Ransomware-Report von ThreatLabz 2024

Inhaltsverzeichnis

Kurzfassung

Ransomware-Angriffe sind im vergangenen Jahr noch ambitionierter und dreister geworden, was sich in einem deutlichen Anstieg solcher Erpressungsangriffe niederschlägt. Zusätzlich zu der Zunahme von Ransomware-Angriffen deckte das ThreatLabz-Forschungsteam **eine Lösegeldzahlung in Höhe von 75 Millionen US-Dollar auf** — die höchste, die jemals von einem Unternehmen gezahlt wurde. Dieser Betrag ist fast doppelt so hoch wie die höchste bisher bekannte Lösegeldzahlung.[1] Allein im Jahr 2023 überstiegen die Lösegeldzahlungen 1 Milliarde US-Dollar, was die enormen finanziellen Auswirkungen derartiger Cyberverbrechen verdeutlicht.

Da Cyberkriminelle ihre Angriffe sogar auf die Kinder von Führungskräften ausdehnen, um schnellere und höhere Lösegeldzahlungen zu erzwingen, zeichnet sich immer deutlicher ab, dass sie vor niemandem Halt machen.[2] Von kritischer Infrastruktur[3] und Großunternehmen[4] bis hin zu kleinen und mittelständischen Unternehmen ist keine Organisation mehr sicher davor, ins Fadenkreuz der nächsten Kampagne oder der sich ständig weiterentwickelden Angriffe zu geraten.

Trotz der strafrechtlichen Verfolgung mehrere Initial Access Broker in den Operationen „Endgame“ und „Duck Hunt“ bleiben die größten Ransomware-Gruppen standhaft, gruppieren sich nach Zwischenfällen schnell neu und starten offensiv neue Angriffe. Leider sind viele Ransomware-Akteure für die Strafverfolgungsbehörden unerreichbar und können daher praktisch ungestraft mit ihren kriminellen Machenschaften fortfahren. Wie in diesem Bericht ausführlich beschrieben, haben die Strafverfolgungsbehörden ihre Druckmittel durch Belohnungen, Sanktionen, Trolling und die Aufdeckung der Personen, die hinter Ransomware stehen, durch verschiedene psychologische Taktiken, verstärkt.

Da die Ransomware-Angreifer ihre Strategien ständig weiterentwickeln, ist es von entscheidender Bedeutung, sich regelmäßig über die Veränderungen in der Bedrohungslandschaft zu informieren.

Der Ransomware-Report von Zscaler ThreatLabz 2024 bietet einen Überblick über die Ransomware-Bedrohungslandschaft von April 2023 bis April 2024 und beschreibt die neuesten Trends, Angriffsziele, Ransomware-Familien und effektive Verteidigungsstrategien.

ThreatLabz stellte anhand der blockierten Angriffsversuche in der Zscaler Cloud fest, dass Ransomware-Angriffe im Jahresvergleich um 17,8 % gestiegen sind, während die durch Analysen von Dataleak-Websites identifizierten Ransomware-Angriffe um 57,8 % zugenommen haben. Die am häufigsten angegriffenen Unternehmen waren in den Branchen Fertigung, Gesundheitswesen und Technologie tätig. Dadurch waren kritische Betriebsabläufe und Infrastrukturen direkt von den Angriffen betroffen.

Die in diesem Report vorgestellten Ergebnisse unterstreichen, wie wichtig es für Unternehmen ist, dem Schutz vor der unaufhaltsamen Welle von Ransomware-Angriffen Priorität einzuräumen. Die Erkenntnisse und Strategien in diesem Report dienen als wichtiger Leitfaden zur Verbesserung Ihrer Ransomware-Abwehr. Wenn Sie die neuesten Trends und Schwachstellen kennen und die empfohlenen Best Practices umsetzen, können Sie das Risiko, Opfer von Ransomware zu werden, erheblich reduzieren und die kritischen Ressourcen und Daten Ihres Unternehmens besser schützen.

[1] Bloomberg, **CNA Financial Paid $40 Million in Ransom After March Cyberattack**, 20. Mai 2021.
[2] Business Insider, **Hackers are now targeting the children of corporate executives in ransomware attacks**, 12. Mai 2024.
[3] Dark Reading, **Ascension Healthcare Suffers Major Cyberattack**, 10. May 2024.
[4] CyberScoop, **Boeing confirms attempted $200 million ransomware extortion attempt**, 8. Mai 2024.

Die wichtigsten Ergebnisse im Überblick

Das Forschungsteam von Zscaler ThreatLabz deckte eine Lösegeldzahlung in Rekordhöhe von 75 Millionen US-Dollar auf – die höchste Lösegeldzahlung eines Unternehmens aller Zeiten — fast doppelt so hoch wie die höchste bisher bekannte Zahlung.

Die Zahl der in der Zscaler Cloud blockierten Ransomware-Angriffe stieg um 17,8 %, und die Anzahl der erpressten Unternehmen auf Dataleak-Websites stieg im gleichen Zeitraum im Vergleich zum Vorjahr um 57,8 %. Und das trotz zahlreicher Strafverfolgungsmaßnahmen, einschließlich der Beschlagnahme von Infrastrukturen sowie Verhaftungen, Strafanzeigen und Sanktionen.

Die Branchen Fertigung, Gesundheitswesen und Technologie waren die Hauptziele von Ransomware-Angriffen. Währenddessen verzeichnete der Energiesektor im Vergleich zum Vorjahr einen Anstieg um 500 %, da kritische Infrastrukturen und die daraus resultierende Anfälligkeit für Betriebsunterbrechungen ihn für Cyberkriminelle besonders attraktiv machen.

Die Vereinigten Staaten bleiben mit 49,95 % der Gesamtangriffe das Hauptziel von Ransomware, gefolgt von Großbritannien, Deutschland, Kanada und Frankreich.

ThreatLabz identifizierte im Analysezeitraum 19 neue Ransomware-Familien, womit sich die Gesamtzahl seit Beginn unserer Aufzeichnungen auf 391 erhöht hat.

Die aktivsten Ransomware-Familien waren **LockBit (22,1 %)**, **BlackCat (auch bekannt als ALPHV) (9,2 %)**und **8Base (7,9 %)**.

Schwachstellen bleiben ein allzu häufiger Angriffsvektor für Ransomware. Dies unterstreicht die Bedeutung rechtzeitiger Patches und eines einheitlichen Schwachstellenmanagements, das durch eine Zero-Trust-Architektur unterstützt wird, um auch dann geschützt zu sein, wenn keine Patches verfügbar sind.

Sprachbasierte Social-Engineering-Angriffe werden zunehmend eingesetzt, um Zugriff auf Unternehmensnetzwerke zu erhalten — eine Technik, die von Scattered Spider und Qakbot verwendet wird.

Bedrohungslage durch Ransomware: Wichtige Trends und Angriffsziele

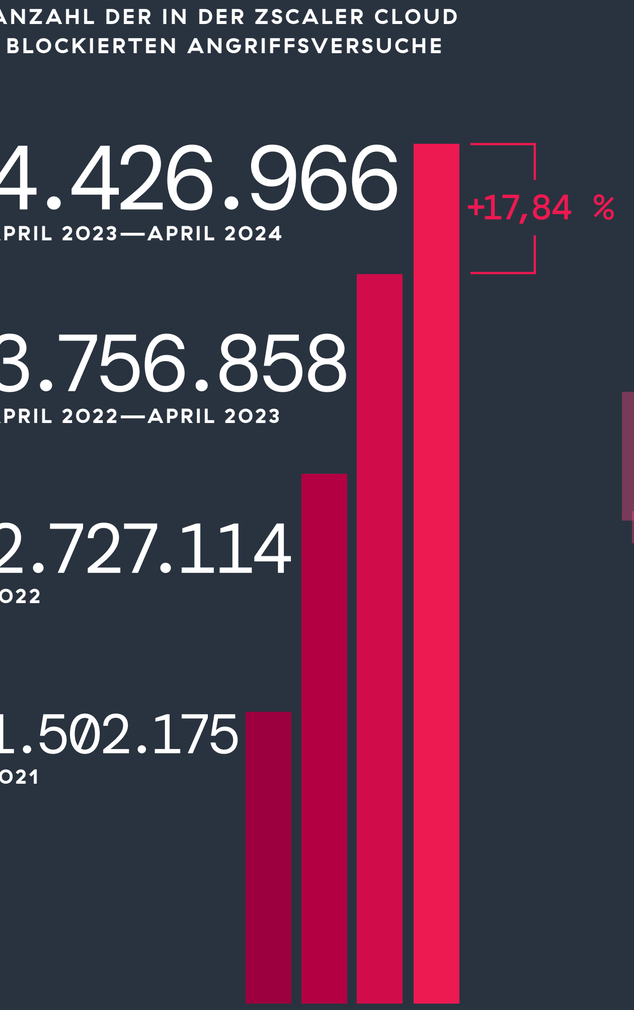
Aufgrund ihrer dynamischen Natur ist Ransomware in den letzten Jahren zu einem der größten Sicherheitsprobleme geworden. Bedrohungsakteure entwickeln ihre Angriffs- und Erpressungsmethoden ständig weiter und nutzen Fortschritte im Bereich der künstlichen Intelligenz (KI), geleakte Quellcodes und fortschrittliche Verschlüsselung, um ihre Schlagkraft und Rentabilität zu maximieren.

In diesem Report werden die folgenden Trends im Hinblick auf Ransomware-Angriffe von April 2023 bis April 2024 untersucht:

- Allgemeine Zunahme von Ransomware-Angriffen
- Branchen, die am stärksten von Ransomware betroffen sind
- Geografische Verteilung der angegriffenen Organisationen
- Verstärkte Strafverfolgungsmaßnahmen gegen Ransomware-Gruppen und Initial Access Broker
- Die größten Ransomware-Bedrohungen und rekordverdächtige Lösegeldzahlungen

Allgemeine Zunahme von Ransomware-Angriffen

Die neueste ThreatLabz-Analyse zeigt einen besorgniserregenden Trend: Im Vergleich zum Vorjahr ist die Zahl der Ransomware-Angriffe gemessen an den blockierten Versuchen in der Zscaler-Cloud um 17,84 % gestiegen. Diese Zunahme der Ransomware-Aktivitäten führt zu erheblichen Störungen und finanziellen Belastungen für betroffene Organisationen jeder Größe. Oftmals stören diese Angriffe den Geschäftsbetrieb, verursachen längere Ausfallzeiten, erhebliche Datenverluste und hohe Wiederherstellungskosten. Die finanzielle Belastung ist beträchtlich, da nicht nur Lösegeld gefordert wird, sondern auch die Wiederherstellung der Systeme und die Schadensbegrenzung mit hohen Kosten verbunden sein können. Angesichts dieser zunehmenden Bedrohungen ist der Bedarf an **robusten Maßnahmen zur Abwehr von Ransomware** größer denn je.



Branchen, die am stärksten von Ransomware betroffen sind

Ransomware-Angriffe stellen für Unternehmen jeder Größe und Branche ein erhebliches Risiko dar. Diese Angriffe können sensible Daten gefährden, zu hohen finanziellen Verlusten führen, die Business Continuity stören und den Ruf schädigen. Verschiedene Branchen stehen vor einzigartigen Herausforderungen im Zusammenhang mit Ransomware, je nachdem, wie sie arbeiten, mit welchen Daten sie zu tun haben und über welche technologische Infrastruktur sie verfügen.

Trotz der Variablen haben diese Erpressungsangriffe stetig zugenommen, wobei die Zahl der betroffenen Unternehmen, die auf Dataleak-Websites aufgeführt sind, seit dem ThreatLabz-Report über Ransomware-Trends im letzten Jahr um 57,81 % gestiegen ist. Die Fertigung war mit Abstand die am stärksten betroffene Branche und verzeichnete 653 Angriffe — mehr als doppelt so viele wie jede andere Branche.

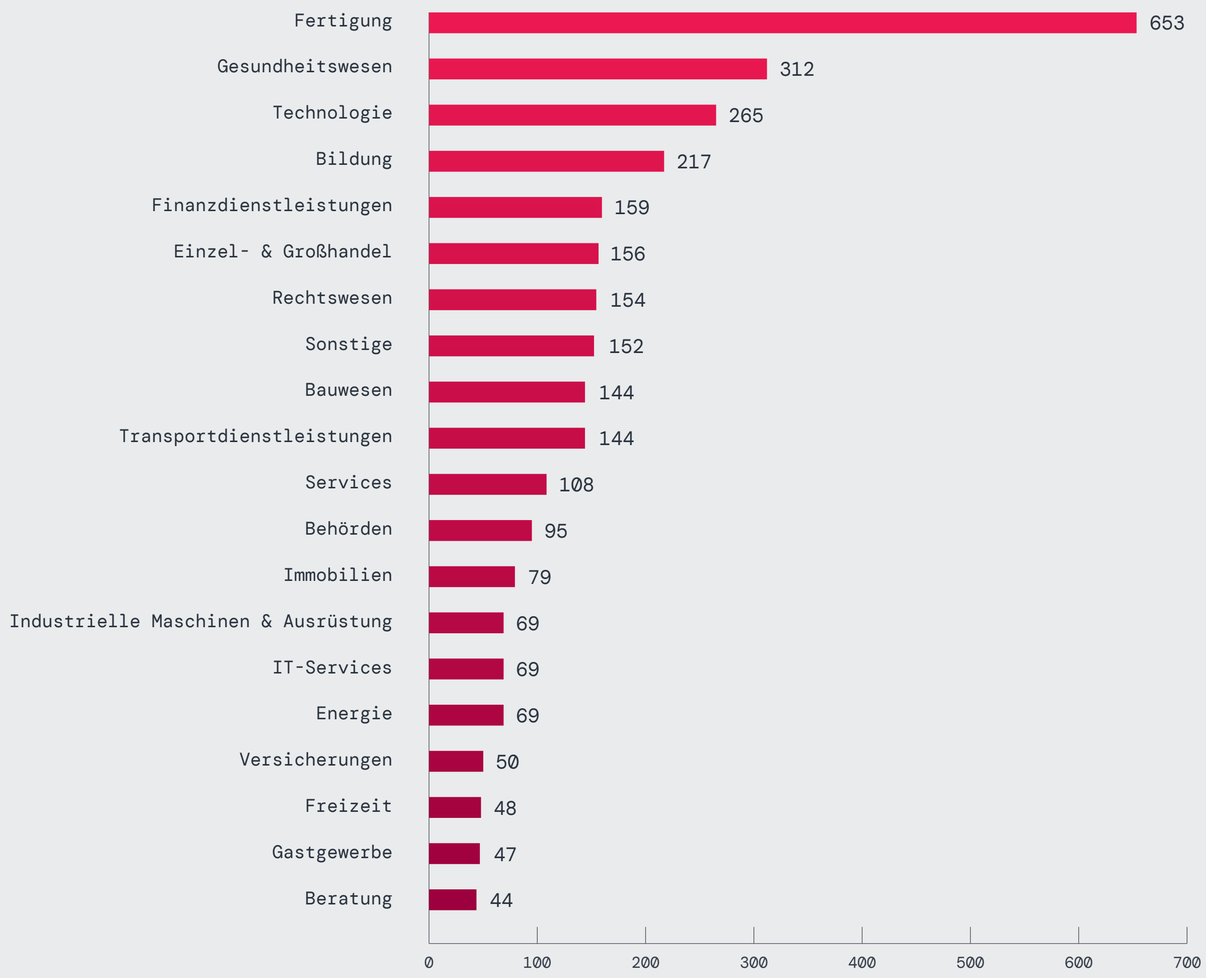


Abb . 1: Ransomware-Angriffe nach Branche basierend auf Dataleak-Websites (nur die 20 am häufigsten angegriffenen Branchen)

Trends im Jahresvergleich

Im Energiesektor war im Vergleich zum Vorjahr ein Anstieg der Ransomware-Angriffe um 527,27 % zu verzeichnen, was wahrscheinlich auf die kritische Natur des Sektors und das hohe Lösegeldpotenzial für Angreifer zurückzuführen ist.

In ähnlicher Weise kam es in der Gastronomie und im Lebensmittelsektor zu einem Anstieg solcher Angriffe um 333,33 %. Dies lässt sich auf die rasche Digitalisierung des Sektors zurückführen, die durch die Einführung moderner Kassensysteme und Online-Bestellplattformen beschleunigt wurde. Durch diese Technologien lassen sich zwar Abläufe optimieren und die Kundenerfahrung verbessern, sie können jedoch auch potenzielle Schwachstellen mit sich bringen.

Dieser Anstieg verdeutlicht zwar die Häufigkeit von Ransomware-Angriffen, erfasst aber möglicherweise nicht das volle Ausmaß der Vorfälle. Viele Angriffe werden nicht gemeldet bzw. werden ohne Information der Öffentlichkeit durch eine Lösegeldzahlung gelöst. Daher sind diese Zahlen als Hinweis auf allgemeine Trends bezüglich der branchenspezifischen Verbreitung von Ransomware und nicht als zuverlässige Darstellung der gesamten Bedrohungslage zu verstehen.

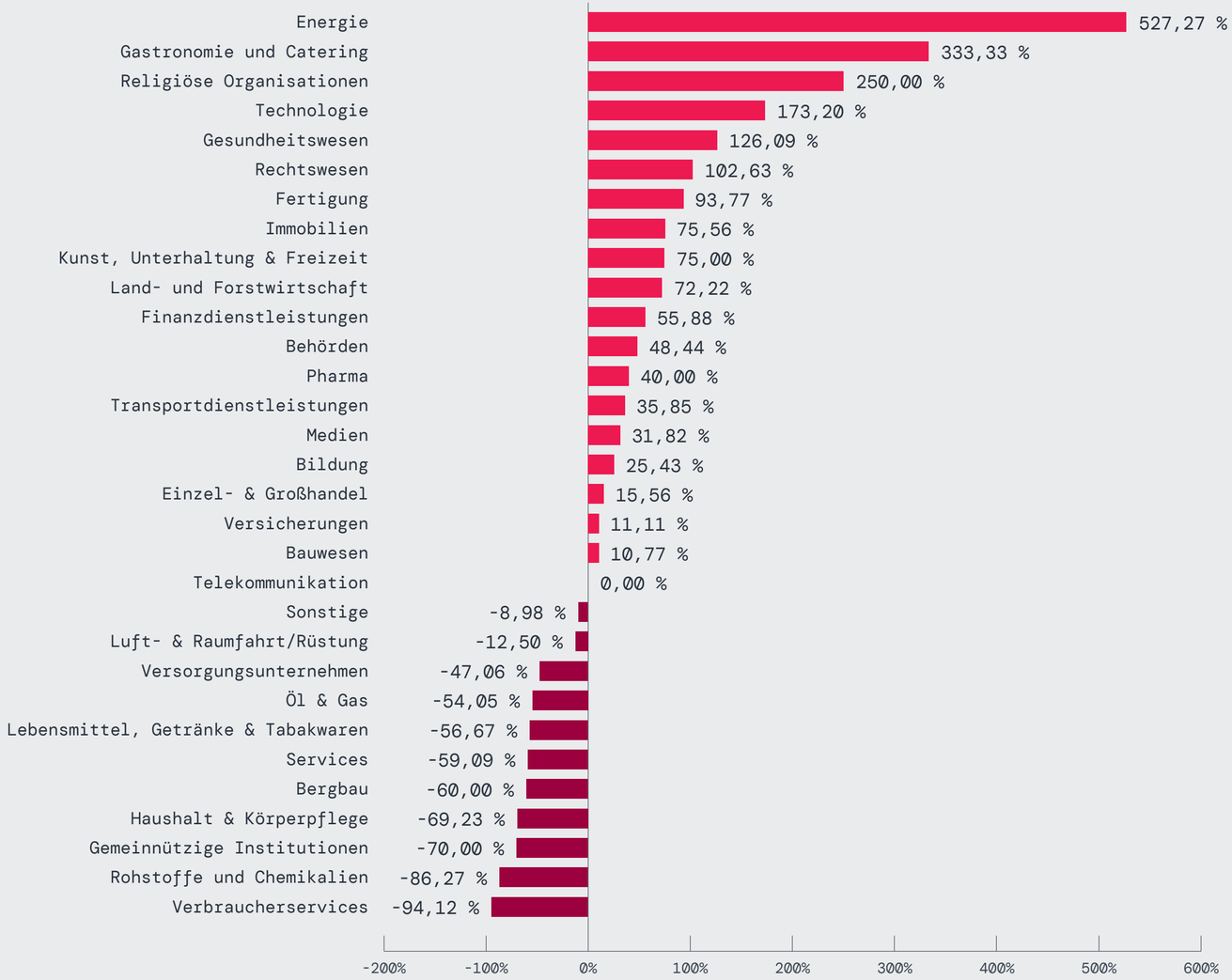


Abb. 2: Prozentuale Veränderung der Ransomware-Angriffe nach Branchen im Jahresvergleich. Es ist zu beachten, dass einige Sektoren im vergangenen Jahr eine relativ geringe Anzahl von Angriffen verzeichneten, sodass ihr Wachstum nun größer erscheint.

Geografische Verteilung der angegriffenen Organisationen

Die Vereinigten Staaten waren mit einer deutlich höheren Anzahl an Ransomware-Angriffen konfrontiert als jedes andere Land und verzeichneten etwa 50 % aller Vorfälle weltweit. Im Vergleich dazu war Großbritannien das am zweithäufigsten betroffene Land, auf das fast 6 % der Ransomware-Angriffe entfielen, gefolgt von Deutschland (4,09 %), Kanada (3,51 %) und Frankreich (3,26 %). Abbildung 3 zeigt eine Heatmap der Länder, die zwischen April 2023 und April 2024 von Ransomware betroffen waren.

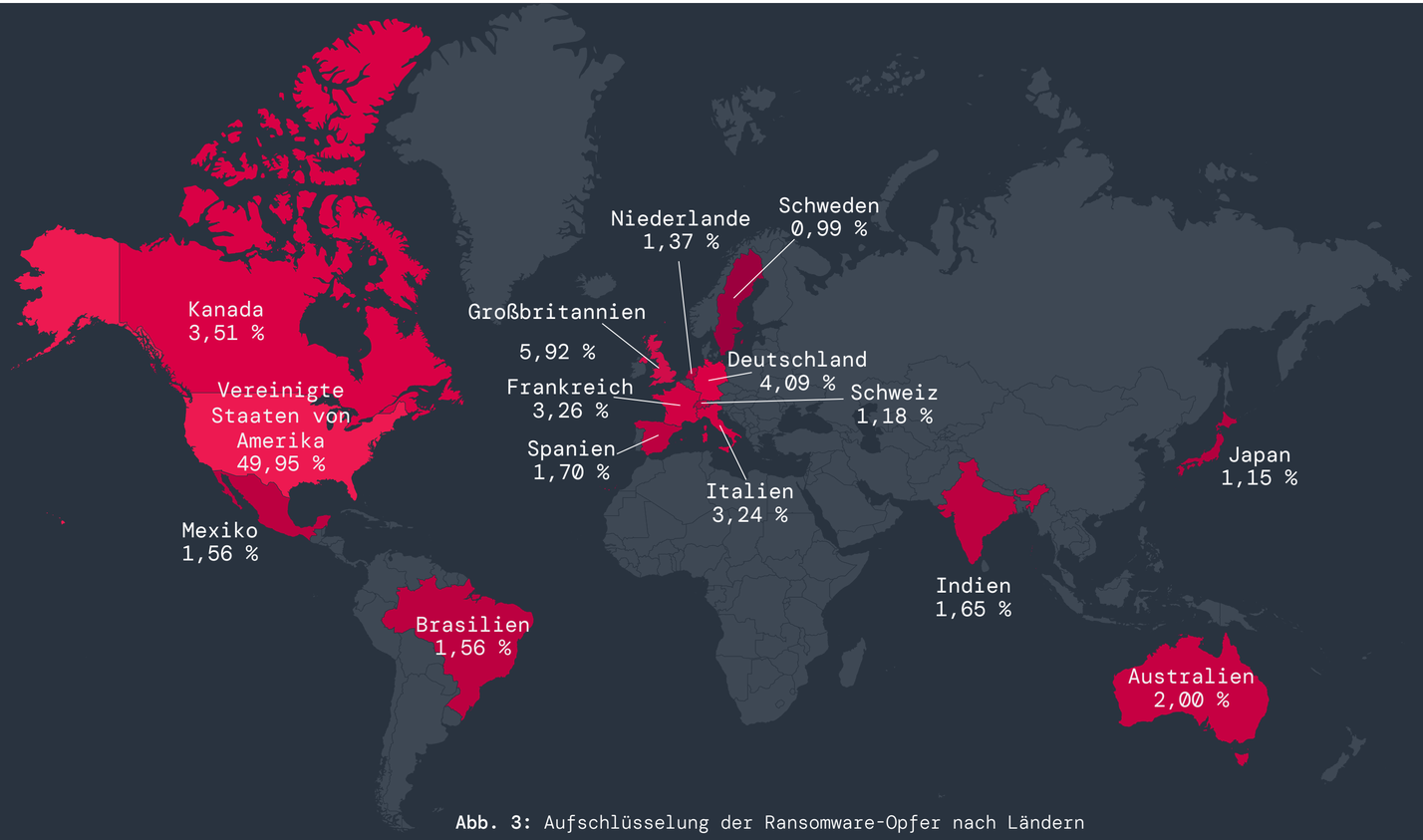


Abb. 3: Aufschlüsselung der Ransomware-Opfer nach Ländern

Kenntnisse über die Verteilung von Ransomware-Angriffen sind für die Risikobewertung, die Zuweisung von Ressourcen, die Entwicklung von Richtlinien, die internationale Zusammenarbeit und die Sensibilisierung der Öffentlichkeit bei der Bekämpfung von Ransomware-Bedrohungen von entscheidender Bedeutung.

Risikobewertung

Durch die Analyse besonders gefährdeter Regionen können Unternehmen in diesen Gebieten ihr eigenes Risikolevel einschätzen und stärkere Cybersicherheitsmaßnahmen implementieren. Einer Untersuchung von ThreatLabz zufolge entfallen 50 % der weltweiten Ransomware-Angriffe auf die USA. Daher sind Organisationen dort dazu angehalten, strengen Sicherheitsprotokollen Priorität einzuräumen.

Ressourcenzuweisung

Mit gezielten Daten können Regierungen und Organisationen Ressourcen strategisch zuteilen und ihren Sicherheitsstatus verbessern, indem sie den Bereichen mit den höchsten Bedrohungsstufen mehr Unterstützung, Finanzmittel und Fachpersonal zuweisen.

Richtlinienentwicklung

Regierungen können Erkenntnisse aus regionalen Ransomware-Angriffen nutzen, um die Gesetzgebung zu optimieren, Sicherheitsstandards zu verbessern, die internationale Zusammenarbeit zu fördern und den Informationsaustausch zwischen dem öffentlichen und dem privaten Sektor zu erleichtern. Ein aktuelles Beispiel hierfür sind die neuen Cybersicherheitsregeln der SEC, die einen wichtigen Schritt zur Verbesserung von Transparenz und Rechenschaftspflicht angesichts wachsender Bedrohungen darstellen.

Internationale Kooperation

Durch die Identifizierung der am häufigsten angegriffenen Länder können Strafverfolgungsbehörden, Organisationen und Regierungen koordinierte Maßnahmen zur Bekämpfung von Ransomware auf nationaler und internationaler Ebene ergreifen. Die Operationen „Duck Hunt“ und „Endgame“ zeigen beispielhaft, wie internationale Zusammenarbeit die Aktivitäten von Cyberkriminellen unterbinden kann.

Öffentliches Bewusstsein

Indem häufig betroffene Länder in den Fokus gerückt werden, können Einzelpersonen, Organisationen und Regierungen ermutigt werden, proaktivere Maßnahmen in Bezug auf Cybersicherheitstraining, Planung von Reaktionen auf Vorfälle und Investitionen in Abwehrtechnologien zu ergreifen.

Trends im Jahresvergleich

ThreatLabz verglich die Ransomware-Angriffe aus dem diesjährigen Report mit dem Ransomware-Report 2023, um Veränderungen zu beurteilen. Unter den 15 Ländern, die am häufigsten angegriffen wurden, verzeichneten die USA einen bemerkenswerten Anstieg von 101,88 % gegenüber dem Vorjahr. Schweden verbuchte einen Anstieg von unglaublichen 350 %, obwohl der Anteil an den Gesamtangriffen deutlich geringer war.

Die Analyse von Ransomware-Trends auf globaler Ebene ist zwar von unschätzbarem Wert, aber es ist auch wichtig, die spezifischen Entwicklungen in verschiedenen Regionen der Welt zu untersuchen. Durch die Untersuchung regionaler Aufschlüsselungen können Organisationen maßgeschneiderte Sicherheitspläne erstellen und Regierungen wirksamere Cybersicherheitsrichtlinien entwickeln.

VERÄNDERUNGEN BEI RANSOMWARE-ANGRIFFEN IN DEN 15 LÄNDERN, DIE AM HÄUFIGSTEN ANGEGRIFFEN WURDEN

Land	Ransomware-Angriffe nach Land (2023)	Ransomware-Angriffe nach Land (2024)	Prozentuale Veränderung
Vereinigte Staaten von Amerika	902	1821	101,88 %
Großbritannien	144	216	50,00 %
Deutschland	110	149	35,45 %
Kanada	151	128	-15,23 %
Frankreich	87	119	36,78 %
Italien	63	118	87,30 %
Australien	69	73	5,80 %
Brasilien	38	57	50,00 %
Spanien	36	62	72,22 %
Mexiko	31	57	83,87 %
Niederlande	17	50	194,12 %
Indien	62	60	-3,23 %
Schweiz	32	43	34,38 %
Japan	44	42	-4,55 %
Schweden	8	36	350,00 %

Abb. 5: Jahresvergleich der Ransomware-Angriffe nach Ländern

VERÄNDERUNGEN BEI DER HÄUFIGKEIT VON RANSOMWARE-ANGRIFFEN IN DER EMEA-REGION

Land	Von Ransomware-Angriffen betroffene Unternehmen (2023)	Von Ransomware-Angriffen betroffene Unternehmen (2024)	Prozentuale Veränderung
Großbritannien	144	216	50,00 %
Deutschland	110	149	35,45 %
Frankreich	87	119	36,78 %
Italien	63	118	87,30 %
Spanien	36	62	72,22 %
Niederlande	17	50	194,12 %
Schweiz	32	43	34,38 %
Schweden	8	36	350,00 %
Belgien	16	34	112,50 %
Südafrika	13	24	84,62 %
Österreich	15	24	60,00 %
Vereinigte Arabische Emirate	12	21	75,00 %

Abb. 6: Jahresvergleich der Ransomware-Angriffe nach Ländern in der EMEA-Region

VERÄNDERUNGEN BEI DER HÄUFIGKEIT VON RANSOMWARE-ANGRIFFEN IN ASIEN-PAZIFIK

Land	Von Ransomware-Angriffen betroffene Unternehmen (2023)	Von Ransomware-Angriffen betroffene Unternehmen (2024)	Prozentuale Veränderung
Australien	69	73	5,80 %
Indien	62	60	-3,23 %
Japan	44	42	-4,55 %
Thailand	13	25	92,31 %
Indonesien	15	23	53,33 %
Malaysia	14	20	42,86 %
Taiwan	23	17	-26,09 %
Philippinen	7	16	128,57 %
Singapur	8	16	100,00 %
China	21	15	-28,57 %
Südkorea	12	10	-16,67 %
Vietnam	10	10	0,00 %

Abb. 7: Jahresvergleich der Ransomware-Angriffe nach Ländern in Asien-Pazifik

Aktivste Ransomware-Gruppen in den Jahren 2023-2024

LockBit (22,1 %), BlackCat (9,2 %) und 8Base (7,9 %) waren im vergangenen Jahr die aktivsten Ransomware-Gruppen, die jeweils für eine beträchtliche Anzahl von Angriffen verantwortlich waren. Abbildung 8 zeigt die Anzahl der Opfer pro Ransomware-Familie während dieses Zeitraums.

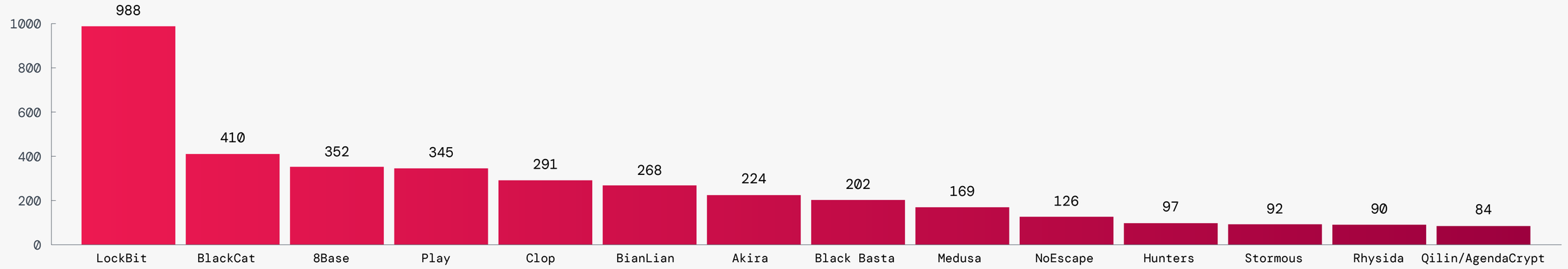


Abb. 8: Ransomware-Angriffe, die auf böswillig betriebenen Dataleak-Websites veröffentlicht wurden

Die neuesten Ransomware-Gruppen

Abbildung 9 zeigt eine Zeitleiste neuer Ransomware-Gruppen, die im Rahmen ihrer Erpressungsstrategie damit begannen, Daten auf Dataleak-Websites zu veröffentlichen.

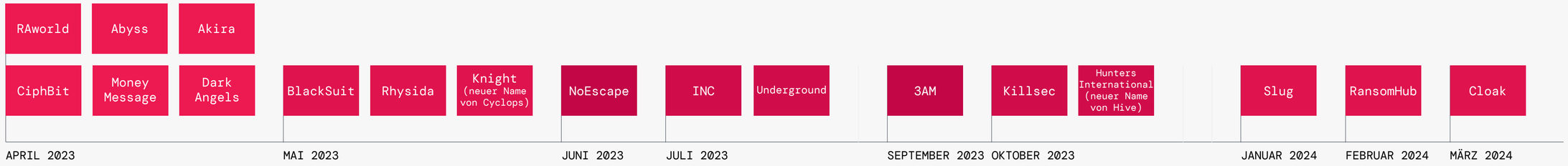


Abb. 9: Neue Ransomware-Gruppen mit Dataleak-Websites.

Ransomware-Angriffe unter Ausnutzung kritischer Sicherheitslücken

Schwachstellen in Software, Systemen und der gesamten digitalen Infrastruktur können als Ausgangspunkt für Ransomware-Angriffe genutzt werden. Organisationen müssen sich dieser Schwachstellen bewusst sein und proaktive Maßnahmen ergreifen, um sie zu beheben.

Die Cybersecurity & Infrastructure Security Agency (CISA) führt eine umfassende Liste von Schwachstellen,[5] einschließlich derer, die aktiv von Ransomware-Gruppen ausgenutzt werden. Es wird dringend empfohlen, dass Organisationen diese Liste genau im Auge behalten und die Behebung der darin genannten Schwachstellen priorisieren. Ein proaktives Schwachstellenmanagement ist unerlässlich, um die allgemeine Cybersicherheit einer Organisation zu stärken.

In vielen Fällen betreffen die von Ransomware-Gruppen ausgenutzten Schwachstellen mit dem Internet verbundene Ressourcen in der externen Angriffsfläche von Organisationen, wie z. B. Gateways, VPNs und andere Technologien für die Remote-Konnektivität. Da sie mit dem Internet verbunden sind, sind diese Schwachstellen für Bedrohungsakteure wesentlich einfacher zu scannen und auszunutzen. In den neuesten Leitlinien des CISA[6] werden Schwachstellen in VPNs und Remote-Konnektivitätslösungen als kritische Problembereiche hervorgehoben und die Einführung der aktuellsten Ansätze wie Zero Trust, SSE und SASE empfohlen, die auf granularen Zugriffskontrollrichtlinien basieren.

Im vergangenen Jahr haben bekannte Ransomware-Familien die in Abbildung 10 dargestellten Schwachstellen gezielt ausgenutzt und dadurch eine Vielzahl von Systemen erheblich beeinträchtigt.

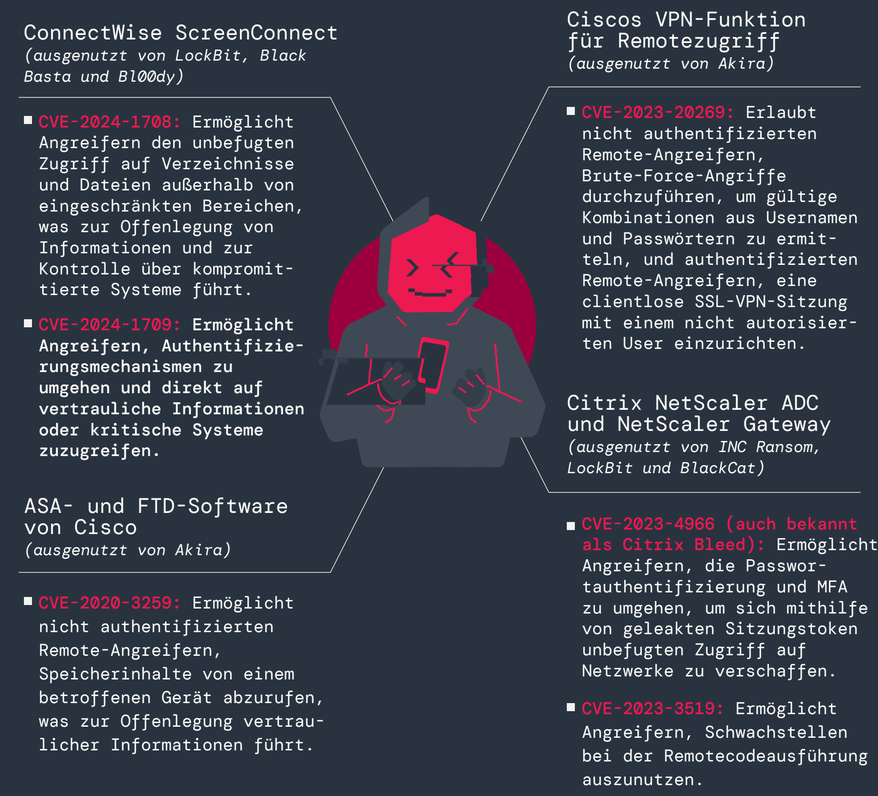


Abb. 10: Verbreitete Schwachstellen von April 2023 bis April 2024

Verfügbare Patches für diese Schwachstellen sollten so schnell wie möglich angewendet werden, ebenso wie die folgenden Maßnahmen zur Schadensbegrenzung:

- Deaktivieren des Remotezugriffs auf Server
- Verwenden sicherer Passwörter und Multifaktorauthentifizierung
- Überwachen von Servern auf verdächtige Aktivitäten

[5] Cybersecurity & Infrastructure Security Agency, **Known Exploited Vulnerabilities Catalog**, aufgerufen am 25. Juni 2024.
[6] Cybersecurity & Infrastructure Security Agency, **Modern Approaches to Network Access Security**, 18. Juni 2024.

Überblick über Ransomware: Welche Vorfälle machen Schlagzeilen?

Ransomware ist allgegenwärtig und erstreckt sich über alle Branchen — und wenn eine Gruppe außer Gefecht gesetzt wird, kommt eine andere wieder zum Vorschein oder es bildet sich eine neue. Hier sind einige aktuelle Berichte, die die sich ständig weiterentwickelnde Ransomware-Landschaft näher beleuchten.

Ransomware im Gesundheitswesen

Das Gesundheitswesen stand in den Jahren 2023 und 2024 vor großen Herausforderungen, da es stark von Ransomware-Gruppen ins Visier genommen wurde. Die Auswirkungen von Betriebsunterbrechungen im Gesundheitswesen sind gravierend: Krankenwagen müssen umgeleitet werden, die Ausstellung von Rezepten verzögert sich und wichtige medizinische Eingriffe müssen verschoben werden. Darüber hinaus kann der Diebstahl sensibler Gesundheitsdaten weitreichende Folgen haben, einschließlich Identitätsdiebstahl und Versicherungsbetrug, was die Schwachstellen im Gesundheitssystem weiter verschärft.

UNVORHERGESEHENE FOLGEN VON LÖSEGELDZAHLUNGEN

Ein Anbieter von Zahlungssystemen im Gesundheitswesen wurde Opfer eines Ransomware-Angriffs, der von der Gruppe BlackCat ausgeführt wurde. Obwohl das Unternehmen den Forderungen der Angreifer nachkam und ein Lösegeld in Höhe von 22 Millionen US-Dollar zahlte, nahm die Angelegenheit eine unerwartete Wendung. BlackCat brach sein Versprechen, einen Teil des Lösegelds mit dem Partner zu teilen, der hinter dem Angriff stand (ein sogenannter „Exit-Scam"), was diesen Partner dazu veranlasste, dem Gesundheitsdienstleister mit der Veröffentlichung sensibler Daten zu drohen.

Diese Geschichte verdeutlicht, dass das alte Sprichwort „Keine Ehre unter Dieben" auch für Cyberkriminelle gilt. Selbst wenn Sie das Lösegeld zahlen, gibt es keine Garantie dafür, dass die Ransomware-Gruppe die gestohlenen Daten nicht trotzdem veröffentlicht oder löscht. Darüber hinaus enthalten einige Ransomware-Entschlüsselungstools Fehler, die eine erfolgreiche Datenwiederherstellung unmöglich machen. Zudem kann die Wiederherstellung von Daten aus einem Backup in manchen Fällen sogar schneller sein.

DOPPELTE ERPRESSUNG, DOPPELTE AUSBEUTUNG

Im Februar 2023 bestätigte ein bekanntes US-amerikanisches Pharmaunternehmen, dass seine IT-Systeme gehackt worden waren. Der Vorfall betraf eine der Tochtergesellschaften des Unternehmens, wobei die gestohlenen Dateien später von der Ransomware-Gruppe Lorenz geleakt wurden.[7] Im Februar 2024 wurde dasselbe Unternehmen dann Opfer eines weiteren Ransomware-Angriffs.[8] Dies scheint Teil eines zunehmenden Trends zu sein, den ThreatLabz beobachtet hat: Innerhalb eines Jahres wird ein Unternehmen mehrmals von Ransomware-Angreifern ins Visier genommen.

[7] BleepingComputer, **Drug distributor AmerisourceBergen confirms security breach**, 8. Februar 2023.
[8] BleepingComputer, **Pharmaceutical giant Cencora says data was stolen in a cyberattack**, 27. Februar 2024.

Die Auswirkungen der SEC-Richtlinien zur Cybersicherheit

Im Jahr 2023 führte die SEC neue Vorschriften zur Offenlegung von sicherheitsrelevanten Vorfällen ein, um die Transparenz und Rechenschaftspflicht börsennotierter Unternehmen zu gewährleisten. Seit dem 15. Dezember 2023 verpflichten diese Regeln zur rechtzeitigen Meldung wesentlicher Cybersicherheitsvorfälle und verlangen detaillierte Informationen über Risikomanagement, Strategie und Governance eines Unternehmens im Bereich Cybersicherheit. Zu den wichtigsten Bestandteilen der neuen SEC-Vorschriften gehört die Aufnahme von Punkt 1.05 in Formular 8-K, der die Meldung wesentlicher Cybersicherheitsvorfälle innerhalb von vier Werktagen nach Feststellung der Relevanz durch das Unternehmen vorschreibt. Darüber hinaus ist im Formular 10-K nun eine jährliche Berichterstattung über das Risikomanagement und die Strategie im Bereich Cybersicherheit erforderlich, beginnend mit den Geschäftsjahren, die am oder nach dem 15. Dezember 2023 enden. Ausländische private Emittenten müssen außerdem einer vergleichbaren Offenlegungspflicht in den Formularen 6-K und 20-K nachkommen.

Diese Regelungen stellen Ransomware-Angreifer, die börsennotierten Unternehmen diskrete Zahlungsmöglichkeiten anbieten, vor eine neue Herausforderung, da die Unternehmen nun verpflichtet sind, den Angriff dennoch vollständig offenzulegen. Positiv zu vermerken ist, dass die neue Verordnung Angriffe ohne Verschlüsselung erschwert, ein neuer Trend, bei dem Ransomware-Angreifer ausschließlich mit der Drohung, gestohlene Daten zu veröffentlichen, Lösegeld fordern.

AUSWIRKUNGEN DER NEUEN REGELN AUF UNTERNEHMEN

Die Cybersicherheitsregelungen der SEC können Unternehmen in Bezug auf Compliance und Risikomanagement vor große Herausforderungen stellen. Diese Vorschriften sollen zwar die Transparenz und den Anlegerschutz verbessern, verlangen jedoch von Unternehmen, dass sie sich in komplexen Anforderungen an die Berichterstattung zurechtfinden und wesentliche Vorfälle unverzüglich melden.

Eine der größten Auswirkungen ist der erhöhte Druck auf Unternehmen, Cybervorfälle genau zu quantifizieren und zu bewerten. Die Ermittlung der Relevanz und der potenziellen Auswirkungen von Cybervorfällen erfordert eine sorgfältige Analyse, die kostspielig sein kann und Unternehmen (große und kleine) dazu zwingen kann, ihre Protokolle zur Reaktion auf Vorfälle zu überdenken und ihre Angaben zu aktualisieren, um die Anforderungen der SEC zu erfüllen.

Darüber hinaus variieren die Fristen je nach Größe und Meldestatus der Unternehmen, was die Komplexität noch erhöht. Kleinere berichtspflichtige Unternehmen haben oft andere und in der Regel längere Fristen für die Einhaltung der Vorschriften als größere Unternehmen. Zwar müssen größere Unternehmen kürzere Fristen einhalten, doch verfügen sie aufgrund ihrer Größe auch über mehr Ressourcen, um die Relevanz eines Cybersicherheitsvorfalls zu analysieren.

Die neuen Offenlegungspflichten machen es börsennotierten Unternehmen auch unmöglich, stillschweigend Lösegeld zu zahlen, ohne ihren Ruf zu schädigen und die Konsequenzen zu tragen, die sich aus der Offenlegung von Informationen über einen Sicherheitsverstoß ergeben.

EINIGE UNTERNEHMEN VERSTOSSEN BEREITS GEGEN DIE REGELN DER SEC

Trotz der klaren Richtlinien der SEC haben einige Unternehmen die neuen Cybersicherheitsvorschriften bereits nicht eingehalten. Jüngste Meldungen bekannter Unternehmen haben Bedenken hinsichtlich der Nichteinhaltung und der Angemessenheit ihrer Berichterstattung über Vorfälle aufgeworfen.[9] In vielen dieser Meldungen fehlen quantitative Daten und detaillierte Bewertungen der finanziellen und betrieblichen Auswirkungen der Cybervorfälle, was genau das ist, was die SEC jetzt vorschreibt. Dadurch, dass Unternehmen trotz der SEC-Regelungen nur unzureichende Angaben zu Cybervorfällen machen, sind möglicherweise verbesserte Leitlinien und behördliche Aufsicht erforderlich, um eine konsistente und wirksame Einhaltung sicherzustellen.

Die Regelungen der SEC zur Cybersicherheit stellen eine bedeutende regulatorische Veränderung dar, die darauf abzielt, die Transparenz und Rechenschaftspflicht bei der Meldung von Vorfällen zu verbessern. Die konsequente und redliche Einhaltung dieser neuen Regeln erfordert eine kontinuierliche Zusammenarbeit zwischen Aufsichtsbehörden, Unternehmen und Interessenvertretern der Branche.

[9] Forbes, **Companies Are Already Not Complying With The New SEC Cybersecurity Incident Disclosure Rules**, 4. März 2024.

Auswirkungen von Strafverfolgungsmaßnahmen

Qakbot durch „Operation Duck Hunt“ lahmgelegt

Am 29. August 2023 kündigten das Federal Bureau of Investigation (FBI) und das Department of Justice (DOJ) in einer koordinierten länderübergreifenden Aktion die Operation Duck Hunt an. Zscaler ThreatLabz stellte den Strafverfolgungsbehörden für diese Operation umfangreiche technische Unterstützung zur Verfügung.[10]
Die mehrstufige Infrastruktur von Quakbot sollte verhindern, dass diese Bedrohung ausgeschaltet werden kann, wie in Abbildung 11 dargestellt.

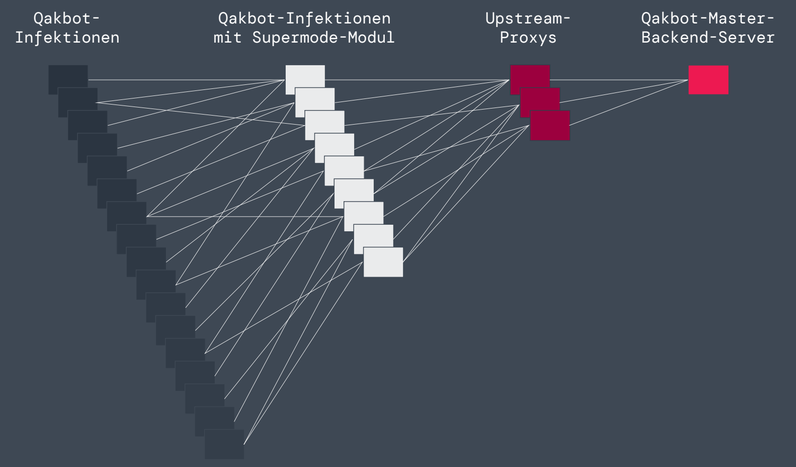


Abb. 11: Die mehrschichtige Infrastruktur von Quakbot

Diese Infrastruktur bestand aus mehreren resilienten Sicherheitsebenen, wobei jede Ebene nur durch koordinierte Maßnahmen ausgeschaltet werden konnte. Die erste Ebene der Qakbot-Infrastruktur umfasste infizierte Systeme, auf denen ein Supernode-Plugin ausgeführt wurde, das den Traffic an mehrere Proxys weiterleitete, die den Master-Qakbot-Backend-Server verbergen sollten.

Operation Duck Hunt leitete die Upstream-Proxyserver des Supernodes auf eine Reihe von Sinkhole-Servern um, um die Qakbot-Infrastruktur sofort zu übernehmen, wie in Abbildung 12 dargestellt.

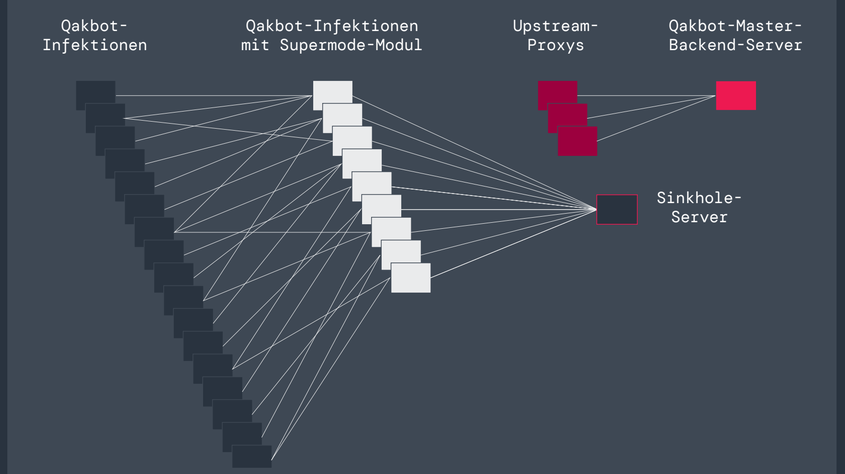


Abb. 12: Qakbot-Architektur nach Umleitung der Upstream-Proxys jedes Supernodes

Nachdem das FBI die Supernodes übernommen hatte, wiesen die Sinkhole-Server die infizierten Computer an, Shellcode herunterzuladen, der wiederum eine DLL lud, die die Malware neutralisierte. Dadurch wurden die betroffenen Computer erfolgreich von der Malware befreit und weitere Angriffe verhindert.

Zum Zeitpunkt der Abschaltung hatte Qakbot weltweit mehr als 700.000 Computer infiziert, davon allein mehr als 200.000 in den Vereinigten Staaten.[11] Vor dieser Operation **war Qakbot fast 15 Jahre lang aktiv** und ursprünglich darauf ausgelegt, Kreditkarten- und Überweisungsbetrug zu erleichtern. Im Jahr 2019 verlagerte sich die Gruppe auf die Rolle eines Initial Access Brokers für Ransomware-Gruppen wie Conti, ProLock, Egregor, REvil, MegaCortex und Black Basta.

Die Qakbot-Malware wurde normalerweise über Spam-E-Mails mit schädlichen Anhängen oder Links verbreitet. Nach der Infektion wurde Cobalt Strike häufig zur lateralen Ausbreitung und schließlich zur Bereitstellung von Ransomware eingesetzt.

Leider gab es keine Verhaftungen oder Anklagen gegen einen der Bedrohungsakteure, und **Qakbot tauchte im Dezember 2023 wieder auf**. Die Gruppe aktualisierte die Malware, um 64-Bit-Versionen von Windows zu unterstützen, änderte das interne Konfigurationsformat und modifizierte die Netzwerkkommunikation, um AES-Verschlüsselung verwenden zu können. Wie wir später in diesem Report noch näher erörtern werden, hat der Qakbot-Bedrohungsakteur seine TTPs seit der Operation Duck Hunt erheblich verändert.

[10] US Department of Justice, **Qakbot Malware Disrupted in International Cyber Takedown**, 29. August 2023.
[11] TechCrunch, **How the FBI took down the notorious Qakbot botnet**, 1. September 2023.

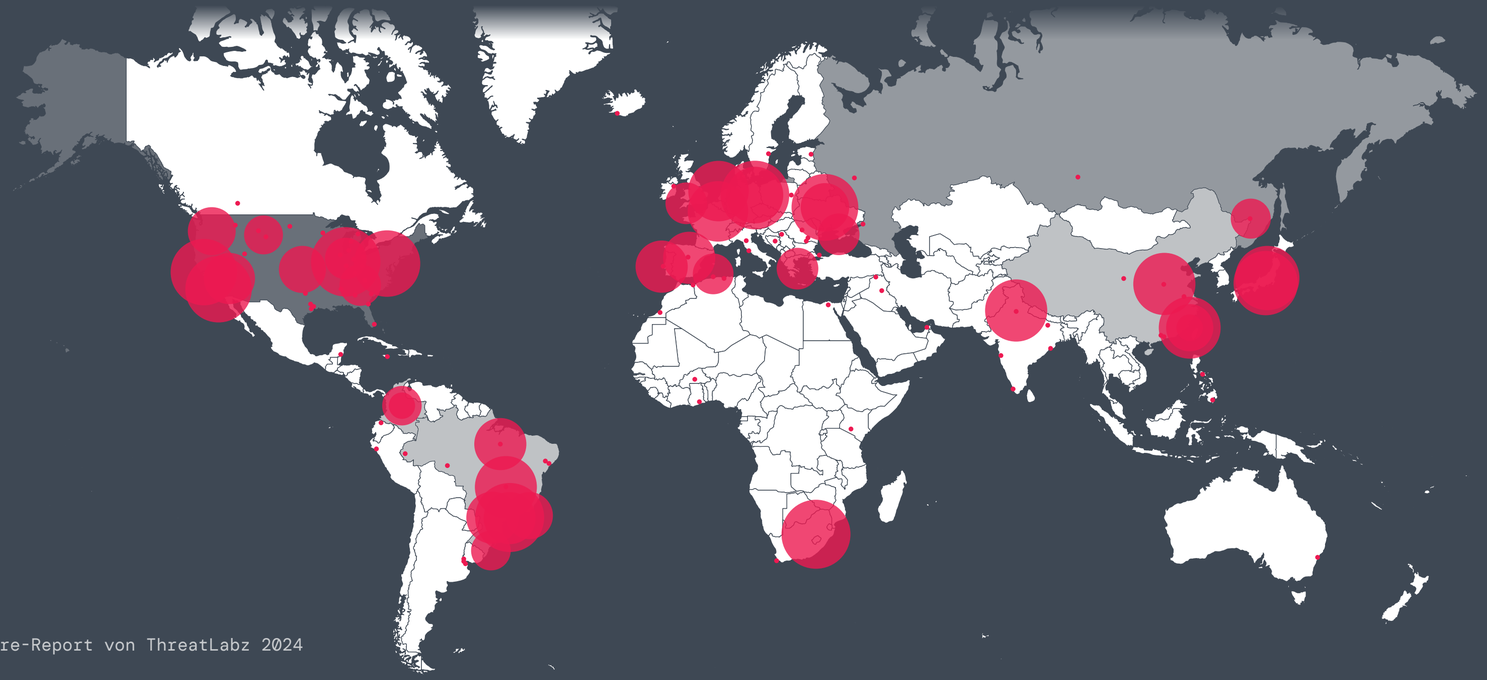
„Operation Endgame“ zielte gleichzeitig auf mehrere Initial Access Broker ab

Am 28. Mai 2024 kündigte Europol in Zusammenarbeit mit zahlreichen internationalen Strafverfolgungsbehörden die Operation Endgame an, die sich gleichzeitig gegen mehrere Initial Access Broker richtete. Dies führte zu mehr als einem Dutzend weltweiter Durchsuchungen, mehreren Verhaftungen und der Abschaltung von mehr als 100 Servern, die für kriminelle Aktivitäten genutzt wurden. Diese Server waren für den Betrieb verschiedener Malware-Downloader (auch „Loader“ genannt) unerlässlich und wurden verwendet, um die Computer der Opfer zu infiltrieren und Schadsoftware, einschließlich Ransomware, zu verbreiten.

Die Malware-Familien, die im Rahmen dieser Operation ins Visier genommen wurden, waren für die Infektion von Millionen von Computern auf der ganzen Welt verantwortlich, darunter auch solche in Gesundheitseinrichtungen und kritischen Infrastrukturservices. Im Rahmen der Operation wurden Maßnahmen gegen SmokeLoader, Pikabot, Bumblebee und IcedID ergriffen.

Zscaler ThreatLabz leistete entscheidende technische Unterstützung beim SmokeLoader-Sinkhole der Bedrohungsbehebung im Rahmen der Operation Endgame.

SmokeLoader ist seit 2011 aktiv und wurde von mehreren Initial Access Brokern für Ransomware verwendet, darunter Raspberry Robin und die Ransomeware-Gruppe Stop (auch bekannt als DJVU). Im Rahmen der Operation Endgame wurden mehr als 1.000 SmokeLoader-Domains beschlagnahmt, die von diesen Bedrohungsgruppen genutzt wurden. Die Domains wurden dann auf einen von den Strafverfolgungsbehörden kontrollierten Sinkhole-Server umgeleitet. Die Karte in Abbildung 13 zeigt infizierte Systeme, die mit dem SmokeLoader-Sinkhole kommunizierten.



Diese Karte zeigt die weitreichenden Auswirkungen, die SmokeLoader weltweit hatte, einschließlich schwerwiegender Infektionen in Lateinamerika, Asien, Nordamerika und Europa.

Abb. 13: Karte der SmokeLoader-Infektionen, die mit dem Operation-Endgame-Sinkhole kommunizieren (Quelle: Zscaler ThreatLabZ)

Wenn mit SmokeLoader infizierte Systeme eine Verbindung zum Sinkhole-Server herstellten, erhielten sie den in die Malware eingebetteten Deinstallationsbefehl. Bis heute wurden mehr als 40.000 mit SmokeLoader infizierte Systeme von der Malware befreit, wie in Abbildung 14 dargestellt.

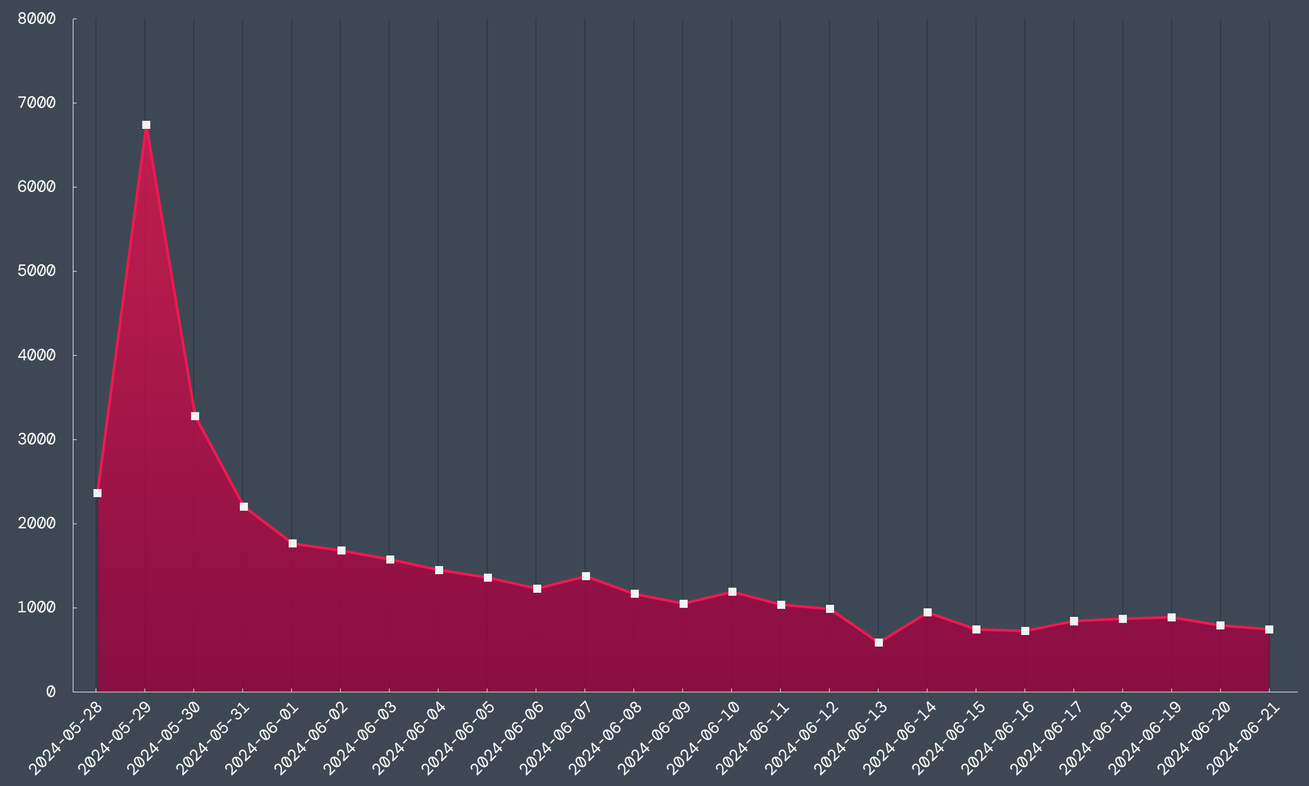


Abb. 14: Im Rahmen der Operation Endgame von Malware befreite SmokeLoader-Systeme

Pikabot tauchte erstmals Anfang 2023 auf und war in der zweiten Jahreshälfte besonders aktiv. Dieser Anstieg war darauf zurückzuführen, dass die Malware zum bevorzugten Initial Access Broker für die Ransomware Black Basta wurde, nachdem Qakbot durch die Operation Duck Hunt ausgeschaltet worden war. Im Februar 2024 **tauchte Pikabot mit erheblichen Änderungen** in seiner Codebasis und -struktur wieder auf. Pikabot wurde von ThreatLabz regelmäßig beim Einsatz von **Cobalt Strike** und **Meterpreter** von Metasploit beobachtet.

Bumblebee wurde im März 2022 entdeckt und hatte Verbindungen zur ehemaligen Ransomware-Gruppe Conti. Die Malware war der Nachfolger des BazarLoader-Malware-Tools der Gruppe, das sie für den Erstzugriff bei Conti- und Diavol-Ransomware-Angriffen verwendeten. ThreatLabz hat häufig beobachtet, dass sowohl BazarLoader als auch Bumblebee Cobalt-Strike-Payloads für die laterale Bewegung einsetzen. Bumblebee wird auch mit Akira- und Black-Basta-Ransomware-Angriffen in Verbindung gebracht.

Ähnlich wie Qakbot wurde IcedID ursprünglich als Banking-Trojaner entworfen, als er 2017 in Umlauf kam. Später verlagerte die Gruppe ihren Schwerpunkt jedoch darauf, als Initial Access Broker für Ransomware zu fungieren. Im Laufe der Jahre wurde der Malware-Code für IcedID für verschiedene Zwecke geforkt und modifiziert. Darüber hinaus haben dieselben Entwickler einen neuen Malware-Loader namens Latrodectus erstellt, der im November 2023 veröffentlicht und wahrscheinlich auch zur Bereitstellung von Ransomware verwendet wurde.

Nach der Operation Endgame gab es bei den meisten dieser Initial Access Broker nur minimale Aktivitäten, **mit Ausnahme von Latrodectus**, der in weniger als einem Monat wieder auftauchte. Diese Pause wird jedoch wahrscheinlich nur von kurzer Dauer sein, da sich die Bedrohungsakteure neu formieren.

Hive-Ransomware als Hunters International wieder aufgetaucht

Im Januar 2023 wurde die Infrastruktur der Hive-Ransomware-Gruppe stillgelegt. Nach einer siebenmonatigen verdeckten Operation gelang es dem FBI, die Server von Hive zu infiltrieren und mehr als 300 Entschlüsselungsschlüssel wiederherzustellen, wodurch Lösegeldzahlungen in Höhe von etwa 130 Millionen US-Dollar verhindert wurden. Das Hive-Kollektiv, das seit Juni 2021 aktiv ist, griff mehr als 1.500 Organisationen weltweit an und erpresste Lösegeld in Höhe von über 100 Millionen US-Dollar.[12] Zu den Opfern gehörten Krankenhäuser, Schulbezirke, Finanzinstitute und verschiedene andere Einrichtungen. Es wurden jedoch keine Verhaftungen im Zusammenhang mit Hive vorgenommen, und die Gruppe trat im Oktober 2023 unter dem neuen Namen Hunters International wieder auf. Cyberkriminelle wechseln nach einer größeren Störung oft ihren Namen.

Die Gruppe nahm eine auffällige Änderung an ihrer Vorgehensweise vor: Sie bietet keine Rabatte mehr an und verhandelt nicht mehr mit Opfern über die Höhe der Lösegeldforderung, wie in Abbildung 15 dargestellt.

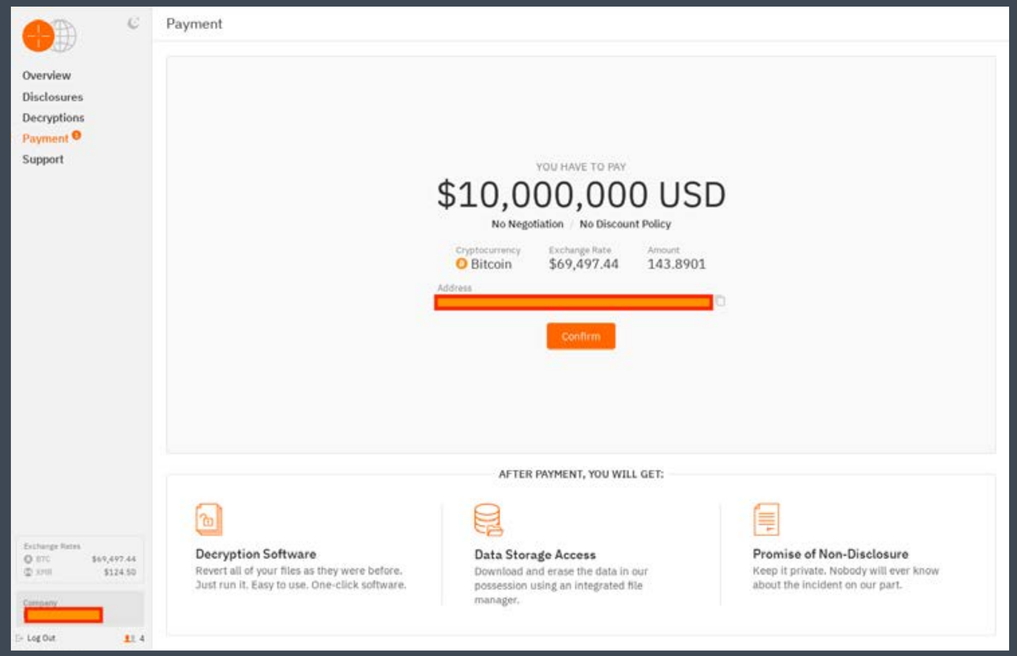


Abb. 15: Opferportal von Hunters International ohne Rabatte oder Verhandlungsmöglichkeiten

Eine solch starre Preispolitik ist bei Ransomware-Gruppen **sehr ungewöhnlich**, da diese häufig erhebliche Rabatte auf die ursprüngliche Lösegeldforderung anbieten. Diese Entscheidung des Hunters-Teams wird wahrscheinlich zu einem geringeren Zahlungsvolumen, aber höheren Zahlungsbeträgen führen.

Hunters International startet weiterhin neue Angriffe und dürfte ohne Festnahmen und strafrechtliche Verfolgung eine ernstzunehmende Bedrohung bleiben.

[12] US Department of Justice, **U.S. Department of Justice Disrupts Hive Ransomware Variant**, 26. Januar 2023.

Die 5 gefährlichsten Ransomware-Gruppen 2024-2025

Da Ransomware und andere Cyberbedrohungen immer komplexer und raffinierter werden, ist es für die Gewährleistung eines hohen Sicherheitsstatus von entscheidender Bedeutung, über die verbreitetsten und gefährlichsten Ransomware-Familien auf dem Laufenden zu bleiben. In diesem Abschnitt werden fünf Ransomware-Familien vorgestellt, die einige der größten Risiken für Unternehmen darstellen, und es werden Einblicke in ihre Taktiken, potenziellen Auswirkungen und jüngsten Aktivitäten gegeben.

1. Dark Angels

Die Ransomware-Gruppe Dark Angels, die die Dataleak-Website Dunghill betreibt, tauchte etwa im Mai 2022 auf. Die Gruppe hat einige der größten Ransomware-Angriffe durchgeführt, hat es aber dennoch geschafft, nur sehr wenig Aufmerksamkeit auf sich zu ziehen. Anfang 2024 stieß ThreatLabz auf ein Opfer, das Dark Angels 75 Millionen US-Dollar gezahlt hatte — mehr als jede andere bisher bekannte Lösegeldzahlung. Diese Summe dürfte das Interesse anderer Angreifer wecken, die diesen Erfolg mit den entsprechenden Taktiken (die wir weiter unten beschreiben) wiederholen möchten. Dark Angels hat es auf verschiedene Branchen abgesehen, darunter das Gesundheitswesen, Regierungsbehörden, den Finanzsektor und das Bildungswesen. In jüngster Zeit wurden Angriffe auf große Industrie-, Technologie- und Telekommunikationsunternehmen beobachtet.

Die Dark-Angels-Gruppe verfolgt einen sehr gezielten Ansatz und greift in der Regel jeweils nur ein einziges großes Unternehmen an. Diese Vorgehensweise steht in krassem Gegensatz zu den meisten Ransomware-Gruppen, die willkürlich Opfer angreifen und den Großteil der Angriffe an angegliederte Netzwerke von Initial Access Brokern und Penetrationstest-Teams auslagern. Sobald Dark Angels ein Ziel identifiziert und kompromittiert hat, entscheidet die Gruppe selektiv, ob die Dateien des Unternehmens verschlüsselt werden sollen. In den meisten Fällen stiehlt die Dark-Angels-Gruppe eine große Menge an Informationen, in der Regel im Bereich von 1 bis 10 TB. Bei großen Unternehmen hat die Gruppe zwischen 10 und 100 TB an Daten exfiltriert, deren Übertragung Tage bis Wochen dauern kann.

Der bekannteste Angriff von Dark Angels fand im September 2023 statt, als die Gruppe in die Systeme eines internationalen Konglomerats eindrang, das neben anderen Services Lösungen für Gebäudeautomationssysteme anbietet. Dark Angels verlangte ein Lösegeld in Höhe von 51 Millionen US-Dollar, behauptete, über 27 TB Unternehmensdaten gestohlen zu haben, und verschlüsselte die virtuellen VMware-ESXi-Maschinen des Unternehmens. Eine RagnarLocker-Ransomware-Variante wurde verwendet, um die Dateien des Unternehmens während des Angriffs zu verschlüsseln. Die Beziehung zwischen RagnarLocker und Dark Angels ist nicht klar, aber die Gruppe verwendete die Ransomware vor der polizeilichen Aktion gegen RagnarLocker,[13] die im Oktober 2023 zur Verhaftung eines führenden Mitglieds führte. Anzumerken ist, dass die Gruppe Dark Angels, als sie zum ersten Mal in Erscheinung trat, eine Babuk-Variante einsetzte, bevor sie zu RagnarLocker wechselte.

Die Strategie der Ransomware-Gruppe Dark Angels, eine kleine Anzahl hochwertiger Unternehmen ins Visier zu nehmen, um hohe Lösegeldzahlungen zu fordern, ist ein Trend, den es zu beobachten gilt. Zscaler ThreatLabz prognostiziert, dass andere Ransomware-Gruppen den Erfolg von Dark Angels bemerken und möglicherweise ähnliche Taktiken einsetzen werden, d. h. sich auf hochwertige Ziele konzentrieren und den Datendiebstahl verstärken, um ihre finanziellen Gewinne zu maximieren.

[13] Europol, **Ragnar Locker ransomware gang taken down by international police swoop**, 20. Oktober 2023.

2. LockBit

LockBit tauchte erstmals im September 2019 auf und gewann aufgrund des großen Ransomware-Partnernetzwerks der Gruppe schnell an Bedeutung. Für den Erstzugriff auf Unternehmensnetzwerke, die Exfiltration von Daten sowie die Auslieferung der Ransomware arbeitet LockBit mit zahlreichen Affiliates zusammen. Die Infiltration beginnt normalerweise über Spam-E-Mails mit schädlichen Anhängen oder Links. Ebenfalls wurde beobachtet, dass LockBit mit Brute-Force-Angriffen Anmeldedaten für Remotedesktopprotokoll (RDP) oder VPNs beschaffte, gestohlene Anmeldedaten über Initial Access Broker erwarb und öffentlich zugängliche Anwendungen zu ihrer Kompromittierung ausnutzte. Das Netzwerk von LockBit hat es auf kritische Sektoren wie den Fertigungssektor, das Gesundheitswesen und die Logistik abgesehen. Die Gruppe hat weltweit mehr als 2.000 Systeme angegriffen und von den Opfern mehr als 120 Millionen US-Dollar erpresst.

Im vergangenen Jahr stand LockBit in Bezug auf das Angriffsvolumen weiterhin an der Spitze. Die LockBit-Gruppe verfolgt eine deutlich andere Strategie als Dark Angels und ermutigt ihre Partner, so viele Organisationen wie möglich anzugreifen, unabhängig von der potenziellen Lösegeldsumme. Dieses hohe Angriffsaufkommen führt häufig dazu, dass kleine Unternehmen mit relativ geringen Lösegeldforderungen ins Visier genommen werden.

LockBit-Ransomware wird auf Windows- und Linux-basierten Systemen bereitgestellt. Es gibt drei Versionen von LockBit für Windows: LockBit Red (das Original), LockBit Black (basierend auf dem BlackMatter-Quellcode) und LockBit Green (basierend auf dem geleakten Conti-Quellcode). Wie im **Ransomware-Report von ThreatLabz 2023** erwähnt, wurde der LockBit-Black-Builder geleakt und viele Cyberkriminelle, die nicht mit LockBit in Verbindung stehen, haben ihn für ihre eigenen Ransomware-Angriffe verwendet. Interessanterweise ist LockBit Black immer noch die am häufigsten eingesetzte Variante der Gruppe. Die spezifische LockBit-Ransomware-Variante, die zur Verschlüsselung der Dateien eines Opfers verwendet wird, wird nun in der Lösegeldforderung neben der Opfer-ID angezeigt. Dadurch kann der Angreifer, der den Angriff durchführt, leicht die eingesetzte LockBit-Variante identifizieren, um das richtige Entschlüsselungstool bereitzustellen, wenn ein Lösegeld gezahlt wird. Abbildung 16 zeigt ein Beispiel für eine aktuelle Lösegeldforderung von LockBit Black.

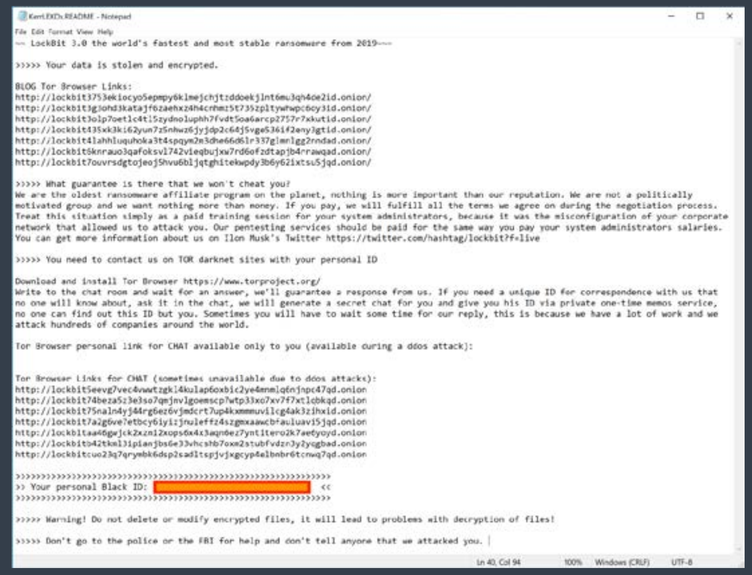


Abb. 16: Beispiel einer aktuellen Lösegeldforderung von LockBit Black

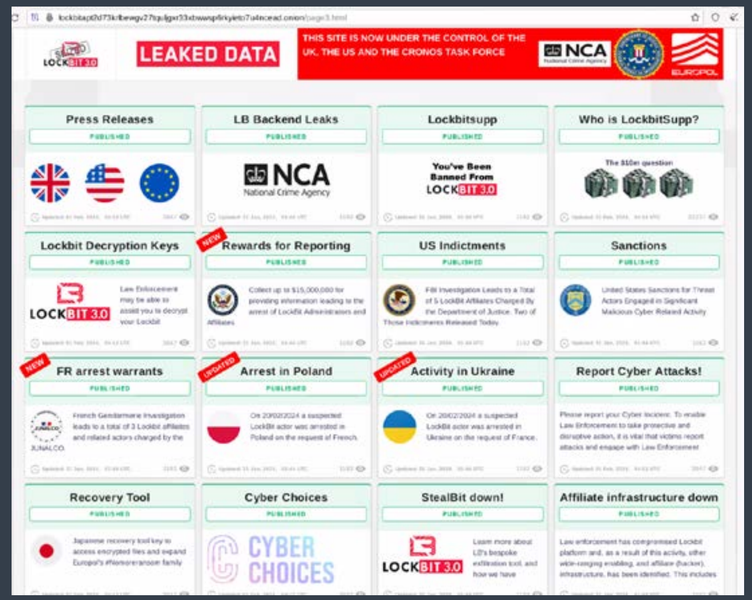


Abb. 17: Beschlagnahmung der Dataleak-Website von LockBit durch Strafverfolgungsbehörden

Am 20. Februar 2024 beschlagnahmten das FBI und die britischen Strafverfolgungsbehörden Teile der Infrastruktur von LockBit, darunter etwa 7.000 Entschlüsselungsschlüssel der Opfer. Nach der Beschlagnahmung konfiszierten die Strafverfolgungsbehörden die LockBit-Dataleak-Website und machten sich über die Cyberkriminellen lustig, indem sie eine ähnliche Version der früheren Website mit verschiedenen Artikeln und Countdown-Timern anzeigten, bis neue Informationen veröffentlicht wurden, wie in Abbildung 17 unten dargestellt.

Leider entdeckte ThreatLabz innerhalb weniger Tage nach der Beschlagnahmung **neue Ransomware-Angriffe**, die von LockBit verübt wurden, sowie eine neue Dataleak-Website. Die Gruppe ist weiterhin aktiv und hat seit der Strafverfolgungsmaßnahme Dutzende neuer Unternehmen angegriffen.

Am 7. Mai 2024 gab das FBI die Anklage gegen den LockBit-Entwickler und -Betreiber Dmitry Yuryevich Khoroshev bekannt. Der LockBit-Betreiber bestritt jedoch umgehend, dass das FBI ihn korrekt identifiziert habe. Ohne weitere Verhaftungen werden LockBit-Angriffe wahrscheinlich in absehbarer Zukunft weitergehen, obwohl ThreatLabz davon ausgeht, dass die Marke LockBit aufgrund der zunehmenden Kontrolle irgendwann eingestellt und unter einem anderen Namen fortgeführt wird.

3. BlackCat

Die im November 2021 erstmals aufgetretene Ransomware BlackCat (auch bekannt als ALPHV) war eine der gefährlichsten Bedrohungen, bis sie im März 2024 abgeschaltet wurde. Ähnlich wie LockBit nutzte BlackCat ein Partnernetzwerk, um Angriffe zu starten, und teilte einen Prozentsatz der Lösegeldzahlungen.

Der wohl berüchtigtste BlackCat-Partner ist eine Gruppe namens Scattered Spider[14] (auch bekannt als Star Fraud). Diese Gruppe besteht aus englischsprachigen Mitgliedern und ist äußerst erfolgreich bei Social-Engineering-Angriffen. Häufig geben sie sich bei Sprachanrufen als IT- oder Helpdesk-Mitarbeiter aus und führen SIM-Austausch-Angriffe durch, um die Multifaktor-Authentifizierung zu umgehen. Am 15. Juni 2024 wurde der mutmaßliche Anführer[15] von Scattered Spider, ein 22-jähriger britischer Staatsbürger, verhaftet. Es ist jedoch noch zu früh, um sagen zu können, welche Auswirkungen diese Verhaftung auf die Handlungsfähigkeit der Gruppe haben wird.

BlackCat war eine der mit den meisten Plattformen kompatiblen Ransomware-Familien, was zum Teil darauf zurückzuführen ist, dass sie die Programmiersprache Rust verwendet. In Abbildung 18 sind die Entschlüsselungstools dargestellt, die für alle Plattformen verfügbar sind, die von der BlackCat-Ransomware unterstützt wurden, kurz bevor die Gruppe ihre Aktivitäten einstellte. Zu den Plattformen gehörten Windows, ESXi, FreeBSD und zahlreiche Varianten von Linux-Betriebssystemen und -Architekturen wie ARM, x86/x64 und PowerPC.

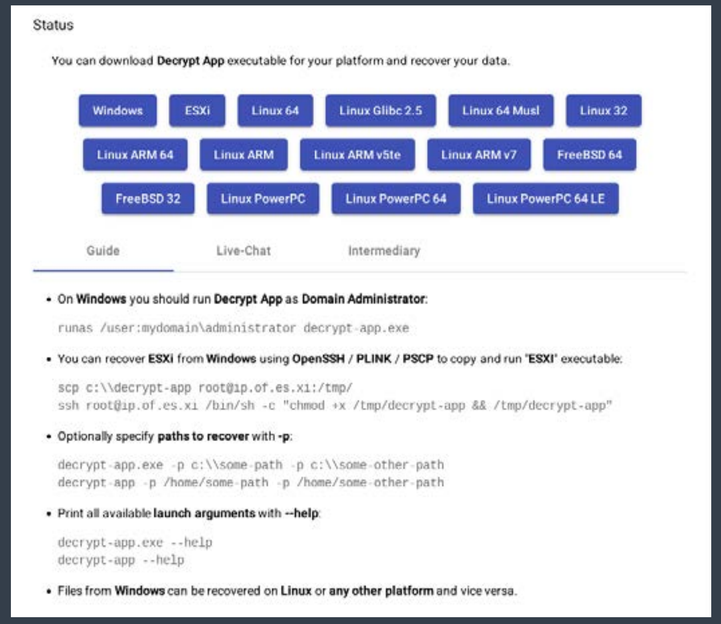


Abb. 18: BlackCat-Entschlüsselungstools wurden für 15 verschiedene Betriebssysteme, Architekturen und Plattformen bereitgestellt

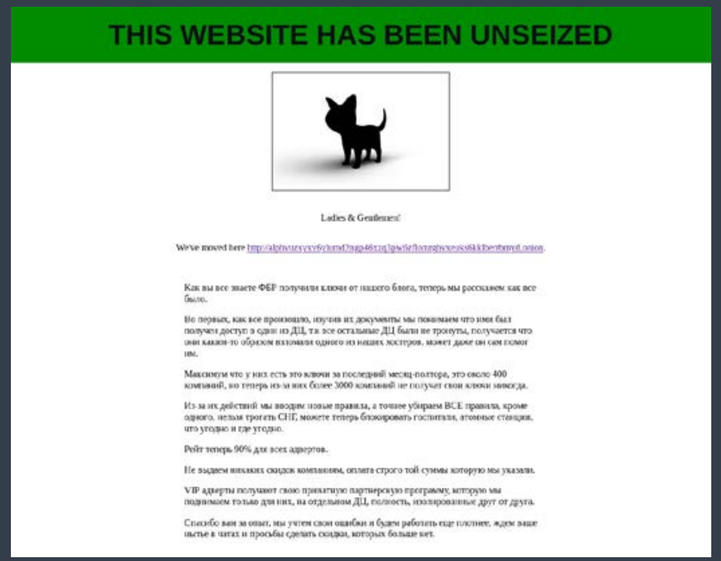


Abb. 19: Die „zurückeroberte" Dataleak-Website von BlackCat nach dem Eingreifen der Strafverfolgungsbehörden

Diese plattformübergreifende Kompilierung ist im Vergleich zu anderen Ransomware-Familien, die in der Regel nur Windows, ESXi und eine kleine Anzahl von Linux-basierten Plattformen unterstützen, ungewöhnlich. Dies deutet darauf hin, dass BlackCat-Partner möglicherweise Unterstützung für zusätzliche Plattformen angefordert haben, um Dateien auf so vielen Systemen wie möglich zu verschlüsseln.

Im Dezember 2023 erhielt das FBI Zugriff auf einen Teil der Infrastruktur von BlackCat. Das FBI versuchte, die Tor-basierten Websites der Gruppe zu beschlagnahmen, einschließlich der Portale für Lösegeldverhandlungen und der Dataleak-Websites. Doch dann kam eine plötzliche Wendung der Ereignisse: BlackCat veröffentlichte eine Nachricht, dass die Gruppe die Dataleak-Website „zurückerobert" habe, und stellte einen Link zu einer neuen Dataleak-Website bereit, die das FBI nicht unter seine Kontrolle bringen konnte, wie in Abbildung 19 unten dargestellt.

Dieses Hin und Her zwischen dem FBI und BlackCat dauerte einige Tage, bis BlackCat davon überzeugt war, dass die neue Dataleak-Website ausreichend beworben worden war. Es ist anzumerken, dass das „Beschlagnahmen" einer Tor-basierten Website nicht so einfach ist wie das einer herkömmlichen DNS-basierten Website, da sie auf kryptografischen Geheimnissen beruht und nicht auf einer zentralen Instanz, die sich an gerichtliche Anordnungen halten muss.

Im März 2024 gab die BlackCat-Gruppe ihre Auflösung bekannt und begründete dies mit der Kompromittierung ihrer Infrastruktur durch das FBI, die sie angeblich daran hinderte, ihre Aktivitäten fortzusetzen. Es kamen jedoch Zweifel an dieser Erklärung auf, da die Auflösung unmittelbar nach dem Erhalt eines Lösegeldes in Höhe von 22 Millionen US-Dollar und der anschließenden Täuschung eines Partners durch einen Exit-Scam, der ihnen bei der Kompromittierung eines Gesundheitsdienstleisters geholfen hatte (siehe weiter oben in diesem Report), erfolgte.

Die BlackCat-Ransomware ist zwar nicht mehr aktiv, aber die Partner, die hinter den Angriffen der Gruppe stehen, sind wahrscheinlich zu anderen Ransomware-as-a-Service-Netzwerken wie RansomHub abgewandert (wo auch die Daten des Gesundheitsdienstleisters, der das Lösegeld in Höhe von 22 Millionen US-Dollar gezahlt hat, inzwischen geleakt wurden). Darüber hinaus ist es unwahrscheinlich, dass die BlackCat-Ransomware-Gruppe selbst ihre Aktivitäten wirklich eingestellt hat. Sie wird wahrscheinlich unter einem neuen Namen wieder auftauchen.

[14] Cybersecurity & Infrastructure Security Agency, **Cybersecurity Advisory: Scattered Spider**, 16. November 2023.
[15] Krebs on Security, **Alleged Boss of 'Scattered Spider' Hacking Group Arrested**, 15. Juni 2024.

4. Akira

Die Ransomware Akira tauchte im April 2023 auf und erlangte schnell einen zweifelhaften Ruhm durch die große Anzahl von Angriffen, die von ihren Partnern durchgeführt wurden. Bei der Bedrohungsgruppe Akira handelt es sich wahrscheinlich um einen weiteren Ableger der nicht mehr existierenden Conti-Gruppe. Tatsächlich wies der Ransomware-Code von Akira ursprünglich viele Ähnlichkeiten mit dem geleakten Conti-Quellcode auf. Die Gruppe hat jedoch kürzlich eine Rust-basierte Ransomware entwickelt, die Hinweise auf Power-Rangers-Charaktere wie Megazord enthält.

Partner von Akira-Ransomware haben verschiedene Mechanismen für den Erstzugriff eingesetzt, unter anderem durch die Ausnutzung von CVE-2023-20269.[16] Die Bedrohungsgruppe, die Bumblebee betreibt und Verbindungen zu Conti-Ransomware hat, ist auch dafür bekannt, dass sie als Initial Access Broker für Akira fungiert. Wie bereits in diesem Report erwähnt, wurde Bumblebee durch die Operation Endgame zerschlagen, was jedoch nur minimale Auswirkungen auf die Aktivitäten von Akira hatte.

Wenn wir die Angriffe von Akira besser verstehen wollen, sollten wir uns genau die Informationen ansehen, die Akira den Opfern zur Verfügung stellt, die ein Lösegeld zahlen. ThreatLabz hat die folgende Chat-Nachricht von Akira abgefangen, die Einzelheiten darüber enthält, wie sie sich ursprünglich über einen Initial Access Broker Zugang zum Netzwerk des Unternehmens verschafft haben, und auch Tipps zur Verhinderung von Ransomware-Angriffen in der Zukunft gibt:

Der Erstzugriff auf Ihr Netzwerk wurde im Dark Web erworben. Dann wurde Kerberoasting durchgeführt und wir haben Passwort-Hashes erhalten. Diese haben wir dann einfach per Brute-Force geknackt und das Passwort des Domain-Administrators bekommen. Nachdem wir uns wochenlang in Ihrem Netzwerk aufgehalten haben, konnten wir einige Fehler entdecken, deren Behebung wir dringend empfehlen:

1. Keiner Ihrer Mitarbeiter sollte verdächtige E-Mails oder Links öffnen oder Dateien herunterladen, geschweige denn auf seinem Computer ausführen.

2. Verwenden Sie sichere Passwörter und ändern Sie diese so oft wie möglich (mindestens 1-2 Mal pro Monat). Verschiedene Ressourcen sollten niemals mit demselben Passwort geschützt werden.

3. Installieren Sie, wenn möglich, eine 2FA.

4. Verwenden Sie die neuesten Versionen von Betriebssystemen, da diese weniger anfällig für Angriffe sind.

5. Aktualisieren Sie alle Softwareversionen.

6. Verwenden Sie Antivirenlösungen und Traffic-Monitoring-Tools.

7. Erstellen Sie einen Jump-Host für Ihr VPN. Verwenden Sie dafür individuelle Anmeldedaten, die sich von denen der ersten Domain unterscheiden.

8. Verwenden Sie eine Backup-Software mit Cloud-Speicher, die einen Token-Schlüssel unterstützt.

9. Schulen Sie Ihre Mitarbeiter so oft wie möglich in Online-Sicherheitsvorkehrungen. Der größte Schwachpunkt ist der Faktor Mensch und die Verantwortungslosigkeit Ihrer Mitarbeiter, Systemadministratoren usw. Wir wünschen Ihnen für die Zukunft Sicherheit, Gelassenheit und viel Erfolg. Vielen Dank für Ihr Mitwirken und Ihre Sorgfalt in Bezug auf Ihre Sicherheit.

Obwohl dieser Rat direkt von Akira kommt, sind die Empfehlungen zutreffend und bieten eine Grundlage für das Verständnis und die Abwehr solcher Angriffe.

Akira ist eine der wenigen großen Ransomware-Gruppen, die nicht direkt von den Strafverfolgungsbehörden bekämpft wurde. Infolgedessen ist Akira nun eine der aktivsten Ransomware-Gruppen, die im nächsten Jahr wahrscheinlich weiterhin neue Angriffe starten wird.

[16] https://nvd.nist.gov/vuln/detail/CVE-2023-20269

5. Black Basta

Die Ransomware Black Basta, die erstmals im April 2022 identifiziert wurde, ist ein weiterer Nachfolger der Conti-Ransomware-Gruppe. Die mit Black Basta in Verbindung stehenden Personen haben verschiedene Methoden angewendet, um Zugang zu Unternehmensnetzwerken zu erhalten. Vor der Operation Duck Hunt (August 2023) war Qakbot einer der wichtigsten Initial Access Broker für Black Basta. Wie bereits erwähnt, übernahm Pikabot nach der Stilllegung diese Funktion. Pikabot wurde jedoch nach der Operation Endgame im Mai 2024 zerschlagen.

ThreatLabz hat seitdem neue Aktivitäten der Bedrohungsgruppe Qakbot verfolgt, die ihre TTPs erheblich verändert hat. Aktuell verwendet die Bedrohungsgruppe keine Spam-E-Mails mehr, um Systeme mit Qakbot zu infizieren, sondern eine Kombination verschiedener Social-Engineering-Techniken. Anstatt Spam-E-Mails an Millionen von Adressen zu senden, führt die Bedrohungsgruppe jetzt gezielte Angriffe durch. Diese Angriffe beginnen damit, dass die Bedrohungsgruppe Spam-E-Mails an eine kleine Anzahl von Zielunternehmen sendet. Die Gruppe ruft dann einen Mitarbeiter dieser Unternehmen an und gibt vor, von der eigenen IT-Abteilung zu sein. Der Anrufer weist das Opfer an, sich über eine Remote-Desktop-Software wie Microsoft Quick Assist in eine Sitzung mit Bildschirmfreigabe einzuloggen, um „die Spam-Filter des Unternehmens für den Mitarbeiter zu aktualisieren“. Sobald der Mitarbeiter dem Bedrohungsakteur Zugriff gewährt, wird ein Windows-Batch-Skript ausgeführt, um das System des Opfers auszukundschaften, Anmeldedaten zu stehlen und eine Backdoor zu installieren. Die Backdoor ändert sich ständig, enthält aber Qakbot, Cobalt Strike und ein SOCKS-Proxy-Tool. Das Batch-Skript enthält eine Befehlszeilenschnittstelle, die der in Abbildung 20 dargestellten ähnelt.

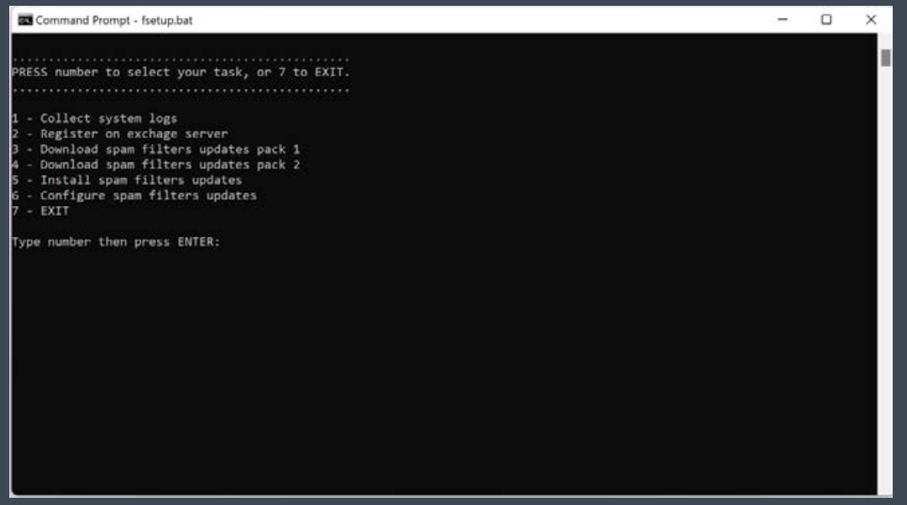


Abb. 20: Bösartige Windows-Batch-Skript-Schnittstelle, die verwendet wird, um eine Backdoor auf dem System eines Opfers als Vorstufe für einen Black-Basta-Ransomware-Angriff einzurichten

Abb. 21: Black-Basta-Ransomware-Angriffskette mit Erstzugriff, vermittelt durch die Qakbot-Bedrohungsgruppe

Sobald diese Backdoor eingerichtet ist, übergibt die Qakbot-Bedrohungsgruppe den Zugang an ein Penetrationstest-Team, das für die laterale Ausbreitung und die letztendliche Bereitstellung der Black-Basta-Ransomware verantwortlich ist.

Auch wenn die Operation Duck Hunt kurzfristig erhebliche Auswirkungen hatte, ist die Bedrohungsgruppe weiterhin aktiv und experimentiert mit neuen Techniken, um Organisationen zu kompromittieren. Im nächsten Jahr wird die Bedrohungsgruppe Qakbot wahrscheinlich weiterhin ein wichtiger Initial Access Broker für Ransomware-Gruppen wie Black Basta bleiben.

Ransomware-Archiv von ThreatLabz

Zscaler ThreatLabz führt ein **öffentliches GitHub-Repository**, das zum Zeitpunkt der Veröffentlichung dieses Artikels 391 Ransomware-Familien und insgesamt 945 Lösegeldforderungen dokumentiert und zwischen April 2023 und April 2024 um 19 Familien und 55 Lösegeldforderungen erweitert wurde. Dieses Archiv kann für die langfristige Beobachtung von Ransomware-Gruppen, einschließlich ihrer Dataleak-Websites und Verhandlungstaktiken, sowie für die Zuordnung von Ransomware-Gruppen, die sich umbenennen, durch stilometrische Analyse nützlich sein.

In Abbildung 22 ist ein stilometrischer Vergleich zwischen einem Chat mit Conti zwecks Lösegeldverhandlungen (oben) und einem entsprechenden Chat mit Black Basta (unten) dargestellt. Hieraus geht hervor, dass es sich bei den Mitgliedern von Black Basta mit ziemlicher Sicherheit um ehemalige Mitglieder von Conti handelt, wie die Ähnlichkeiten in ihrer Satzstruktur, Wortwahl und sogar in bestimmten Anweisungen zeigen.

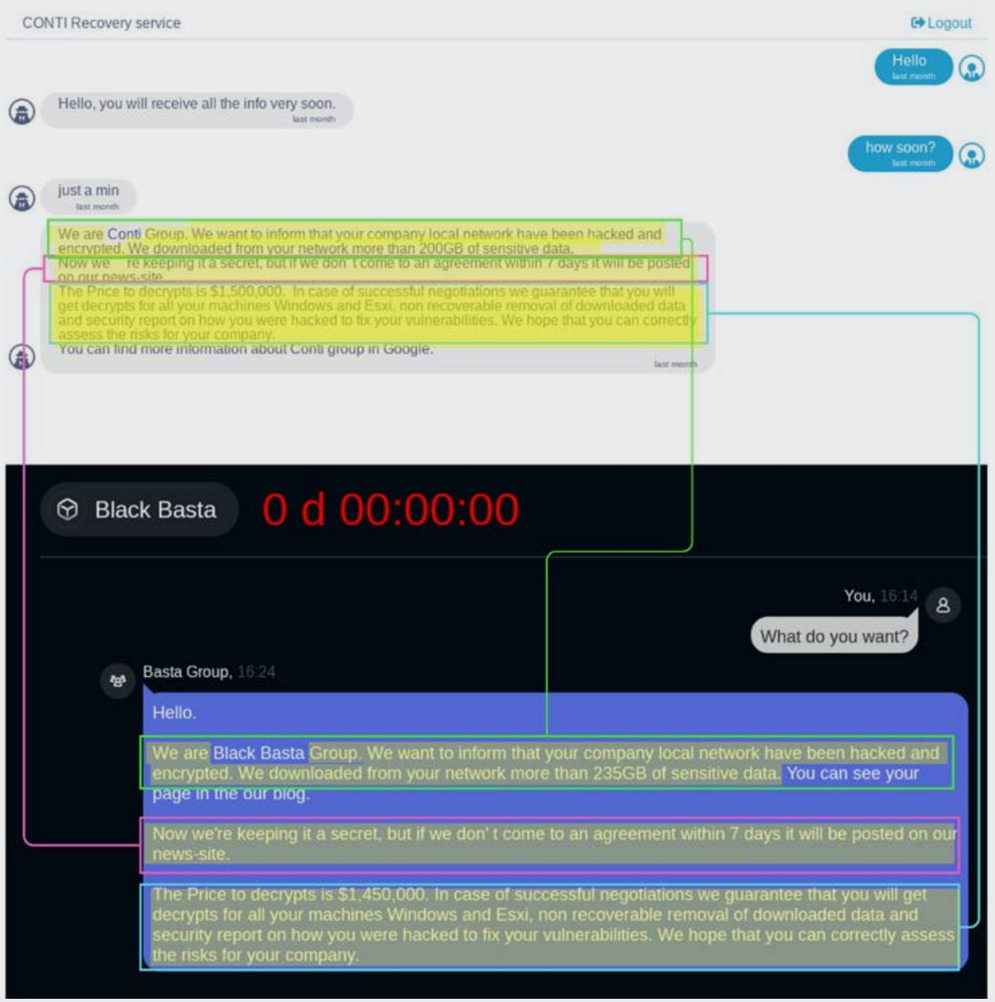


Abb. 22: Stilometrischer Vergleich zwischen einem Chat mit Conti zwecks Lösegeldverhandlungen (oben) und einem entsprechenden Chat mit Black Basta

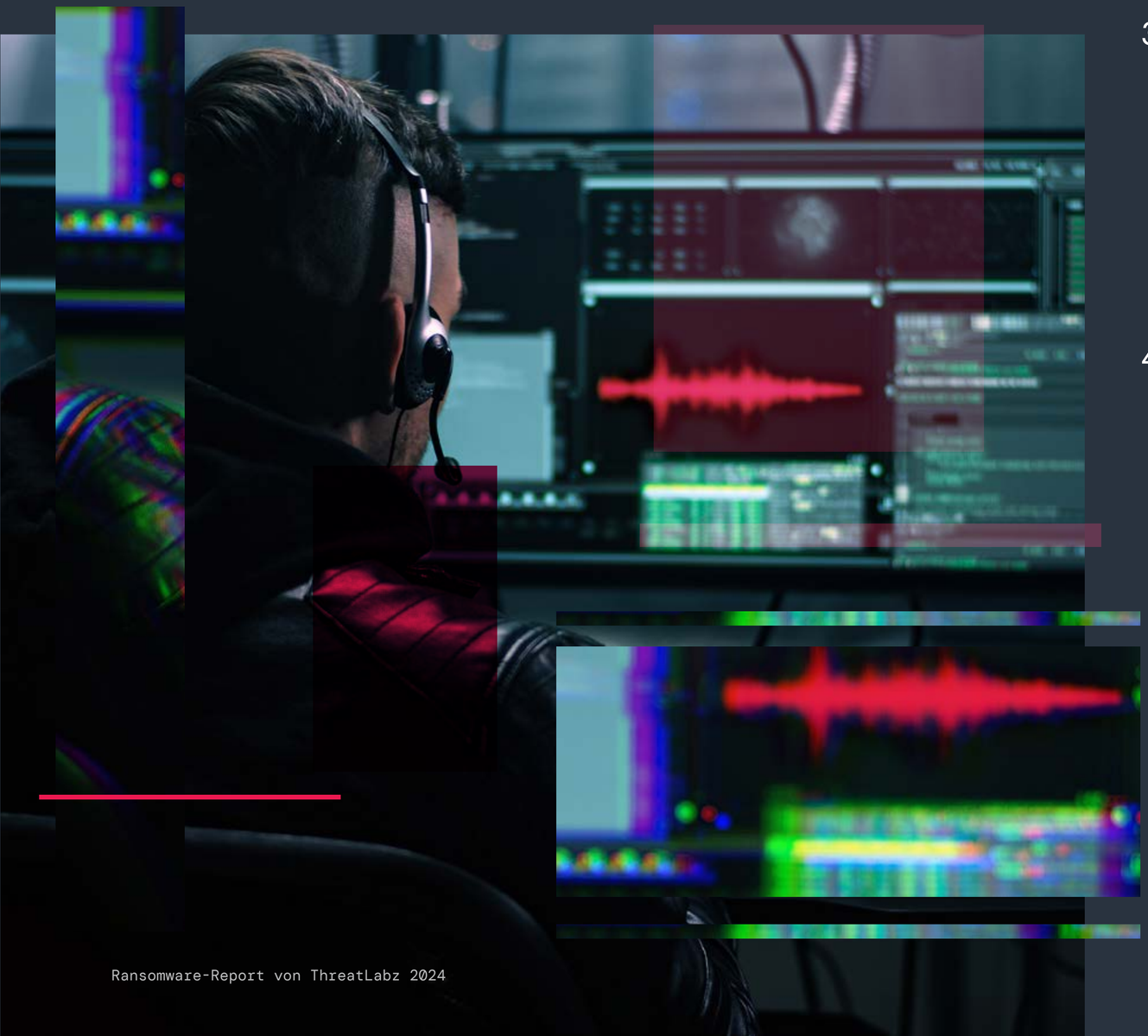
Prognosen für 2025

1. Ransomware-Angreifer werden sehr gezielte Angriffsstrategien anwenden.

Im letzten Jahr war Dark Angels eine der erfolgreichsten und am wenigsten bekannten Ransomware-Gruppen mit einer klar definierten Strategie, eine kleine Anzahl von milliardenschweren Unternehmen ins Visier zu nehmen und sie zu hohen Lösegeldzahlungen zu nötigen. Diese Strategie verfolgt gleich zwei Ziele: die Kontrolle durch die Strafverfolgungsbehörden und die Sicherheitsbranche zu verringern und gleichzeitig mehr Ressourcen für die Infiltration großer Unternehmen einzusetzen, die bereit sind, hohe Lösegeldzahlungen zu leisten, um riesige Mengen gestohlener Daten zu schützen. Dies hat dazu geführt, dass die Gruppe die größte bekannte Lösegeldzahlung in Höhe von 75 Millionen US-Dollar erhalten hat, was im Jahr 2025 das Interesse anderer Ransomware-Bedrohungsakteure wecken dürfte, dieses Vorgehen nachzuahmen.

2. Bei gezielten Angriffen wird zunehmend sprachbasiertes Social Engineering zum Einsatz kommen.

Im Jahr 2025 erwarten wir einen Anstieg gezielter Angriffe durch spezialisierte Initial Access Broker. Diese Broker, wie beispielsweise Qakbot und Scattered Spider, setzen ausgeklügelte Techniken ein, um sich Zugriff zu verschaffen, insbesondere sprachbasierte Social-Engineering-Angriffe („Vishing“), um Personen dazu zu bewegen, Zugriff auf eine Unternehmensumgebung zu gewähren, die dann letztendlich zur Exfiltration von Daten und zur Bereitstellung von Ransomware genutzt wird. Dieser sich abzeichnende Trend verdeutlicht, wie eng die Cyberkriminellen zusammenarbeiten, und wie wichtig es ist, wachsam zu bleiben und fortschrittliche Sicherheitsmaßnahmen zu ergreifen, um diesen sich ständig weiterentwickelnden Bedrohungen entgegenzuwirken.



3. Ransomware-Angreifer werden zunehmend GenAI einsetzen, um effektivere, personalisierte und lokalisierte Kampagnen zu erstellen.

Die zunehmende Verbreitung generativer KI im Jahr 2025 und darauffolgenden Jahren wird es Angreifern ermöglichen, Spam-E-Mails mit korrekter Grammatik und Rechtschreibung zu verfassen und sich mithilfe von Voice Cloning als Mitarbeiter auszugeben, um Zugriff inklusive aller nötigen Berechtigungen zu erhalten. In den kommenden Jahren könnten KI-generierte Stimmen mit regionalen Akzenten und Dialekten versehen werden, um die Glaubwürdigkeit zu erhöhen und die Erfolgswahrscheinlichkeit zu steigern — und Ransomware-Angreifern so dabei zu helfen, Angriffe noch überzeugender und unauffälliger zu gestalten.

4. Im Rahmen der neuen SEC-Regeln werden mehr Cybersicherheitsvorfälle gemeldet werden.

Aufgrund der Entscheidung der SEC, die eine strengere Berichterstattung über Cybersicherheitsvorfälle vorschreibt, werden im Jahr 2025 weiterhin mehr Organisationen Ransomware-Vorfälle melden. Dies wird hoffentlich zu mehr Transparenz führen und sich positiv auf das Verantwortungsbewusstsein und proaktive Abwehrmaßnahmen auswirken, was wiederum zu Verbesserungen bei Cybersicherheitsmaßnahmen führen wird.

5. Ransomware-Angriffe mit umfangreicher Datenexfiltration werden zunehmen.

Angriffe, bei denen große Datenmengen exfiltriert werden, einschließlich mehr Vorfälle ohne Verschlüsselung, werden im kommenden Jahr erheblich zunehmen. Bei diesem Trend, der 2022 verstärkt in Erscheinung trat, konzentrieren sich die Bedrohungsakteure ausschließlich auf die Exfiltration von Daten, ohne die Systeme zu verschlüsseln. Durch dieses Vorgehen können Angreifer schneller und flexibler agieren und die Angst vor der Veröffentlichung sensibler Daten ausnutzen, um Opfer zur Zahlung von Lösegeld zu zwingen. Diese Entwicklung unterstreicht den kontinuierlichen Wandel der Ransomware-Strategien hin zu effizienteren und schlagkräftigeren Methoden.

6. Insbesondere Unternehmen im Gesundheitswesen werden weiterhin das Ziel von Ransomware-Gruppen sein.

Gesundheitsdaten werden auch im Jahr 2025 von großem Wert sein und daher nach wie vor im Fokus stehen. Viele Unternehmen im Gesundheitswesen schaffen es nicht, veraltete Systeme durch moderne, fortschrittliche Sicherheitsmaßnahmen zu ersetzen, was sie besonders angreifbar macht. Infolgedessen müssen diese Organisationen mit wiederholten Datenpannen und Erpressungsversuchen rechnen. Wer es versäumt, geeignete Maßnahmen zu ergreifen und Zero-Trust-Verteidigungsstrategien zu priorisieren, könnte ins Visier von Ransomware-Gruppen geraten.

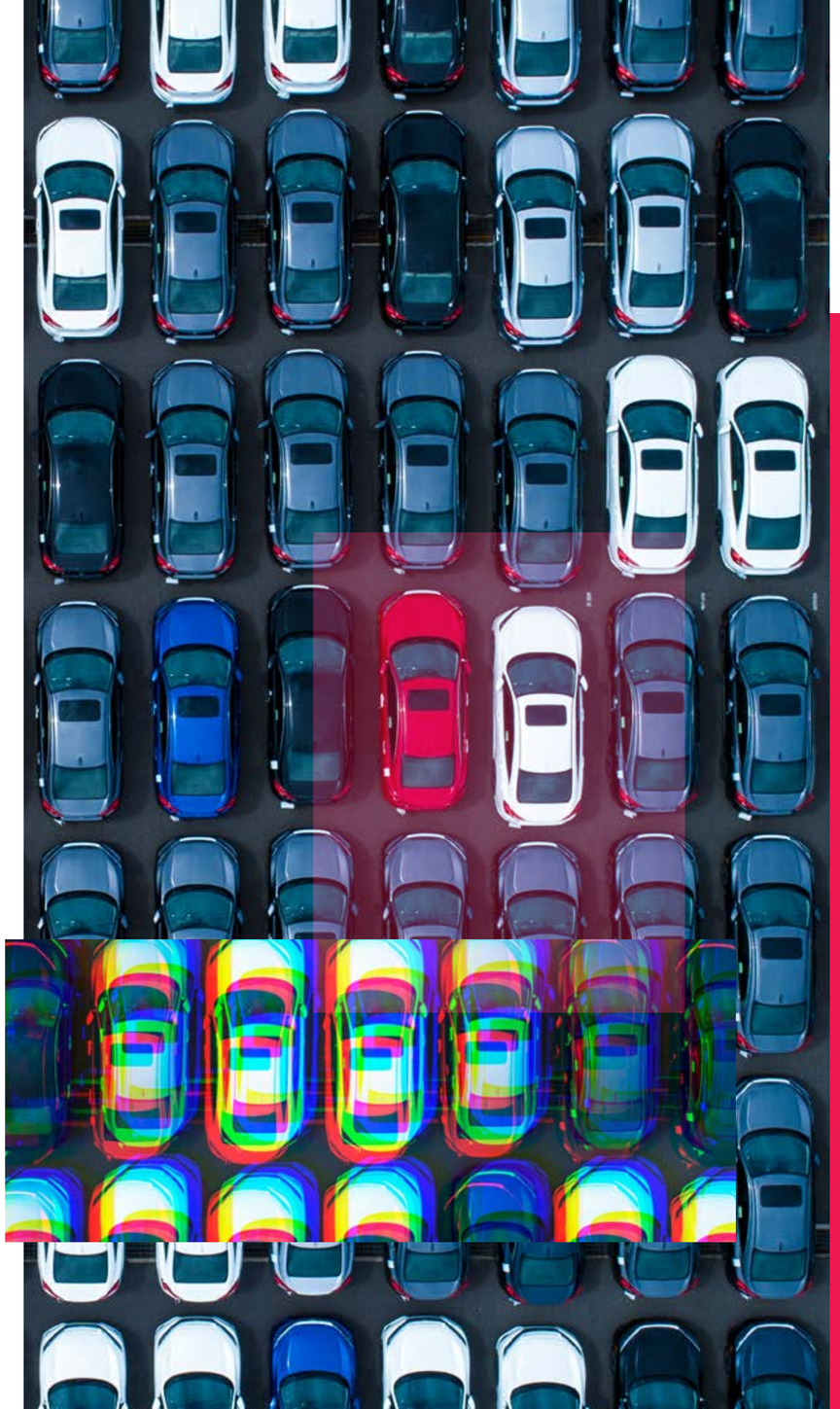
7. Die internationale Zusammenarbeit gegen cyberkriminelle Organisationen wird sich weiter verstärken.

Strafverfolgungsbehörden und Privatwirtschaft werden weiterhin bei der Bekämpfung von Ransomware-Angriffen zusammenarbeiten, z. B. durch die Zerschlagung großer Initial Access Broker und Ransomware-Gruppen. Die internationale Zusammenarbeit wird mit zunehmender globaler Vernetzung immer wichtiger, da Cyberkriminelle dadurch leichter über Landesgrenzen hinweg agieren können. Durch den Austausch von Informationen und Fachwissen werden diese koordinierten Maßnahmen globale Ransomware-Netzwerke effektiver lahmlegen. Zscaler ThreatLabz war im vergangenen Jahr federführend und maßgeblich an der Bereitstellung technischer Unterstützung für mehrere dieser Operationen beteiligt.

So vereinfacht Zscaler den Schutz vor Ransomware

Die zunehmende Komplexität und die steigenden Kosten von Ransomware-Angriffen zeigen, wie wichtig umfassende Zero-Trust-Abwehrmaßnahmen sind. Die Plattform **Zscaler Zero Trust Exchange™** bietet einen ganzheitlichen Ansatz zur Abwehr von Ransomware und somit eine einfache Lösung für dieses Problem.

Mithilfe der Zero Trust Exchange können Unternehmen in jeder Phase eines Angriffs intelligentere Abwehrmaßnahmen implementieren. Zunächst wird verhindert, dass Angreifer User und Anwendungen entdecken oder ausnutzen können, indem diese verborgen werden und nur autorisierten Usern oder Geräten zugänglich sind. Der gesamte — verschlüsselte wie unverschlüsselte — ein- und ausgehende Traffic wird durch Inline-Überprüfung untersucht. Authentifizierte User und Geräte werden direkt mit den jeweils benötigten Anwendungen verbunden, ohne jemals Zugang zum Netzwerk zu erhalten. Falls es Angreifern also doch gelingt, die Authentifizierung zu umgehen, können sie sich trotzdem nicht lateral durchs Netzwerk bewegen und entsprechend auch keine Daten exfiltrieren bzw. verschlüsseln.



ZERO TRUST ALS UNVERZICHTBARER SCHUTZ VOR RANSOMWARE
Veraltete Sicherheitsarchitekturen sind gegen die heutigen Ransomware-Angriffe wirkungslos.

ALTE LÖSUNGEN AUSMUSTERN:
Herkömmliche Sicherheitsmaßnahmen und Einzellösungen, einschließlich Firewalls und VPNs „der nächsten Generation“, führen oft zu Transparenzlücken, Komplexität und erheblichen Kosten. Mit diesen veralteten Ansätzen können verschlüsselte Dateien und Traffic nicht kosteneffizient überprüft werden, sodass Unternehmen anfällig für laterale Bewegungen und Ransomware-Angriffe sind, die Transparenz- und Kontrolldefizite ausnutzen - oft mit verheerenden Folgen.

MIT ZERO TRUST ERSETZEN: Eine Zero-Trust-Architektur geht davon aus, dass jeder User, jedes Gerät und jede Verbindung potenziell kompromittiert ist. Dieser Ansatz erfordert eine kontinuierliche Überprüfung und strenge Zugriffskontrollen. Durch die konsequente Überprüfung von Identitäten und die Untersuchung des gesamten Traffics, einschließlich verschlüsselter Daten, reduziert Zero Trust das Risiko, dass sich Angriffe im Netzwerk ausbreiten, erheblich und neutralisiert Ransomware-Bedrohungen, bevor sie Schaden anrichten können.

ZSCALER STOPPT RANSOMWARE IN JEDER PHASE DES ANGRIFFSZYKLUS— von Aufklärungsphase und Erstzugriff bis hin zu lateraler Ausbreitung, Datendiebstahl und Ausführung von Payloads.

Minimierung der Angriffsfläche: Die Zero Trust Exchange basiert auf einer Zero-Trust-Architektur, die angreifbare veraltete VPN- und Firewall-Architekturen ersetzt, die die Angriffsfläche vergrößern. Zscaler minimiert die Angriffsfläche weiter, indem User, Geräte und Anwendungen hinter einem Cloud-Proxy verborgen werden, sodass sie vom Internet aus nicht sichtbar oder auffindbar sind. Ähnlich wie eine Telefonzentrale, die Anrufe an autorisierte Personen weiterleitet, verbindet Zscaler nur den richtigen, autorisierten User oder das richtige Gerät mit einer bestimmten Anwendung.

Verhinderung des Erstzugriffs: Die Zero Trust Exchange beinhaltet eine umfassende TLL-/SSL-Überprüfung, Browser-Isolierung, fortschrittliches Inline-Sandboxing und richtliniengestützte Zugriffskontrollen, um zu verhindern, dass User auf bösartige Websites zugreifen und um unbekannte Bedrohungen zu erkennen, bevor sie Ihr Netzwerk erreichen. Dadurch wird das Risiko des Erstzugriffs durch Angreifer minimiert.

Unterbindung lateraler Bewegungen: Dank der User-to-App- und App-to-App-Segmentierung verbinden sich User direkt mit Anwendungen (und Anwendungen mit anderen Anwendungen) und nicht mit dem Netzwerk, wodurch das Risiko lateraler Bewegungen entfällt. Durch die zentrale Verwaltung von Richtlinien zur Zugriffskontrolle fungiert Zscaler als Kontrollpunkt für den Internet-Traffic und schließt so Wege, die sonst von Angreifern genutzt werden würden. Zscaler kann dank ITDR- (Identity Threat Detection & Response) und Deception-Funktionen auch potenzielle Angreifer identifizieren und daran hindern, sich lateral zu bewegen, unabhängig davon, ob es sich um externe Bedrohungen oder böswillige Insider handelt.

Vermeidung von Datenverlusten: Inline-Maßnahmen zum Schutz vor Datenverlusten in Kombination mit einer vollständigen SSL-/TLS- Überprüfung verhindern, dass Daten gestohlen werden können. So stellt Zscaler sicher, dass sowohl ruhende Daten als auch Daten während der Übertragung geschützt sind.

ABWEHR KI-GESTÜTZTER BEDROHUNGEN MIT KI- + ZERO-TRUST-INNOVATIONEN

Dank dieser KI-gestützten Funktionen bietet Zscaler einen robusten Schutz vor Ransomware und gewährleistet umfassende Sicherheit für Unternehmen in der sich ständig weiterentwickelnden Bedrohungslandschaft:

- ***KI-gestützte Phishing- und C2-Erkennung*** gegen bislang unbekannte Phishing-Websites und C2-Infrastruktur mithilfe der KI-basierten Inline-Erkennung des Zscaler Secure Web Gateway (SWG).
- ***KI-gestütztes Sandboxing*** bietet umfassenden Schutz vor Malware und Zero-Day-Bedrohungen durch die Analyse verdächtiger Dateien in einer kontrollierten Umgebung.
- ***KI-gestützte Segmentierung*** auf Basis automatisierter Zugriffsrichtlinien, um die Angriffsfläche zu minimieren und laterale Ausbreitung mithilfe von Userkontext, Verhalten, Standort und Telemetrie für unternehmensinterne Anwendungen zu stoppen.
- ***Dynamische, risikobasierte Richtlinien*** analysieren kontinuierlich die mit Usern, Geräten und Anwendungen verbundenen Risiken, um dynamische Sicherheits- und Zugriffsrichtlinien durchzusetzen.
- ***KI-gestützte Browser-Isolierung***, die User durch einen undurchdringlichen Air Gap vom Internet isoliert; Web-Inhalte werden als gestochen scharfer Bilderstrom angezeigt und das Risiko von Datenverlusten und aktiven Bedrohungen ausgeschaltet.
- ***KI-gestützte Datenerkennung und -klassifizierung*** sorgt für sofortige Datentransparenz und -klassifizierung über Endgeräte, Inline- und Cloud-Daten hinweg, wodurch es für Ransomware schwieriger wird, sensible Daten anzugreifen und zu verschlüsseln.

Ganzheitlicher Schutz in jeder Phase der Angriffskette

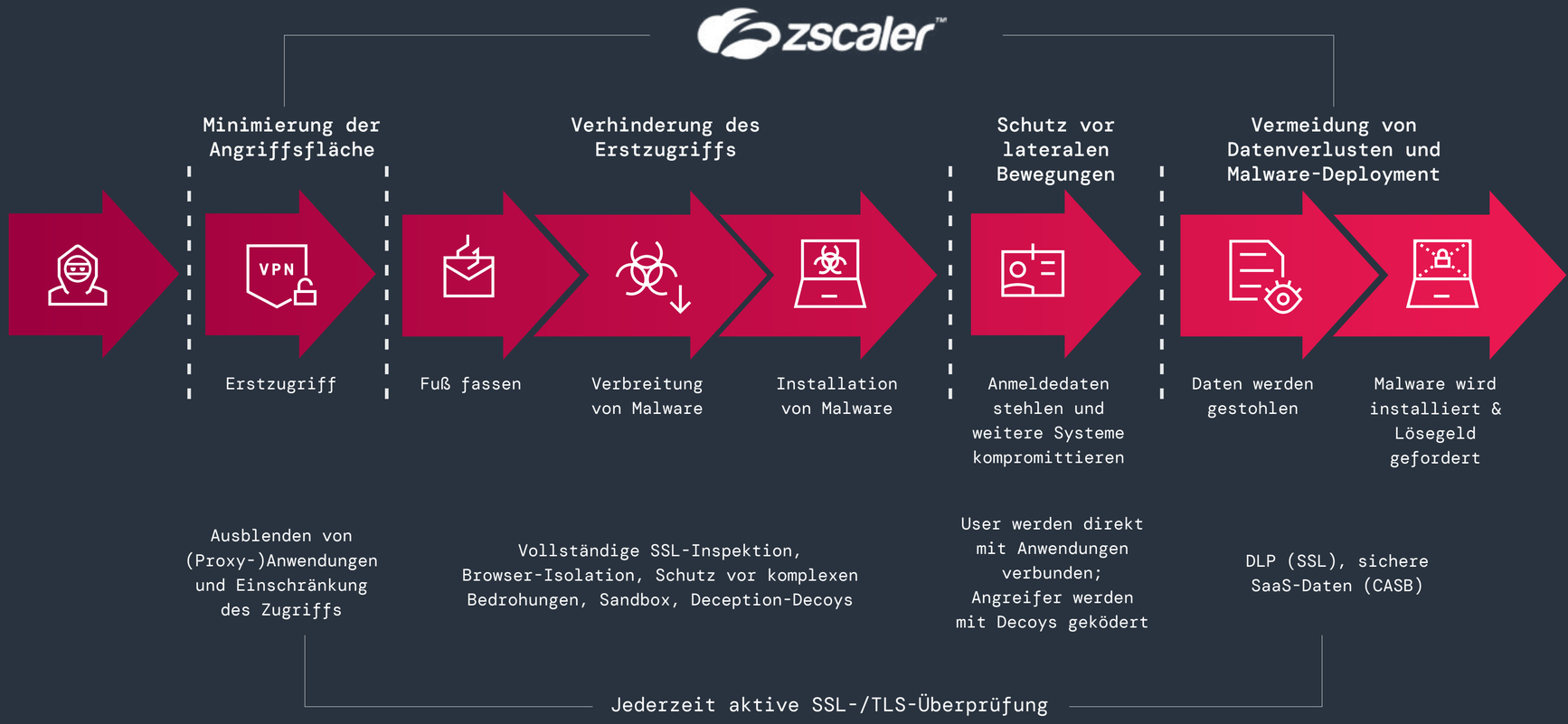


Abb. 23: Vorteile einer Zero-Trust-Architektur in sämtlichen Phasen von Ransomware-Angriffen

Weitere relevante Produkte von Zscaler

Zscaler Internet Access™ (ZIA™) bietet sicheren und direkten Zugriff auf das Internet und Schutz vor komplexen Bedrohungen. Die fortschrittlichen Funktionen von ZIA zur Verhinderung von Bedrohungen und Sandboxing helfen dabei, Ransomware-Downloads und C2-Kommunikation (Command-and-Control) zu unterbinden und so das Eindringen von Ransomware zu verhindern.

Zscaler Private Access™ (ZPA™) stellt sicheren Zugriff auf interne Anwendungen ohne Internetverbindung bereit und nutzt dabei ein Zero-Trust-Modell. ZPA stellt sicher, dass nur autorisierte User und Geräte auf kritische Anwendungen zugreifen können, wodurch die Angriffsfläche reduziert und Ransomware-Angriffe verhindert werden.

Zscaler Zero Trust Firewall fängt TLS-/SSL-Traffic ab und untersucht ihn, um im verschlüsselten Traffic verborgene Malware zu erkennen und deren Eindringen in das Netzwerk zu verhindern.

Zscaler Deception ködert und entlarvt Angreifer beim Versuch, sich lateral durchs Netzwerk zu bewegen bzw. sich erweiterte Zugriffsberechtigungen zu verschaffen, mit Decoys, die echten Servern, Anwendungen, Verzeichnissen und User-Konten täuschend ähnlich sehen.

Zscaler Sandbox analysiert verdächtige und ausführbare Dateien in einer kontrollierten virtuellen Umgebung und kann so schädlichen Code identifizieren und blockieren, sodass Unternehmen dateibasierter Ransomware und Zero-Day-Angriffen immer einen Schritt voraus sind.

Zscaler Cloud Browser isoliert Websitzungen und streamt nur Pixel an Geräte, um das Risiko von Drive-by-Downloads und Zero-Day-Exploits, die von Ransomware-Betreibern genutzt werden könnten, effektiv zu unterbinden.

Zscaler ITDR (Identity Threat Detection and Response) stellt leistungsstarke Funktionen zum Erkennen von und Schutz vor identitätsbezogenen Angriffen bereit. Damit verhindern Sie Bedrohungen wie Diebstahl von Anmeldedaten, Missbrauch von Berechtigungen, Active-Directory-Angriffe, riskante Berechtigungen usw.

Zscaler Data Protection bietet konsistente, einheitliche Sicherheit für in Übertragung befindliche und ruhende Daten in SaaS- und öffentlichen Cloud-Anwendungen und verringert so die Wahrscheinlichkeit einer Datenexfiltration, während gleichzeitig die potenziellen Auswirkungen von Ransomware-Angriffen gemindert werden.

Praxisempfehlungen zur Ransomware-Prävention

Eine Verteidigungsstrategie, die auf einer Zero-Trust-Architektur basiert, ist eine bewährte Sicherheitsmaßnahme, um Ransomware zu stoppen. Um dieser vielschichtigen Bedrohung zu begegnen, sind jedoch proaktive Planung, kontinuierliche Zusammenarbeit und strategische Investitionen erforderlich.

Die Experten von ThreatLabz haben die neuesten Best Practices zusammengestellt, um Ransomware-Risiken zu reduzieren und Ihr Unternehmen vor bestehenden und neuen Bedrohungen zu schützen.

- **Führen Sie regelmäßige und sichere Backups Ihrer Daten durch.** Achten Sie darauf, dass alle Daten regelmäßig und zuverlässig gesichert werden, auch offline. Passen Sie Backup-Strategien an sich verändernde Bedrohungen an.
- **Halten Sie Ihre Software auf dem neuesten Stand.** Installieren Sie umgehend die neuesten Sicherheitspatches, um bekannte Schwachstellen zu beheben. Verwenden Sie KI-gestützte Threat Intelligence-Plattformen, um Sicherheitspatches effektiv zu priorisieren und zu verwalten.
- **Richten Sie eine Multifaktorauthentifizierung (MFA) ein.** Fügen Sie User-Konten eine zusätzliche Sicherheitsebene hinzu, um das Risiko unbefugter Zugriffe zu minimieren. Integrieren Sie MFA-Lösungen, um Kontoübernahmen effektiv zu erkennen und zu verhindern.
- **Führen Sie eine einheitliche Sicherheitsrichtlinie für Ihr Unternehmen ein.** Stellen Sie sicher, dass alle User einheitliche Sicherheitsverfahren befolgen, einschließlich MFA und regelmäßiger Sicherheitsupdates, um Erstzugriffe zu verhindern. Bei einer dezentralen Belegschaft ist es umso wichtiger, eine SSE-Architektur (Security Service Edge) zu implementieren, um User unabhängig von ihrem Standort zu schützen.
- **Stärken Sie die Anwendungssicherheit.** Entfernen Sie Anwendungen aus dem öffentlichen Internet, um zu verhindern, dass Ransomware-Angreifer Schwachstellen ausnutzen. Implementieren Sie eine Zero-Trust-Architektur für interne Anwendungen, um sie vor Ransomware-Angriffen zu schützen.
- **Setzen Sie Zugriff mit minimaler Rechtevergabe durch.** Implementieren Sie entsprechende Richtlinien, um den Zugriff von Usern auf die für ihre Aufgaben erforderlichen Ressourcen zu beschränken. Nutzen Sie KI-gestützte Lösungen, um das Userverhalten dynamisch zu analysieren und Zugriffsrechte entsprechend anzupassen.
- **Stärken Sie den Identitätsschutz.** Verschaffen Sie sich mit ITDR-Tools einen Überblick über Identitätsfehlkonfigurationen und beheben Sie Schwachstellen in Ihrem Active Directory, die Angreifer ausnutzen, um ihre Berechtigungen auszuweiten und sich lateral zu bewegen. So können Sie zudem versteckte Identitätsbedrohungen erkennen.
- **Überprüfen Sie den gesamten Traffic.** Heutzutage werden 86 % der Bedrohungen über verschlüsselte Kanäle übertragen, die oft nicht überprüft werden, was es selbst nicht sonderlich versierten Angreifern leicht macht, Sicherheitskontrollen zu umgehen. Es ist unerlässlich, den gesamten Traffic zu überprüfen, ob verschlüsselt oder nicht, um eine Kompromittierung zu verhindern.
- **Implementieren Sie Zero Trust Network Access (ZTNA).** Setzen Sie granulare User-to-Application- und Application-to-Application-Segmentierung ein und vermitteln Sie den Zugriff über Zugriffskontrollen mit minimaler Rechtevergabe, um laterale Bewegungen zu unterbinden, die Exposition von Daten zu minimieren und Ihren allgemeinen Sicherheitsstatus zu verbessern.

- **Nutzen Sie die KI-gestützte Browser-Isolierung.** Schützen Sie User durch die KI-basierte Isolierung verdächtiger Internetinhalte und User mit hohem Risiko vor Web-Bedrohungen. Durch die Isolierung der Browser-Erfahrung und die Unterbindung potenziell schädlicher Aktionen (wie die Eingabe von Anmeldedaten) können User sicher auf verdächtige URLs und Dateien zugreifen, ohne die Sicherheit ihrer Systeme zu gefährden.

- **Verwenden Sie KI-gestütztes, fortschrittliches Sandboxing.** Blockieren Sie bisher unbekannte und nur schwer zu erkennende Malware mit einer Sandbox, die unbekannte Bedrohungen und verdächtige Dateien mithilfe von KI-/ML-Analysen automatisch erkennt und unter Quarantäne stellt.

- **Implementieren Sie Inline-DLP (Data Loss Prevention).** Schützen Sie sich vor Daten-exfiltration und -offenlegung, indem Sie DLP-Maßnahmen einsetzen.

- **Nutzen Sie Deception-Technologie.** Setzen Sie Deception-Tools und Honeypots ein, um Angreifer in die Irre zu führen und den Schutz vor Systeminfiltration zu verstärken.

- **Nutzen Sie einen Cloud Access Security Broker (CASB).** Kontrollieren und überwachen Sie die Nutzung von Cloud-Anwendungen mit einem CASB, um böswillige Aktivitäten wie das Herunterladen von Dateien und die Exfiltration von Daten zu verhindern.

- **Bieten Sie fortlaufende Mitarbeiterschulungen an.** Führen Sie regelmäßige Schulungen zum Sicherheitsbewusstsein durch, um Mitarbeiter über Ransomware-Bedrohungen aufzuklären. Setzen Sie Simulationen realer Ransomware-Szenarien ein, um die Reaktionsfähigkeit der Mitarbeiter zu verbessern.

- **Entwickeln Sie einen umfassenden Plan zur Reaktion auf Ransomware.** Erstellen Sie einen Reaktionsplan, der Datenwiederherstellung, Reaktion auf Vorfälle und Kommunikations-protokolle umfasst, um im Falle eines Ransomware-Angriffs schnell und effektiv handeln zu können.

Folgen Sie dem Forschungsteam von Zscaler ThreatLabz. Erhalten Sie regelmäßig Einblicke in die neuesten Ransomware-Bedrohungen und Entwicklungen in diesem Bereich, einschließlich veröffentlichter IOCs (Indicators of Compromise) und Aufschlüsselungen nach dem MITRE ATT&CK-Framework. Diese Informationen können Sie nutzen, um Ihr Team zu schulen, Ihren Sicherheitsstatus zu verbessern und IoT-Angriffe zu verhindern.

ThreatLabz betreibt auch GitHub-Repositories mit IOCs, Tools (einschließlich Proof-of-Concept-Ransomware-Entschlüsselungstools) und ein Archiv über Lösegeldforderungen aller großen Ransomware-Gruppen.

Folgen Sie ThreatLabz auf X @ThreatLabz und lesen Sie unseren Blog zur Sicherheitsforschung.

Methodik

Diesem Report liegt ein umfassender Forschungsprozess zugrunde, in dessen Rahmen Daten aus verschiedenen Quellen analysiert wurden, um Ransomware-Trends zu erkennen und zu verfolgen. Insbesondere wurden Daten aus folgenden Quellen zwischen April 2023 und März 2024 erfasst und ausgewertet:

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

- **Externe Informationsquellen:** Wir haben auch Daten aus externen Informationsquellen wie Bedrohungsdaten-Feeds, Open-Source-Recherchen und Berichten von Strafverfolgungsbehörden gesammelt, die zusätzliche Informationen über Ransomware-Angreifer, ihre Ziele und ihre Methoden lieferten.

- **Eigene Analyse von Ransomware-Samples und Angriffsdaten durch das ThreatLabz-Team.** Das ThreatLabz-Threat-Intelligence-Team beobachtet Ransomware-Familien in großem Maßstab durch Reverse Engineering und automatisierte Malware-Analyse, um effektive Reaktionsstrategien zu entwickeln. ThreatLabz arbeitet auch eng mit internationalen Strafverfolgungsbehörden zusammen und hat bei jüngsten Aktionen, darunter Operation Duck Hunt und Operation Endgame, eine bedeutende Rolle gespielt.

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.

Über Zscaler

Zscaler (NASDAQ: ZS) beschleunigt die digitale Transformation, damit Kunden agiler, effizienter, stabiler und sicherer arbeiten können. 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 150 Rechenzentren auf der ganzen Welt bereitgestellt. Weitere Informationen finden Sie unter **www.zscaler.de.**