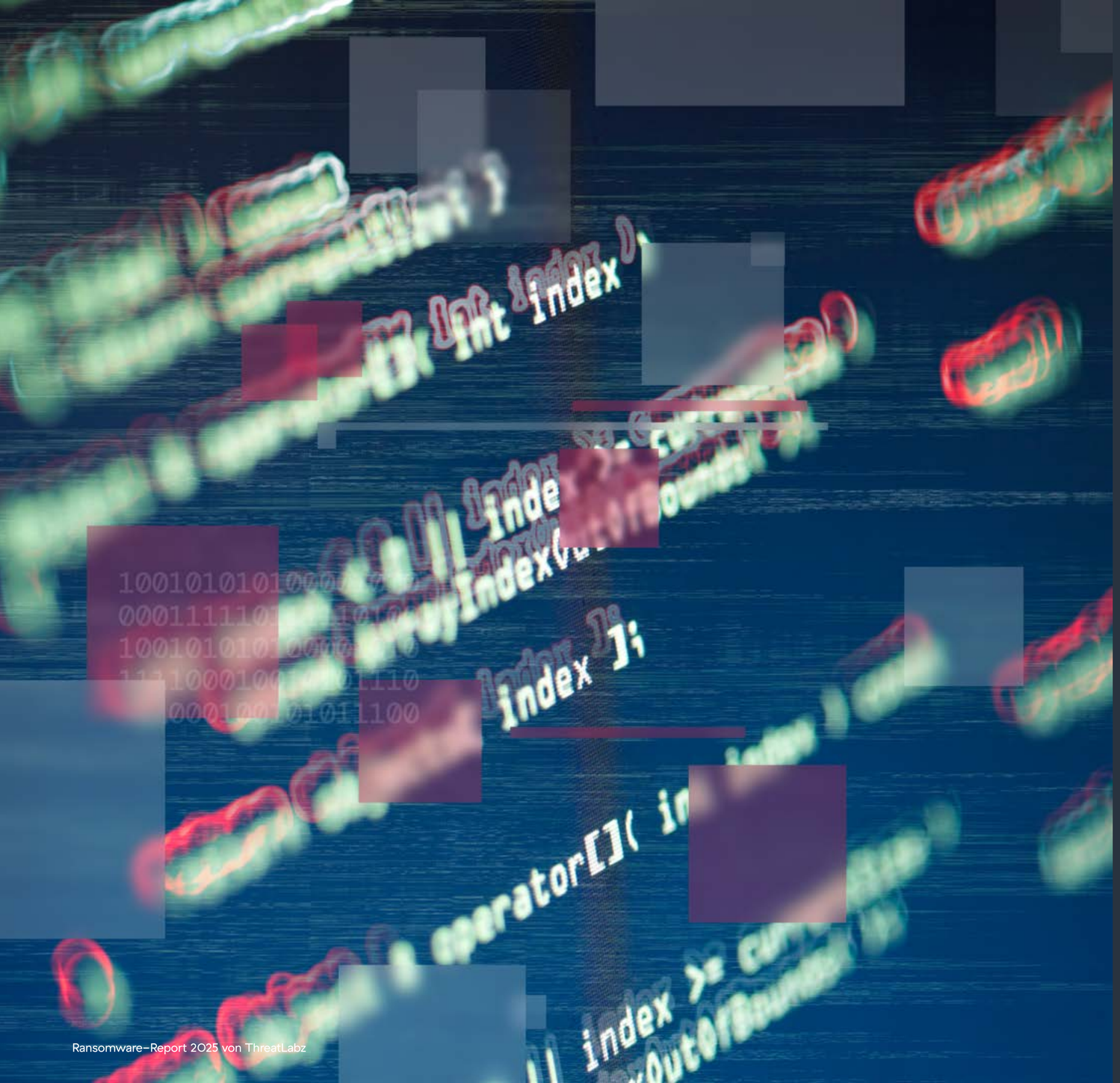
3. Sprachbasierte Angriffe werden zunehmen, da die Betreiber von Ransomware ihre Social-Engineering-Taktiken optimieren.

Ransomware-Gruppen werden weiterhin sprachbasierte Angriffsvektoren durch Voice-Phishing („Vishing“) und KI-generierte Audiodaten nutzen, um sich Zugriff auf die IT-Umgebungen ihrer Opfer zu verschaffen. Bei diesen Taktiken werden das menschliche Vertrauen und die Dringlichkeit ausgenutzt. Oft geben sich die Täter als Führungskräfte oder IT-Fachkräfte aus, um die Mitarbeiter dazu zu bringen, ihre Anmeldedaten preiszugeben oder Zugriff auf interne Systeme zu gewähren. Da generative KI-Tools immer zugänglicher werden, werden Ransomware-Bedrohungsakteure das Vishing im Wesentlichen auf Autopilot stellen und Taktiken wie mehrsprachiges Stimmenklonen und adaptive Anrufskripte nutzen, um Unternehmensmitarbeiter zu täuschen und Tür und Tor für Verschlüsselung und Erpressung zu öffnen.

4. Datenerpressung wird weiterhin ein Hauptgrund für Lösegeldzahlungen sein, und die Zahl der Diebstähle wird zunehmen.

Datendiebstahl wird zum wichtigsten Hebel bei Ransomware-Kampagnen, und dieser Trend wird sich weiter verstärken. Gruppen wie Clop, BianLian und Hunters International haben den Übergang zu reinen Erpressungsangriffen vorangetrieben und die Verschlüsselung vollständig aufgegeben. ThreatLabz stellte fest, dass mehrere dieser Gruppen mittlerweile durchschnittlich Hunderte Gigabyte pro Opfer stehlen. Da Unternehmen ihre Sicherungs- und Wiederherstellungsfunktionen verbessern, werden Bedrohungsakteure gestohlene Daten zunehmend als Waffe einsetzen, um die betroffenen Unternehmen zur Zahlung zu drängen.

© 2025 Zscaler, Inc. Alle Rechte vorbehalten.



5. Geleakte Quellcodes und Ransomware-Builder werden die nächste Generation von Angriffen begünstigen.

Da weiterhin Tools und Quellcodes zur Erstellung von Ransomware (absichtlich oder unabsichtlich) geleakt werden, wird es zu einer neuen Welle von Angriffen mit geringem Aufwand und großer Wirkung kommen. Lecks bei großen Ransomware-Gruppen haben bereits zu Spin-off-Operationen, umbenannten Varianten und Nachahmerkampagnen geführt. Neue Gruppen werden auf geleaktem Code aufbauen, Payloads und Übermittlungstechniken modifizieren und dabei vorhandene Erkennungssignaturen umgehen.

6. Die Strafverfolgungsbehörden werden ihren Fokus künftig stärker auf die Zerschlagung der Ransomware-Infrastruktur richten.

Die Einsätze der internationalen Strafverfolgungsbehörden werden immer effektiver und gezielter. Sie schalten nicht nur Ransomware-Gruppen aus, sondern auch die Infrastruktur und Services, die ihre Angriffe ermöglichen. Die Operation Endgame hat gezeigt, dass Plattformen zur Verbreitung von Malware in großem Maßstab zerschlagen werden können.

7. Ransomware-Partner werden weiterhin zwischen Gruppen wechseln.

Das Ransomware-as-a-Service-Modell (RaaS) bietet Partnern Flexibilität — und sorgt für eine unberechenbare Bedrohungslage. Partner wechseln häufig zwischen Gruppen. Den Ausschlag dafür geben Faktoren wie Druck seitens der Behörden, Auszahlungsbedingungen, Tools oder Ruf. Diese ständige Bewegung führt zu einer recycelten Infrastruktur, überlappenden Taktiken und schnellen Umbenennungen, wenn der Betrieb unterbrochen wird. Solange Partner-Modelle profitabel bleiben und nur geringe Risiken bergen, wird sich dieses Muster fortsetzen.

© 2025 Zscaler, Inc. Alle Rechte vorbehalten.

Zero Trust + KI: Die Zscaler-Lösung zum Schutz vor Ransomware

Ransomware gedeiht in Umgebungen, die von fragmentierter Sicherheit, eingeschränkter Transparenz und flachen Netzwerkhierarchien mit implizitem Vertraue gekennzeichnet sind. Dennoch verlassen sich viele Unternehmen immer noch auf herkömmliche Sicherheitstools — Firewalls der nächsten Generation, VPNs und Einzelprodukte wie Anti-Malware —, die nicht für die Abwehr heutiger Bedrohungen konzipiert wurden.

Diese veralteten Architekturen schaffen mehr Risiken, als sie mindern. Sie hinterlassen kritische Lücken im Ransomware-Schutz, von blinden Flecken im verschlüsselten Datenverkehr bis hin zu isolierter Bedrohungstransparenz und komplexer, inkonsistenter Richtlinienverwaltung. Schlimmer noch: Diese Architekturen basieren auf weitreichenden, übermäßig freizügigen Zugriffsmodellen, die interne Ressourcen exponieren. Sobald Angreifer sich im Netzwerk eingenistet haben, können sie sich lateral durch das System bewegen. Dadurch wird es für Bedrohungsakteure einfacher, Ransomware zu verbreiten, ihre Berechtigungen zu erweitern und unbemerkt auf vertrauliche Daten zuzugreifen.

Die **Zscaler Zero Trust Exchange™** eliminiert diese Risiken, indem sie veraltete, netzwerkzentrierte Modelle durch eine Cloud-native, KI-gestützte Zero-Trust-Architektur ersetzt. Die einheitliche, skalierbare Plattform minimiert Risiken und optimiert den standortunabhängigen Ransomware-Schutz für User, Geräte und Anwendungen.

ZSCALER STOPPT RANSOMWARE IN ALLEN PHASEN DES ANGRIFFSZYKLUS:

- **Minimierung der Angriffsfläche:** Eliminieren Sie effektiv exponierte Infrastruktur, die von Ransomware angegriffen werden kann, indem Sie User, Anwendungen und Geräte hinter einem Cloud-Proxy verbergen, wo sie vom Internet aus nicht sichtbar oder auffindbar sind. Dadurch wird die Angriffsfläche deutlich verkleinert. Es gibt keine öffentlichen IP-Adressen und keinen direkten Netzwerkzugriff — Ransomware-Bedrohungsakteure können interne Ressourcen weder finden noch erreichen. Die Technologie zur Vorhersage von Sicherheitsverletzungen nutzt KI, um Angriffsszenarien zu simulieren und wahrscheinliche Pfade zu identifizieren, die Bedrohungsakteure ausnutzen könnten. So können Sicherheitsteams potenzielle Schwachstellen beheben, bevor ein Angriff erfolgt.

- **Schutz vor Kompromittierung:** Schützen Sie User vor dem Zugriff auf schädliche Inhalte und erkennen Sie unbekannte Bedrohungen, bevor sie Ihr Netzwerk erreichen, durch vollständige TLS/SSL-Überprüfung sowie Inline-Sandboxing und Isolierung. Diese Funktionen stoppen Ransomware, bevor sie ausgeführt werden kann, und minimieren so das Risiko einer Kompromittierung.

- **Schutz vor lateralen Bewegungen:** User bzw. Anwendungen werden direkt mit Anwendungen, nicht mit dem Netzwerk selbst verbunden. Dadurch wird das Risiko lateraler Bewegungen eliminiert. KI-gestützte Segmentierung passt den Zugriff basierend auf Userverhalten, Gerätestatus und Anwendungskontext an. Ransomware-Bedrohungen können sich nicht von einem System auf ein anderes ausbreiten, selbst wenn ein Endgerät kompromittiert ist. KI und Identity Threat Detection and Response (ITDR) helfen dabei, anomale Zugriffsmuster aufzudecken, während Deception-Technologie und Decoys Ransomware-Bedrohungsakteure in überwachte Fallen locken.

- **Schutz vor Datenexfiltration:** Erpresserische Ransomware-Kampagnen basieren auf dem Diebstahl vertraulicher Daten. Inline-DLP (Data Loss Protection), CASB und Funktionen zur Traffic-Überprüfung blockieren unbefugte Übertragungen an genehmigte Cloud-Apps, Schatten-IT und Command-and-Control-Infrastrukturen (C2).



© 2025 Zscaler, Inc. Alle Rechte vorbehalten.

ZU DEN WICHTIGSTEN KI-GESTÜTZTEN RANSOMWARE-SCHUTZMASSNAHMEN VON ZSCALER GEHÖREN:

- **Die Vorhersage von Sicherheitsverstößen** verhindert potenzielle Sicherheitsverletzungsszenarien mithilfe generativer KI und mehrdimensionaler Vorhersagemodelle.
- **Die Phishing- und C2-Erkennung** nutzt die KI-basierte Inline-Erkennung des Zscaler Secure Web Gateway, um bisher unbekannte Phishing-Websites und C2-Infrastrukturen zu erkennen und zu blockieren.
- **Inline-Sandboxing** bietet umfassenden Schutz vor Malware und Zero-Day-Bedrohungen durch die Verwendung fortschrittlicher KI-Modelle zur Analyse verdächtiger Dateien in einer kontrollierten Umgebung.
- **Zero Trust Browser** nutzt KI, um schädliche Webinhalte zu identifizieren und zu isolieren und so Datenverluste und die Verbreitung von Malware zu verhindern.
- **Bei der Segmentierung** wird maschinelles Lernen verwendet, um automatisch Empfehlungen für App-Segmente und Richtlinien zu generieren. Dadurch wird letztendlich sowohl die Angriffsfläche als auch die laterale Bewegungsfreiheit minimiert.
- **Dynamische, risikobasierte Richtlinien** bewerten kontinuierlich den Risikostatus von Usern, Geräten und Anwendungen mithilfe KI-gesteuerter Verhaltensanalysen, um dynamische Sicherheits- und Zugriffsrichtlinien durchzusetzen.
- **Durch die Datenerkennung und -klassifizierung** werden vertrauliche Daten auf allen Endgeräten, im Inline-Verkehr und in Cloud-Apps sofort gescannt und klassifiziert. Dadurch wird es für Ransomware schwieriger, vertrauliche Daten anzugreifen und zu verschlüsseln.
- **DLP-Kontrollmechanismen** blockieren unbefugte Datenübertragungen, unterstützt durch KI-basierte Inhaltsprüfung und Richtliniendurchsetzung, und verhindern so, dass Ransomware-Betreiber vertrauliche Daten stehlen, um sie zu erpressen.



MIT DER WEITERENTWICKLUNG DER RANSOMWARE-TAKTIKEN MÜSSEN SICH AUCH DIE ABWEHRMASSNAHMEN WEITERENTWICKELN. DIE ZSCALER ZERO TRUST EXCHANGE UNTERSTÜTZT UNTERNEHMEN DABEI, IHRE ANGRIFFSFLÄCHE ZU VERKLEINERN, NEUARTIGE UND SCHWER FASSBARE RANSOMWARE-BEDROHUNGEN ZU STOPPEN, LATERALE BEWEGUNGEN (AUCH NACH EINER KOMPROMITTIERUNG) ZU VERHINDERN UND ERPRESSUNGSVERSUCHE ZU UNTERBINDEN, BEVOR DATEN EXFILTRIERT WERDEN.

© 2025 Zscaler, Inc. Alle Rechte vorbehalten.

Checkliste zur Ransomware-Prävention

Zero Trust ist ein Muss, wenn es darum geht, Ransomware zu stoppen, kann aber alleine noch keine wirksame Ransomware-Abwehr gewährleisten. Darüber hinaus sind Maßnahmen auf mehreren Betriebsebenen erforderlich, darunter Mitarbeiterschulungen, sichere Backups und ein gut durchdachter Reaktionsplan.

Die hier vorgestellte Checkliste basiert auf Erkenntnissen von ThreatLabz-Experten und enthält die wirksamsten Schritte, die Sie unmttelbar umsetzen können, um Ihr Ransomware-Risiko zu verringern und langfristige Resilienz aufzubauen.

Sichern Sie Ihre Daten regelmäßig

- [ ] Führen Sie regelmäßig verschlüsselte Online- und Offline-Backups durch.
- [ ] Testen Sie Wiederherstellungsverfahren regelmäßig und passen Sie Sicherungsstrategien an die Weiterentwicklung der Ransomware-Taktiken an.

Erzwingen Sie die Multifaktor-Authentifizierung (MFA)

- [ ] Setzen Sie MFA für alle Userkonten durch, insbesondere für solche mit erweiterten Zugriffsberechtigungen.
- [ ] Integrieren Sie den Identitätsschutz, um Kontoübernahmen effektiv zu erkennen und zu blockieren.

Stärken Sie die Anwendungssicherheit

- [ ] Um zu verhindern, dass Ransomware-Akteure Schwachstellen ausnutzen, sollten Anwendungen nicht öffentlich exponiert werden.
- [ ] Implementieren Sie eine Zero-Trust-Architektur für interne Anwendungen, um sie vor Ransomware zu schützen.

Aktualisieren Sie Software und Systeme regelmäßig

- [ ] Wenden Sie neue Sicherheitspatches zur Schließung bekannter Schwachstellen möglichst zeitnah an.
- [ ] Nutzen Sie KI-gestützte Bedrohungsinformationen, um Patches basierend auf realen Risiken zu priorisieren.

Standardisieren Sie die Sicherheitsrichtlinien Ihres Unternehmens

- [ ] Stellen Sie sicher, dass für alle User einheitliche Sicherheitsverfahren gelten, einschließlich MFA, Software-Updates und Zugriffskontrollen.
- [ ] Wechseln Sie zu einer SSE-Architektur (Security Service Edge), um User On-Premise oder an Remote-Standorten zu schützen.

Wenden Sie Zugriffskontrollen nach dem Prinzip der minimalen Rechtevergabe an

- [ ] Implementieren Sie Richtlinien nach dem Prinzip der minimalen Rechtevergabe, um den Zugriff der User strikt auf die für ihre jeweiligen Rollen erforderlichen Daten und Systeme zu beschränken.
- [ ] Setzen Sie KI-gestützte Lösungen ein, um das Verhalten dynamisch zu analysieren und Berechtigungen entsprechend anzupassen.



© 2025 Zscaler, Inc. Alle Rechte vorbehalten.

Stärken Sie den Identitätsschutz

- [ ] Verwenden Sie ITDR-Tools, um falsch konfigurierte Identitäten zu überwachen, Schwachstellen im Active Directory zu beheben, die Angreifer ausnutzen, um Berechtigungen zu erweitern und sich lateral in der Umgebung zu bewegen, und um heimliche Identitätsbedrohungen zu erkennen.

Verwenden Sie KI-gesteuerte Browserisolierung

- [ ] Isolieren Sie Benutzersitzungen sicher vom Internet, um Drive-by-Downloads, Phishing und den Diebstahl von Anmeldedaten zu verhindern.
- [ ] Ermöglichen Sie Usern den Zugriff auf verdächtige Websites in einer isolierten, schreibgeschützten Umgebung.

Setzen Sie Deception-Technologie ein

- [ ] Stellen Sie Fallen auf (z. B. Honeypots, gefälschte Anmeldedaten), um Angreifer frühzeitig in der Kill Chain zu erkennen und in die Irre zu führen.
- [ ] Verwenden Sie Warnmeldungen von Deception-Systemen, um die Reaktion auf Vorfälle zu beschleunigen.

Bieten Sie Ihren Mitarbeitern fortlaufende Schulungen an

- [ ] Informieren Sie User regelmäßig über Ransomware-Techniken, darunter Phishing, Social Engineering und gefälschte Software-Updates.
- [ ] Simulieren Sie reale Angriffsszenarien, um die Reaktionsfähigkeit Ihrer Mitarbeiter zu verbessern.

Überprüfen Sie den gesamten verschlüsselten und unverschlüsselten Traffic

- [ ] 87 % aller Bedrohungen verbergen sich in verschlüsselten Kanälen. Untersuchen Sie den gesamten Traffic, ob verschlüsselt oder nicht, um versteckte Bedrohungen aufzudecken und Kompromittierungen zu verhindern.

Implementieren Sie KI-gestütztes Sandboxing

- [ ] Erkennen und blockieren Sie neuartige Malware mit KI/ML-gestützter verhaltensbasierter Analyse.
- [ ] Stellen Sie verdächtige Dateien unter Quarantäne, bevor sie die Endgeräte erreichen.

Steuern Sie den SaaS-Zugriff mit einem CASB

- [ ] Überwachen und verwalten Sie die Nutzung von Cloud-Apps, um schädliche Aktivitäten wie Dateidownloads und Datenexfiltration zu blockieren.
- [ ] Setzen Sie Richtlinien für die gemeinsame Nutzung und das Herunterladen von Daten durch.

Erstellen Sie einen getesteten Ransomware-Reaktionsplan

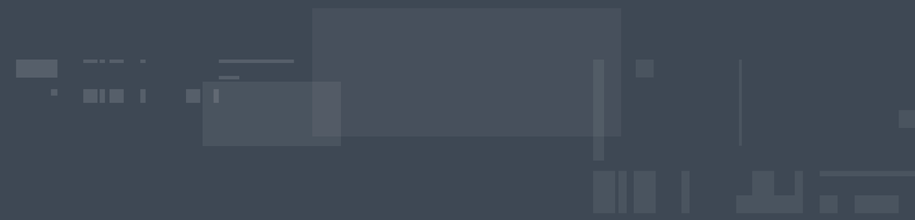
- [ ] Schließen Sie Verfahren zur Datenwiederherstellung, Reaktion auf Vorfälle und Kommunikationsprotokolle ein.
- [ ] Führen Sie regelmäßig Planspiele durch, um die Bereitschaft zu bewerten und etwaige Lücken zu schließen.

Implementieren Sie Zero Trust Network Access (ZTNA)

- [ ] Ersetzen Sie den umfassenden Netzwerkzugriff durch eine präzise, identitätsbasierte Segmentierung einzelner Verbindungen.
- [ ] Vermitteln Sie Zugriff nach dem Prinzip der minimalen Rechtevergabe, um laterale Bewegungen zu verhindern und die Angriffsfläche zu verringern.

Implementieren Sie Inline-DLP (Data Loss Prevention)

- [ ] Verhindern Sie Datenexfiltration und die Übertragung vertraulicher Dateien durch den Einsatz von Inline-DLP-Maßnahmen.
- [ ] Wenden Sie Richtlinien auf Web-, Cloud- und E-Mail-Kanäle an.



© 2025 Zscaler, Inc. Alle Rechte vorbehalten.

Forschungsmethodik

Diesem Report liegt ein umfassender Forschungsprozess zugrunde, in dessen Rahmen Daten aus verschiedenen Quellen analysiert wurden, um Ransomware-Trends zu erkennen und zu verfolgen. Das ThreatLabz-Team erfasste im Zeitraum von April 2024 bis April 2025 Daten aus folgenden Quellen:

- **Die globale Security Cloud von Zscaler.** Die Cloud von Zscaler verarbeitet täglich über 500 Billionen Signale, blockiert dabei mehr als 9 Milliarden Bedrohungen und Richtlinienverstöße und führt über 250.000 Sicherheitsupdates pro Tag für Zscaler-Kunden durch. Wir haben diese Daten, die Informationen zu Quell-IP-Adressen, Ziel-IP-Adressen und Dateitypen im Zusammenhang mit Ransomware-Angriffen enthalten, analysiert, um Ransomware-Aktivitäten zu identifizieren.

- **Analysen des TreatLabz-Teams von Ransomware-Samples und Angriffsdaten.** ThreatLabz verfolgt Ransomware-Gruppen und Bedrohungsakteure sowie die entsprechende Angriffstelemetrie. Das Team führt tiefgreifendes Reverse Engineering durch, um die von Erstzugriffsbrokern verwendeten Tools sowie die Ransomware selbst, einschließlich der Dateiverschlüsselungsalgorithmen, zu verstehen. In mehreren Fällen hat das Team kryptografische Schwachstellen entdeckt, die ausgenutzt werden können, um Dateien ohne Zahlung eines Lösegelds zu entschlüsseln, und Entschlüsselungstools entwickelt. Das Team stellt diese Tools internationalen Strafverfolgungsbehörden kostenlos zur Verfügung. ThreatLabz hat außerdem eine proprietäre Malware-Automatisierungsplattform entwickelt, die Bedrohungen in der Zscaler-Cloud automatisch erkennen und stoppen kann.

- **Externe Informationsquellen.** Wir haben außerdem unsere eigenen Daten zusammengestellt und gegebenenfalls mit Open-Source-Recherchen verglichen.

Über ThreatLabZ

ThreatLabz ist als Forschungsabteilung von Zscaler für die Früherkennung neuer Bedrohungen zuständig. Dieses erstklassige Team sorgt dafür, dass die Tausenden von Organisationen, die weltweit mit der globalen Zscaler-Plattform arbeiten, jederzeit geschützt sind. Neben der Erforschung und Verhaltensanalyse von Malware-Bedrohungen tragen die ThreatLabz-Experten auch zur Entwicklung neuer Prototypen für Advanced Threat Protection auf der Zscaler-Plattform bei und führen regelmäßig interne Revisionen durch, um sicherzustellen, dass Zscaler-Produkte und -Infrastrukturen die geltenden Sicherheitsstandards erfüllen. Detaillierte Analysen neuer Bedrohungen werden regelmäßig unter **research.zscaler.com** veröffentlicht.

Folgen Sie Zscaler ThreatLabz, **um regelmäßig Einblicke in die neuesten Ransomware-Bedrohungen und -Entwicklungen zu erhalten, einschließlich veröffentlichter IOCs (Indicators of Compromise) und MITRE ATT&CK-Zuordnungen. Mit diesen Informationen können Sie Ihr Team schulen, Ihren Sicherheitsstatus verbessern und Ransomware-Angriffe verhindern.**

ThreatLabz unterhält außerdem GitHub-Repositories mit IOCs, Tools (einschließlich Proof-of-Concept-Tools zur Entschlüsselung von Ransomware) und ein Archiv mit Lösegeldforderungen aller großen Ransomware-Gruppen.

X @ThreatLabz
ThreatLabz-Blog

Über Zscaler

Zscaler (NASDAQ: ZS) unterstützt Sie bei der digitalen Transformation – für agiles, effizientes, unterbrechungsfreies und sicheres Arbeiten. Die Zscaler Zero Trust Exchange™ schützt tausende Kunden mittels sicherer Verbindungen zwischen Usern, Geräten und Anwendungen an jedem beliebigen Standort vor Cyberangriffen und Datenverlusten. Als weltweit größte Inline-Cloud-Sicherheitsplattform wird die SASE-basierte Zero Trust Exchange in über 160 Rechenzentren auf der ganzen Welt bereitgestellt. Weitere Informationen erhalten Sie unter www.zscaler.com/de.

© 2025 Zscaler, Inc. Alle Rechte vorbehalten.



zscaler™ | Zero Trust Everywhere

Über Zscaler

Zscaler (NASDAQ: ZS) unterstützt Sie bei der digitalen Transformation – für agiles, effizientes, unterbrechungsfreies und sicheres Arbeiten. Die Zscaler Zero Trust Exchange™ schützt tausende Kunden mittels sicherer Verbindungen zwischen Usern, Geräten und Anwendungen an jedem beliebigen Standort vor Cyberangriffen und Datenverlusten. Die in 160 Rechenzentren auf der ganzen Welt verfügbare SSE-basierte Zero Trust Exchange™ ist die weltweit größte Inline-Cloud-Sicherheitsplattform. Weitere Informationen finden Sie unter **zscaler.com/de** — oder folgen Sie uns auf Twitter unter **@zscaler**.

©2025 Zscaler, Inc. Alle Rechte vorbehalten. Zscaler™ sowie weitere unter **zscaler.com/de/legal/trademarks** aufgeführte Marken sind entweder (i) eingetragene Handelsmarken bzw. Dienstleistungsmarken oder (ii) Handelsmarken bzw. Dienstleistungsmarken von Zscaler, Inc. in den USA und/oder anderen Ländern. Alle anderen Marken sind Eigentum ihrer jeweiligen Inhaber.

Zscaler, Inc. (Hauptsitz) Welche Strategie verfolgen Sie bei der Netzwerktransformation? 120 Holger Way Welche Strategie verfolgen Sie bei der Netzwerktransformation? San Jose, CA 95134, USA

+1 408 533 0288 **zscaler.com/de**

