Cyberint
A Check Point Company

BEDROHUNGSLANDSCHAFT DER REISE- UND TOURISTIKBRANCHE

July 2025

TABLE OF CONTENTS

EXECUTIVE SUMMARY

Cyberint hat einen Bericht über die Bedrohungslandschaft erstellt, der sich auf die Reise- und Touristikbranche konzentriert. Der folgende Bericht beschreibt die jüngsten Cyber-Ereignisse, Cyber-Bedrohungsprognosen und gibt einen Überblick über die Cyberint-Services als Lösung zur Eindämmung digitaler Bedrohungen.

Von 2023 bis 2025 sah sich die globale Reisebranche mit einem Anstieg gezielter Cyberangriffe konfrontiert, darunter DDoS-Angriffe, Ransomware-Vorfälle, Datenschutzverletzungen durch falsch konfigurierte Cloud-Speicher und Kompromittierungen der Lieferkette Dritter. Der Bericht enthält einen Überblick über diese Ereignisse weltweit. Außerdem enthält er eine Liste der wichtigsten TTPs (Tools und Techniken) der Hacker sowie eine Liste der damit verbundenen IOCs, die beachtet und blockiert werden sollten.

Im Folgenden sind die von Cyberint erwarteten Trends aufgeführt, die auf den entsprechenden Vorfällen basieren:

DDoS-Angriffe, die Buchungssysteme stören

Diese Angriffe werden oft auf Hauptreisezeiten abgestimmt und nutzen die Abhängigkeit der Branche von Echtzeit-Online-Diensten aus. Es wird erwartet, dass Hacker weiterhin Botnets einsetzen werden, um den Betrieb lahmzulegen, was möglicherweise zu Erpressungsforderungen für die Wiederherstellung der Dienste führt.

Datenschutzverletzungen durch falsch konfigurierte Cloud-Speicher

Angreifer verwenden zunehmend fortschrittliche Tools und automatisierte Skripte, um Daten aus ungeschützten Cloud-Speichern zu identifizieren und zu exfiltrieren. Kleine bis mittelgroße Reiseunternehmen ohne starke DevSecOps-Praktiken sind nach wie vor stark gefährdet.

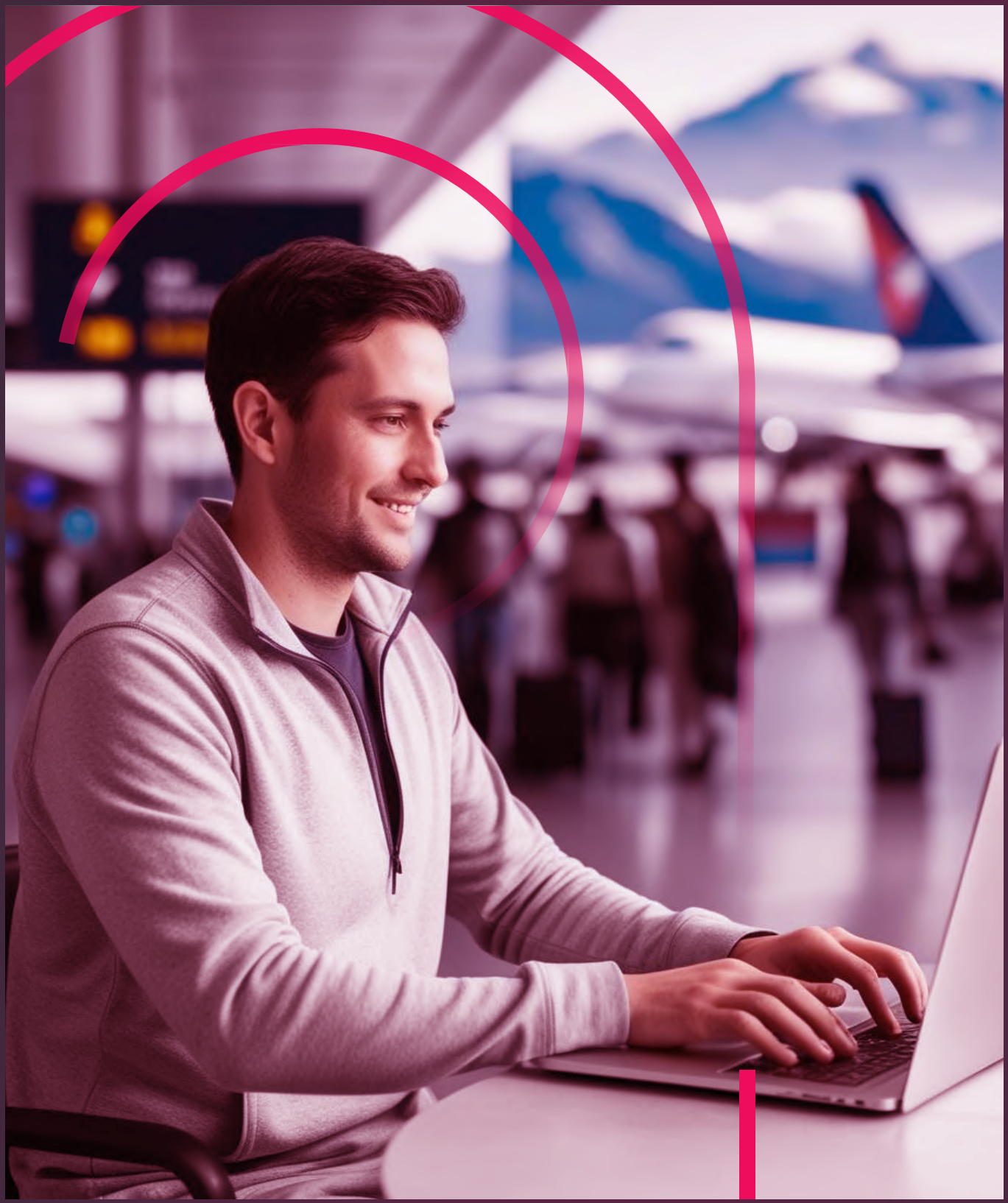
Phishing und Ausnutzung von Anmeldedaten

Angreifer nutzen fortschrittliche Social-Engineering-Techniken, einschließlich Imitationen und KI-generierte Phishing-Köder, um Anmeldedaten von Mitarbeitern abzugreifen. Diese Angriffe ermöglichen den Einsatz von Ransomware, die interne Datenexfiltration und das Fortbestehen des Systems.

Kompromittierung der Lieferkette und Risiken für Drittanbieter

Hacker umgehen gehärtete Perimeter, indem sie Anbieter von Zahlungsverarbeitung, Authentifizierung und Cloud-Infrastruktur ins Visier nehmen und oft veraltete oder unsichere Anwendungen nutzen, um in Kernsysteme einzudringen und sensible Daten zu exfiltrieren

Um diese sich entwickelnden Bedrohungen abzuschwächen, bietet Cyberint kontinuierliche Threat Intelligence (TI) und Attack Surface Monitoring (ASM), die auf das externe Risikoumfeld der Reisebranche zugeschnitten sind. Wir erkennen Frühindikatoren für eine Gefährdung, exponierte Anlagen und Aktivitäten von verschiedenen Hackergruppen oder Individuen durch eine umfassende Überwachung über einen umfangreichen Pool von Quellen. Dieser proaktive Ansatz ermöglicht es Reiseunternehmen, gezielten Bedrohungen einen Schritt voraus zu sein und negative Auswirkungen auf den Betrieb und den Ruf zu minimieren.



CYBER-VORFÄLLE

TIMELINE WICHTIGER EREIGNISSE

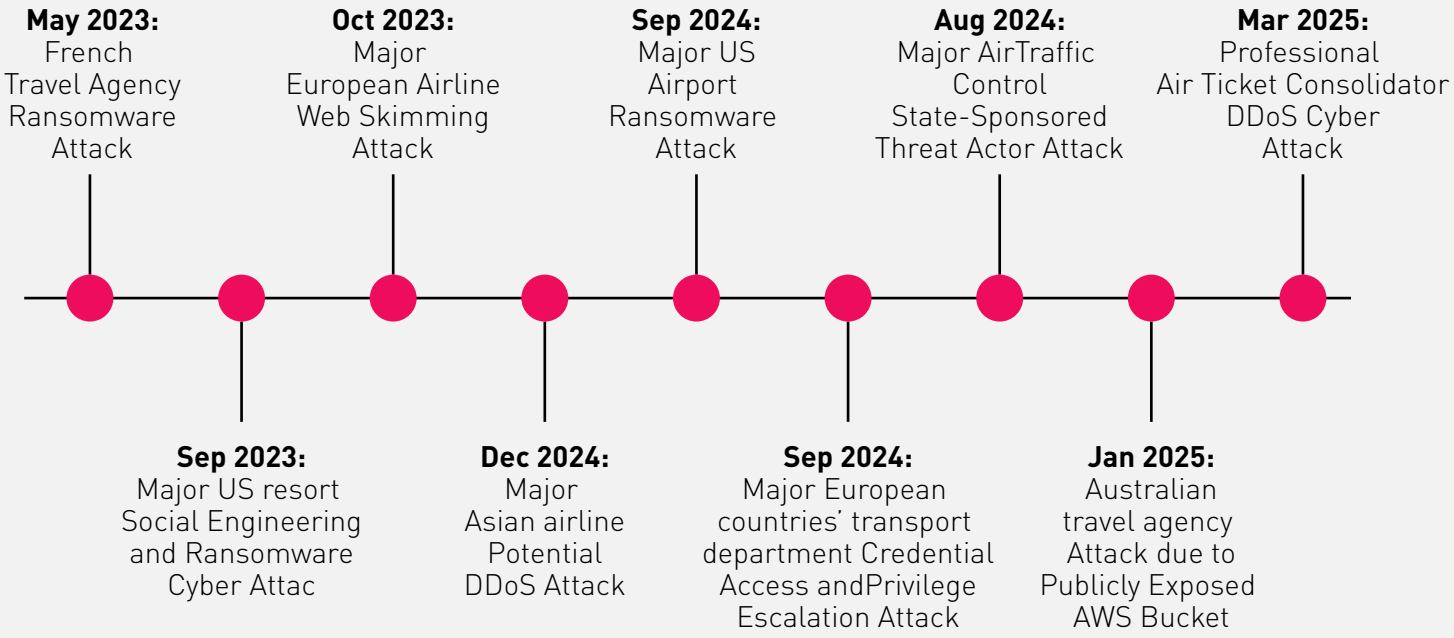


Figure 1: Timeline of Cyber Attacks Covered in this Report

CYBER INCIDENTS DETAILS

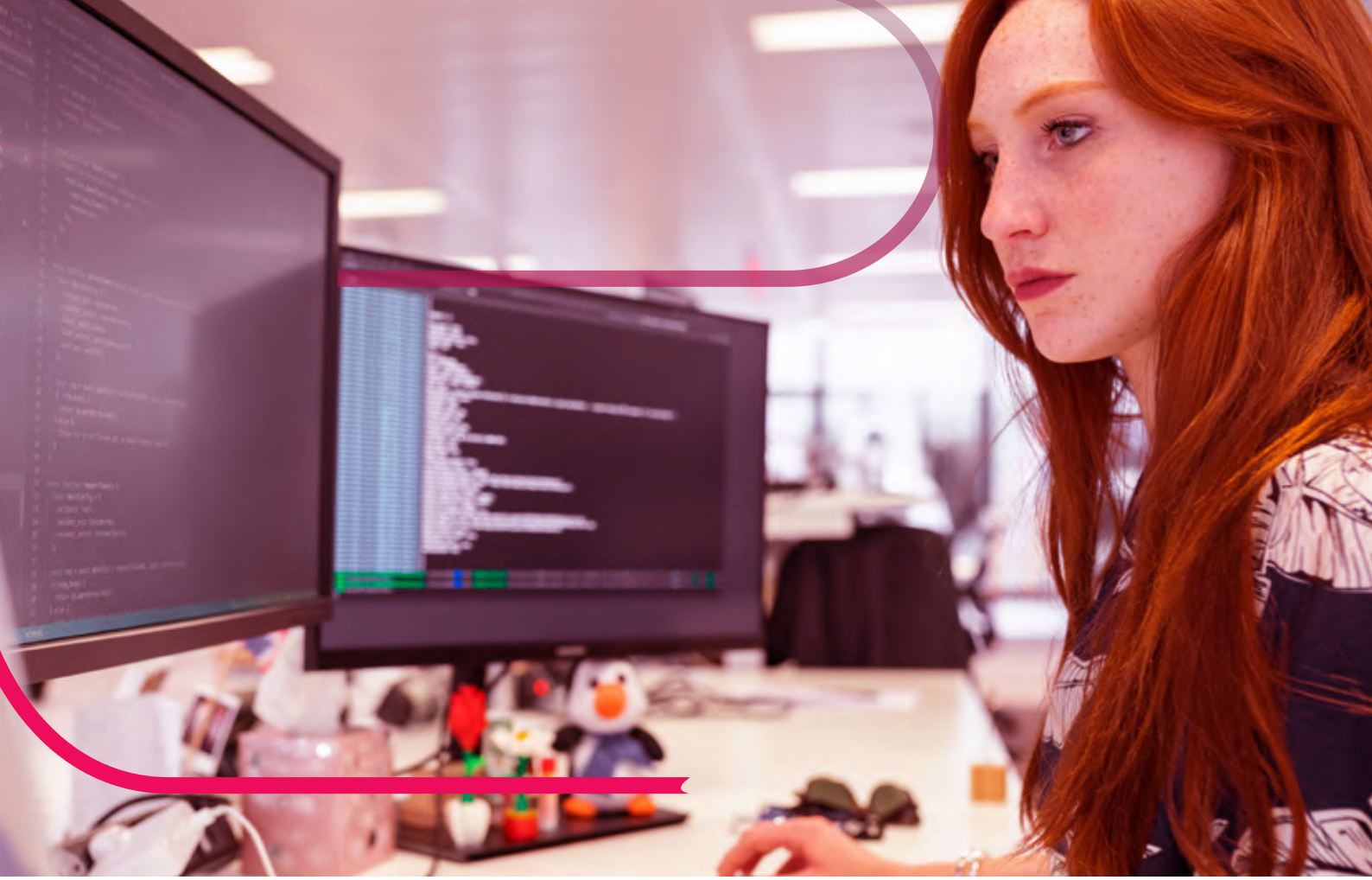
Online Ticket Merchant DDoS Attack

Im März 2025 wurde der Betrieb eines Unternehmens durch eine Cyber-Attacke gestört, von der Kunden in Deutschland, Österreich, der Schweiz und weltweit betroffen waren.
Das Buchungssystem "Cockpit" wurde durch einen möglichen DDOS-Angriff beeinträchtigt.

Angriff auf ein australisches Reisebüro aufgrund eines öffentlich zugänglichen AWS-Buckets

Im Januar 2025 wurde ein australisches Reisebüro angegriffen, was zum Verlust von 112.000 Datensätzen aus der nicht passwortgeschützten Datenbank des Unternehmens mit einer Größe von 26,8 GB führte, darunter Details wie Passbilder, Reisevisa, Reiserouten und Tickets sowie teilweise Kreditkartennummern von Kunden. Es wurde festgestellt, dass Tabellen mit detaillierten Informationen über mehr als 13.000 Kunden, darunter Namen, E-Mail-Adressen, Reisekosten und Reiseziele, nach außen gelangt sind. Bei den meisten betroffenen Reisenden handelt es sich um Australier, aber auch Kunden aus Neuseeland, Irland und Großbritannien sind betroffen.

Die Sicherheitsverletzung war auf einen öffentlich zugänglichen Amazon AWS Cloud Storage Bucket zurückzuführen, der falsch konfiguriert war. Diese Angriffe beginnen in der Regel mit der Suche nach offenen Systemen oder falsch konfiguriertem Cloud-Speicher. Es wurden Tools oder Skripte verwendet, um nach offenen S3-Buckets oder Cloud-Speicherdiensten zu suchen (z. B. Bucket Finder, S3Scanner, Shodan, Censys oder Grayhat Warfare). Hacker nutzen auch schlagwortbasierte Automatisierungen, um nach Dateien wie passwords.txt, .env, db_backup.sql usw. zu suchen.



Deutsche Flugsicherung Staatlich gesponserter Angriff

Im August 2024 wurde die administrative IT-Infrastruktur der Deutschen Flugsicherung, die die interne Bürokommunikation abwickelt, angegriffen. Dies ermöglichte den unbefugten Zugriff auf sensible Daten. Fancy Bear (auch bekannt als APT28), ein Bedrohungsakteur, der dem russischen Militärgeheimdienst zugeschrieben wird, wurde für diesen Angriff verantwortlich gemacht.

Angriff auf Anmeldeinformationen und Privilegieneskalation bei einer staatlichen Reiseorganisation

Im September 2024 wurde eine staatliche Reiseorganisation von einem Cyberangriff heimgesucht, der dazu führte, dass die Beantragung von Fotokarten aufgrund von Bedenken hinsichtlich der Systemsicherheit vorübergehend ausgesetzt wurde.

Dies betraf auch die Registrierung neuer Karten, die Erstattung unvollständiger Fahrten mit kontaktlosen Karten und die Verbesserung des Buchungssystems für den Dial-a-Ride-Dienst. Auch der Live-Reisedaten-Feed war beeinträchtigt. Bestehende Buchungen wurden zwar berücksichtigt, aber neue Buchungen konnten nur telefonisch vorgenommen werden, bis das System wiederhergestellt war. Es wurde auf die Daten von 5.000 Personen zugegriffen, darunter Namen, Kontaktdaten und Daten zur Erstattung von Oyster-Karten. Dazu gehörten auch Bankkontonummern und Bankleitzahlen.

Berichten zufolge verwendeten die Angreifer LicensingUI.exe (eine signierte Windows-Binärdatei), um Nutzdaten auszuführen. TfL musste die Passwörter von 30.000 Mitarbeitern persönlich zurücksetzen, was das Ausmaß des Angriffs verdeutlicht. Der Angreifer hat sich möglicherweise dauerhafte und erweiterte Rechte verschafft, möglicherweise mithilfe von geplanten Aufgaben oder Admin-Tokens.

Ransomware-Angriff auf US-Flughafen

Im September 2024 wurden mehrere kritische Systeme eines US-Flughafens durch einen Cyberangriff beeinträchtigt, der Rhysida-Mitgliedern zugeschrieben wird.

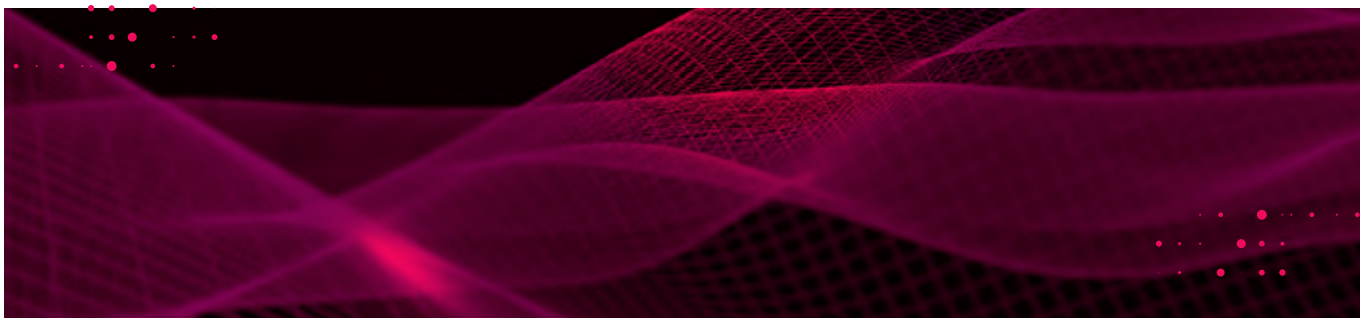
Verzögerungen bei der Gepäckabfertigung führten dazu, dass die Koffer den Reisenden erst lange nach ihrer Ankunft ausgehändigt wurden. Aufgrund von Systemausfällen mussten die Passagiere handgeschriebene Bordkarten verwenden. Die internen Hafensysteme waren verschlüsselt, was den Wiederherstellungsprozess behinderte.

Die Bedrohungsakteure griffen auf einige personenbezogene Daten aus zuvor verwendeten Hafensystemen für Mitarbeiter-, Auftragnehmer- und Parkdaten (90000 Personen) zu und luden diese herunter. Zu den heruntergeladenen Informationen gehörten Namen, Geburtsdaten, Sozialversicherungsnummern (oder die letzten vier Ziffern der Sozialversicherungsnummern), Führerschein- oder andere staatliche Ausweisnummern sowie medizinische Informationen.

Rhysida-Akteure arbeiten als Ransomware-as-a-Service (RaaS), bei dem Ransomware-Tools und -Infrastrukturen in einem Gewinnbeteiligungsmodell vermietet werden. Es wurde beobachtet, dass Rhysida-Akteure externe Remote-Dienste nutzen, um zunächst auf ein Netzwerk zuzugreifen und darin zu verbleiben. Es wurde auch beobachtet, dass sie sich an internen VPN-Zugangspunkten mit kompromittierten gültigen Anmeldedaten authentifizieren, insbesondere weil in Unternehmen standardmäßig keine MFA aktiviert ist. Darüber hinaus wurden sie dabei beobachtet, wie sie Zerologon - eine kritische Schwachstelle in Microsofts Netlogon Remote Protocol - ausnutzten und erfolgreiche Phishing-Versuche unternahmen.

Potenzieller DDoS-Angriff auf asiatische Fluggesellschaften

Im Dezember 2024 wurde eine asiatische Fluggesellschaft Opfer eines Cyberangriffs, der zu Flugverspätungen führte. JAL gab zwar nicht öffentlich bekannt, wer die Bedrohung verursacht hat, bestätigte aber, dass keine Kundendaten abgeflossen sind oder Computerviren entdeckt wurden. Bei dem Vorfall kam es zu einem sprunghaften Anstieg des Datenverkehrs, was auf einen DDoS-Angriff hindeutet, der die Systeme der Fluggesellschaft und den Ticketverkauf unterbrochen hat.



Web-Skimming-Angriff auf eine europäische Fluggesellschaft

Im Oktober 2023 verschaffte sich IncRansom (eine russische Hackergruppe) unbefugten Zugang zum Zahlungssystem der Fluggesellschaft. Die Methode des Angriffs wurde zwar nicht bestätigt, doch handelt es sich höchstwahrscheinlich um Web-Skimming.
Durch den Angriff wurden sensible Kundendaten offengelegt, darunter Kreditkarteninformationen wie Kartennummern, Ablaufdaten und CVV-Codes. Die Fluggesellschaft hat die betroffenen Kunden umgehend benachrichtigt und ihnen geraten, ihre Karten zu sperren, um eine mögliche betrügerische Nutzung zu verhindern. Im März 2024 aktualisierte die Fluggesellschaft ihre Informationen und teilte mit, dass weitere persönliche Daten wie Namen, Personalausweis- oder Reisepassnummern, Geburtsdaten, Telefonnummern, E-Mail-Adressen und Nationalitäten offengelegt worden waren.

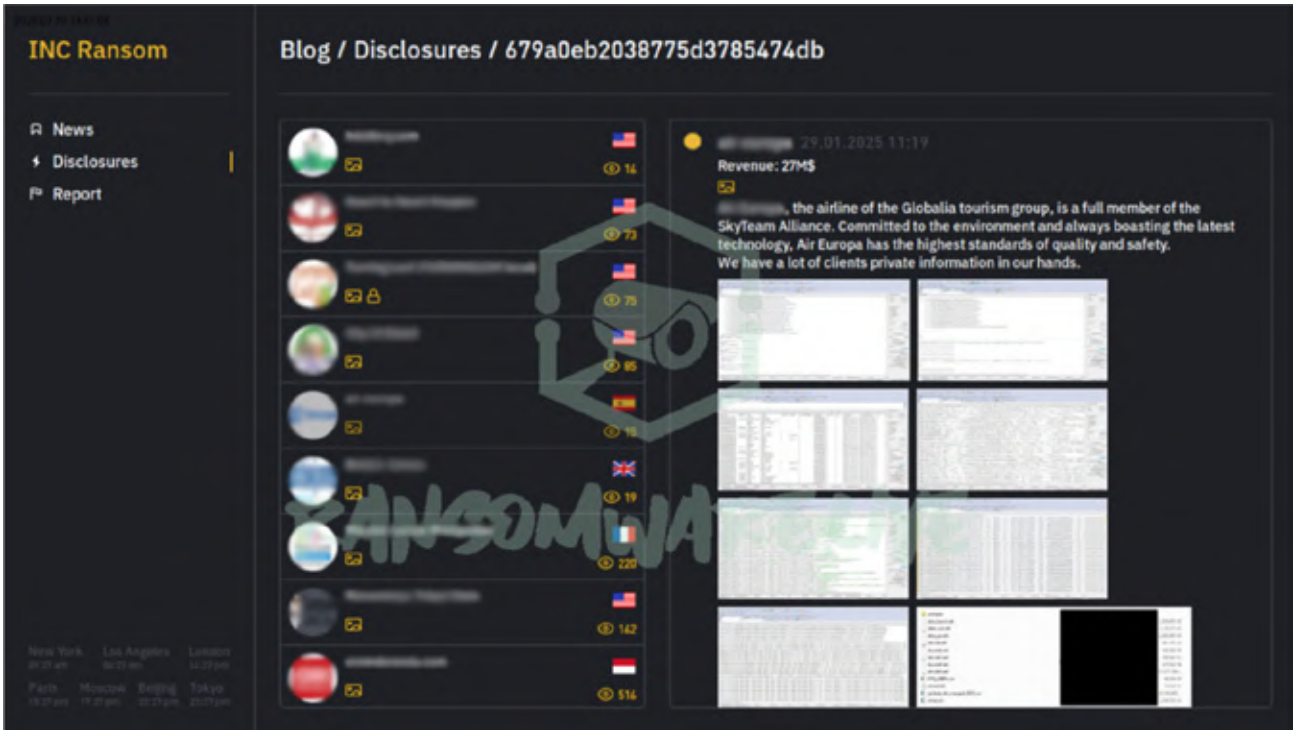


Figure 2: Screenshot from INCRansomware DLS affecting European Airline

Social-Engineering- und Ransomware-Cyberangriff auf ein US-Resort

Im September 2023 wurde ein US-Resort von einem Cyberangriff betroffen, der von Scattered Spider und ALPHV gemeinsam durchgeführt wurde.

Scattered Spider-Mitglieder recherchierten auf LinkedIn über die Mitarbeiter des Resorts, um Informationen zu sammeln. Sie gaben sich als Mitarbeiter aus und brachten den IT-Helpdesk dazu, ihnen Anmeldedaten zu geben. Mit diesen verschafften sich die Angreifer Administrator-Zugang zu den Okta- und Azure-Umgebungen des Resorts, wodurch sie sich seitlich in den Systemen bewegen konnten. ALPHV installierte dann Ransomware auf mehreren VMware ESXi Hypervisor-Servern.

Auf diesen Servern befanden sich Tausende von virtuellen Maschinen, die wichtige Gastgewerbesysteme wie Spielautomaten, Online-Reservierungssysteme, digitale Zimmerschlüssel und Websites unterstützten. ALPHV behauptet auch, in dieser Zeit 6 TB an Kundendaten exfiltriert zu haben, woraufhin sie Verhandlungen mit MGM aufnahmen, um die Veröffentlichung der gestohlenen Daten zu verhindern.

Ransomware-Angriff auf ein Reisebüro

Im Mai 2023 griff Lockbit ein französisches Reisebüro an. Nachdem sich das Reisebüro geweigert hatte, das Lösegeld zu zahlen, veröffentlichte LockBit etwa 7.000 bis 10.000 Fotokopien von Reisepässen im Dark Web. Diese Dokumente stammten von Kunden, die an Gruppenreisen teilnahmen, was etwa 2 % des Kundenstamms des Reisebüros ausmachte. Lockbit arbeitet mit einem RaaS-Modell (Ransomware as a Service). Die TTPs des Unternehmens finden Sie im Anhang.

(Weitere Informationen zu TTPs und IOCs auf der Grundlage einzelner Bedrohungsakteure finden Sie im Anhang).

TOP 10 KRITISCHSTE TTPS IN DIESEM SEKTOR

Die nachstehenden TTPs wurden aufgrund ihrer Auswirkungen, ihrer Häufigkeit in realen Vorfällen und ihrer Schwierigkeit, sie zu erkennen oder zu entschärfen, als schwerwiegend eingestuft.

T1078	**Valid Accounts** Used for persistence and evasion by almost all major actors
T1190	**Exploit Public-Facing Application** Common initial access point (e.g., Citrix, VPN flaws)
T1059	**Command and Scripting Interprete** Core execution method (Bash, PowerShell, etc.)
T1566	**Phishing** Widely used by both ransomware and APT actors for initial access
T1027	**Obfuscated Files or Information** Key defense evasion technique used to avoid detection
T1055	**Process Injection** Critical for evading AV/EDR and escalating privileges
T1003.003	**LSASS Memory Dumping** Credential harvesting, crucial for lateral movement
T1021.001	**Remote Desktop Protocol (RDP)** Popular for lateral movement and post-exploitation
T1112	**Modify Registry** Used to disable protections, establish persistence
T1486	**Data Encrypted for Impact** Core ransomware activity-file encryption and extortion

Figure 3: List of Top 10 TTPs associated with Tour Operations and Travel Sector

TRENDPRÄDIKATIONEN

Die folgenden Prognosen wurden aus der Analyse der jüngsten Cybervorfälle abgeleitet, die auf den Reisesektor und die Geschäftsabläufe von Reiseunternehmen abzielten, darunter DDoS-Angriffe, falsch konfigurierter Cloud-Speicher, Social Engineering und Ransomware.

Jede Vorhersage konzentriert sich auf bestimmte Angriffsvektoren, die bei Vorfällen zwischen 2023 und 2025 beobachtet wurden, und prognostiziert, wie sich diese Bedrohungen in Zukunft entwickeln und auf Reiseunternehmen und -betriebe auswirken könnten.

1 ZUNAHME VON DDOS-ANGRIFFEN AUF BUCHUNGS- UND FAHRKARTENSYSTEME

Die vorfälle bei the ticketing company (märz 2025) und asian airlines (dezember 2024) verdeutlichen, dass es sich um kritische angriffe handelte, bei denen ddos-kampagnen wichtige buchungs- und ticketingsysteme störten, was zu betriebsverzögerungen und kundenunzufriedenheit führte. Bei diesen angriffen wurde die abhängigkeit der reisebranche von echtzeit-online-plattformen/systemen ausgenutzt.

In zukunft werden bedrohungsakteure wahrscheinlich weiterhin ddos-angriffe durchführen, um buchungssysteme oder ticketverkaufsplattformen von fluggesellschaften zu überwältigen, mit dem ziel, die hauptreisezeiten (z. B. Ferienzeiten) zu stören. Zusätzlich zu den zunehmenden geopolitischen spannungen werden cyberangriffe mit staatlicher unterstützung wahrscheinlich häufiger und raffinierter werden, um kritische infrastrukturen und finanzsysteme zu stören und volkswirtschaften zu destabilisieren.

Die angreifer werden wahrscheinlich botnets nutzen, die durch ki-gesteuerte datenverkehrsverstärkung verbessert werden, um herkömmliche ddos-abwehrmaßnahmen zu umgehen. In der luftfahrt gehen rund ein viertel der vorfälle auf schwachstellen von anbietern zurück, was den angreifern die möglichkeit bietet, den datenverkehr mithilfe von ki-gesteuerten botnetzen zu verstärken. Kleinere Reisebüros mit begrenzten Budgets für Cybersicherheit könnten besonders anfällig sein und mit Ausfallzeiten und Umsatzeinbußen rechnen.

Sollte sich dieser Trend fortsetzen, könnte es zu einer Zunahme von Erpressungsversuchen kommen, bei denen Angreifer Lösegeld fordern, um DDoS-Kampagnen zu stoppen, und so den Bedarf des Sektors an ununterbrochenen Diensten ausnutzen. Diese Taktik wurde in einem anderen Sektor bei einem Ransomware-Angriff auf das Gesundheitswesen im Jahr 2024 beobachtet, bei dem BlackCat/ALPHV Millionenbeträge für die Wiederherstellung kritischer Systeme verlangte, was die Rentabilität von Angriffen auf zeitkritische Vorgänge verdeutlicht. Dies würde letztlich dazu führen, dass der Sektor in cloudbasierten DDoS-Schutz investieren, die Sicherheit der Anbieter prüfen und die Buchungsplattformen Stresstests unterziehen müsste. protection, audit vendor security, and stress-test booking platforms.

2 MEHR DATENSCHUTZVERLETZUNGEN DURCH FALSCH KONFIGURIERTEN CLOUD-SPEICHER

Im jahr 2025 kam es bei einem australischen reiseunternehmen zu einer schwerwiegenden datenverletzung, als ein cloud-speicher-bucket auf aws ohne passwort öffentlich zugänglich gemacht wurde. Infolgedessen wurden über 112.000 kundendatensätze offengelegt, darunter eingescannte reisepässe und teilweise kreditkartennummern. Dieser vorfall verdeutlicht eine grosse schwachstelle, die die gesamte reise- und tourismusbranche betrifft: falsch konfigurierte cloud-speichersysteme.

Bedrohungsakteure automatisieren zunehmend die Entdeckung und Ausnutzung von falsch konfiguriertem Cloud-Speicher - insbesondere auf Plattformen wie AWS und Azure. Tools wie Bucket Finder, S3Scanner und Suchmaschinen wie Shodan und Censys ermöglichen es Angreifern, öffentlich zugängliche Buckets leicht zu finden. Sobald sie identifiziert sind, werden übermäßig freizügige Berechtigungen (z. B. READ, LIST oder WRITE) ausgenutzt, um anonym auf gespeicherte Daten zuzugreifen oder sie zu verändern. Angreifer setzen dann schlüsselwortbasierte Skripte mit AWS CLI oder boto3 ein, um nach sensiblen Dateien wie .env, passwords.txt oder db_backup.sql zu suchen. Wenn HTTPS nicht erzwungen wird, können die Daten sogar über unverschlüsselte Kanäle exfiltriert werden.

Da die Reise- und Tourismusbranche weiterhin auf Cloud-Infrastrukturen umsteigt, insbesondere bei kleinen bis mittelgroßen Anbietern, denen es an robusten Cybersicherheitskontrollen mangelt, wird falsch konfigurierter Cloud-Speicher eine der am häufigsten ausgenutzten Schwachstellen bleiben. Der Einsatz von automatisierten Scanning-Tools und KI-gesteuerten Suchtaktiken wird weiter zunehmen, so dass Angreifer wertvolle Daten in großem Umfang identifizieren und extrahieren können. Es ist zu erwarten, dass gezielte Erpressungen und auf Datenlecks basierender Betrug zunehmen werden. Dies wird die Aufsichtsbehörden dazu veranlassen, die Compliance-Standards zu verschärfen und die Unternehmen dazu zwingen, kontinuierliche Konfigurationsprüfungen, strenge Zugangskontrollen und End-to-End-Verschlüsselungsrichtlinien einzuführen.

3 PHISHING-KAMPAGNEN, DIE DIE ANMELDEDATEN VON MITARBEITERN AUSNUTZEN

Der Angriff auf das US-Resort (2023) zeigte ein zunehmendes Bedrohungsmuster: Phishing- und Imitationsangriffe werden als Einstiegspunkt für die Kompromittierung interner Systeme genutzt. Der Bedrohungsakteur Scattered Spider gab sich erfolgreich als Mitarbeiter aus, nachdem er LinkedIn-Profile recherchiert, IT-Helpdesk-Mitarbeiter zur Herausgabe von Anmeldedaten überredet und Ransomware installiert hatte, die betriebliche Systeme lahmlegte.

Im Jahr 2025 ist mit einer Zunahme von KI-gestützten Phishing-Kampagnen zu rechnen, die speziell auf Mitarbeiter von Reisebüros, Fluggesellschaften und Flughafenbetreibern abzielen. Dies ist besonders kritisch, da sich über 70 % der Angriffe im Luftfahrtsektor auf den Diebstahl von Anmeldedaten und den unbefugten Zugriff auf die IT-Infrastruktur konzentrieren. Die Angreifer verwenden KI-generierte E-Mails, die sich als vertrauenswürdige Anbieter oder Führungskräfte ausgeben, wie im Fall des Resorts, um Mitarbeiter dazu zu bringen, Zugang zu Systemen wie Reservierungsplattformen oder Zahlungsgateways zu gewähren. Die hohe Mitarbeiterfluktuation in der Reisebranche und der Trend zur Telearbeit werden die Anfälligkeit erhöhen. Möglicherweise werden vermehrt doppelte Erpressungstaktiken angewandt, bei denen gestohlene Kundendaten (z. B. Reisepässe, Kreditkarten) durchsickern, wenn kein Lösegeld gezahlt wird, wie dies beim Angriff auf das Reisebüro LockBit der Fall war.

Phishing-Angriffe sind seit langem eine beliebte Taktik von Cyberkriminellen, und mit der Integration von generativer KI werden diese Angriffe in Zukunft noch ausgefeilter werden. Angreifer werden KI nutzen, um hochgradig personalisierte Phishing-E-Mails, -Texte oder -Nachrichten in sozialen Medien zu erstellen, die durch die Analyse öffentlich verfügbarer Daten auf einzelne Ziele zugeschnitten sind. Darüber hinaus werden raffinierte Phishing-Websites zunehmend durch KI-gesteuerte Chatbots ergänzt.

Diese Chatbots imitieren das Support-Personal mit einer menschenähnlichen Sprache, ähnlichen Tippgeschwindigkeiten und dynamischer Inhaltsgenerierung, was es schwierig macht, ihre Authentizität zu erkennen. Neuere KI-Sprachmodelle ermöglichen zudem eine äußerst überzeugende Sprachimitation. Diese Fähigkeit bietet Kriminellen weitere Social-Engineering-Möglichkeiten durch Phishing-Anrufe, bei denen sie sich als Support-Mitarbeiter, Bankangestellte und andere maßgebliche Personen ausgeben können, um Zugang zu privaten Informationen oder Systemen zu erhalten. Darüber hinaus bieten diese KI-Tools auch nicht-englischsprachigen Bedrohungsakteuren die Möglichkeit, US-Personal mit höheren Erfolgschancen anzugreifen.

4 ANGRIFFE AUF DIE LIEFERKETTE ÜBER DRITTANBIETER

Der Angriff auf eine europäische Fluggesellschaft (2024) erfolgte wahrscheinlich durch Web-Skimming über ein kompromittiertes Zahlungssystem, wobei Kreditkartendaten und persönliche Informationen preisgegeben wurden. Auch der Angriff auf einen US-Flughafen (2024) zeigte die Schwachstellen in den Systemen von Drittanbietern auf, wobei sich Rhysida-Mitglieder Zugang zu den Daten von Mitarbeitern und Auftragnehmern verschafften. Diese Vorfälle spiegeln einen breiteren Trend wider: die Ausnutzung von öffentlich zugänglichen Anwendungen (T1190) und Schwachstellen in der Lieferkette, durch die hochwertige Systeme im Reisesektor gefährdet werden.

Angesichts der zunehmenden Abhängigkeit von Cloud-Diensten und Ökosystemen mit mehreren Anbietern werden Angreifer wahrscheinlich weiterhin die schwächsten Glieder der digitalen Lieferketten ausnutzen. Im Jahr 2025 könnten Angriffe auf die Lieferkette, die auf Drittanbieter wie Zahlungsabwickler, Buchungsplattformen und Identitätsprüfungsdienste abzielen, eskalieren. Die Angreifer könnten sich darauf konzentrieren, kleinere, weniger sichere Anbieter zu infiltrieren, um größere Reiseunternehmen zu kompromittieren. Nach dem Eindringen erbeuten die Angreifer häufig Eingabedaten (T1056), extrahieren sensible Kunden- oder Finanzdaten aus internen Systemen und Repositories (T1213) und schleusen sie über vertrauenswürdige Webdienste oder Cloud-Plattformen (T1048.003) ein, wodurch sie sich der herkömmlichen Sicherheitserkennung entziehen können.

Diese Angriffe haben das Potenzial, zu einer groß angelegten Datenexfiltration, Finanzbetrug und Betriebsunterbrechungen zu führen, insbesondere für Unternehmen, die sich auf veraltete Herstellersoftware verlassen, was die Anfälligkeit für Zero-Day-Schwachstellen erhöht. Es wird erwartet, dass Bedrohungsakteure auch weiterhin opportunistisch auf Unternehmen mit schwachen Abwehrmechanismen in der Lieferkette abzielen und die mangelnde Kontrolle der Unternehmen über ihre Drittanbieter ausnutzen werden.

Die Europäische Agentur für Netz- und Informationssicherheit (ENISA) hat die Risiken in der Lieferkette als wachsendes Problem bezeichnet und auf ihre Heimlichkeit, Komplexität und weitreichenden Folgen hingewiesen. Viele Organisationen in allen Branchen sind auf diese Bedrohungen nicht ausreichend vorbereitet. Die Reisebranche ist aufgrund ihrer starken Abhängigkeit von Cloud-Plattformen und komplizierten Anbieter-Ökosystemen besonders anfällig.

Darüber hinaus setzen 2024 immer mehr Unternehmen KI-Großsprachenmodelle (Large-Language Models, LLMs) ein, und es wird erwartet, dass im Laufe des Jahres 2025 weitere hinzukommen werden. Bedrohungsakteure sind sich dieses neuen Trends bewusst und versuchen, ihn auszunutzen, indem sie Datenvergiftungsangriffe auf Trainingsmodelle durchführen, auf denen LLMs basieren.

CYBERINT, NOW A CHECK POINT COMPANY SOLUTIONS

In Anbetracht der jüngsten Bedrohungstrends ist es wichtig, die verschiedenen Dienstleistungen zu verstehen, die Cyberint zum Schutz vor diesen Risiken anbietet.

Cyberint, jetzt ein Unternehmen von Check Point, überwacht verschiedene Assets, darunter Domains, E-Mails, externe IP-Adressen, hochrangige Mitarbeiter und mehr. Jedes Asset wird sorgfältig konfiguriert, um den entscheidenden Anforderungen gerecht zu werden, mit denen die Sicherheitsteams das ganze Jahr über konfrontiert sind.

Diese Assets werden täglich in der Cyberint-Lösung durch Automatisierung der Angriffsflächenüberwachung (ASM), Sammlung von Bedrohungsdaten, Phishing-Erkennung und engagierte Zusammenarbeit mit Analysten überwacht.

ÜBERWACHUNG DER ANGRIFFSFLÄCHE

Das Modul Attack Surface Monitoring der Cyberint-Lösung führt tägliche und wöchentliche nicht-intrusive Scans der folgenden Kategorien von Assets durch:

- **Domänen**
- **Subdomänen**
- **IP-Adressen**
- **Azure Data Lake / Speicherblöcke**
- **Google Cloud-Speicher**
- **Amazon S3 Buckets**

Automatisierte tägliche Scans überwachen kontinuierlich anfällige Technologien, Fehlkonfigurationen, ausnutzbare oder offene Ports und andere potenzielle Schwachstellen. Wenn ein Problem erkannt wird, wird automatisch eine Warnung generiert und an das Warnmodul gesendet, wo das Team die Situation überprüfen und die entsprechenden nächsten Schritte festlegen kann.

Dieser tägliche Scan ist für die Überwachung potenzieller Schwachstellen bei externen Ressourcen, insbesondere Amazon S3-Buckets, unerlässlich, da er in direktem Zusammenhang mit dem Aerticket-Cyberangriff steht, bei dem Bedrohungsakteure auf einen falsch konfigurierten Cloud-Speicher-Bucket zugriffen.

Das Modul Attack Surface Monitoring (ASM) bietet durch tägliche und wöchentliche, nicht-intrusive Scans einen kontinuierlichen Einblick in ein breites Spektrum digitaler Assets. Es identifiziert Schwachstellen, Fehlkonfigurationen und exponierte Dienste über Domänen, IPs und Cloud-Speicher hinweg und nutzt dabei öffentliche Daten und optionale Cloud-Integrationen, um zugehörige Assets aufzudecken, die möglicherweise nicht direkt bereitgestellt werden.

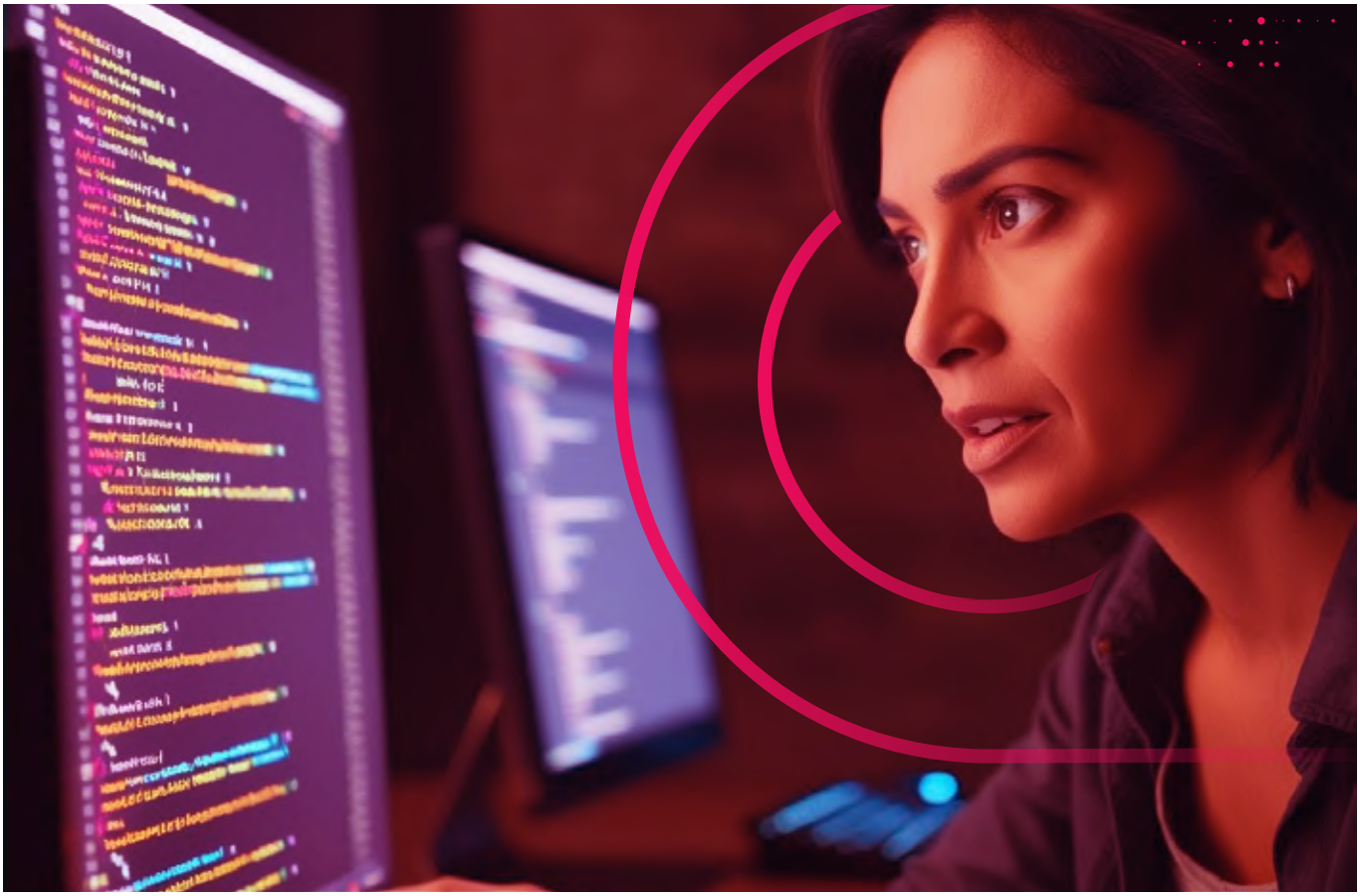
Dieser umfassende Ansatz stellt sicher, dass Unternehmen ihre externe Gefährdung im Auge behalten und rechtzeitig Maßnahmen zur Behebung von Problemen ergreifen können.

ÜBERWACHUNG VON BEDROHUNGSDATEN

Phishing-Erkennung

Im Rahmen des Phishing-Schutzes von Cyberint können zentrale Domain-Assets sowohl für Threat Intelligence als auch für Attack Surface Monitoring markiert werden, was eine automatische Erkennung von verdächtigen Lookalike-Domains ermöglicht.

Um die Automatisierung zu ergänzen, identifiziert Cyberint, jetzt ein Check Point-Unternehmen, Phishing Beacon proaktiv Phishing-Seiten, indem es ein nicht-intrusives Skript in die geschützte Website einbettet. Es alarmiert uns, wenn böswillige Akteure versuchen, dieselbe Website auf nicht autorisierten Domains zu klonen.



Jagd auf Bedrohungen

Die Überwachung von Bedrohungsdaten wird durch die strategische Festlegung von Schlüsselressourcen verstärkt. Sobald diese Anlagen identifiziert sind, werden sie kontinuierlich über eine breite Palette von Informationsquellen, einschließlich Untergrundforen, Code-Repositories und soziale Medien, überwacht, um potenzielle Risiken aufzudecken. Der zuständige Analyst überprüft die gesammelten Informationen täglich und informiert die zuständigen Sicherheitsteams über alle relevanten Bedrohungen.
Darüber hinaus konsumiert das Analystenteam von Cyberint, jetzt ein Unternehmen von Check Point, ständig eine Vielzahl von Berichten, die es uns ermöglichen, uns kontinuierlich an die sich ständig verändernde Bedrohungslandschaft in bestimmten Branchen anzupassen und Empfehlungen zu Best Practices zu geben, um aufkommende Bedrohungen zu entschärfen.

Supply Chain Monitoring

Darüber hinaus ist die Überwachung der Lieferkette ein Service, den Cyberint, jetzt ein Unternehmen von Check Point, anbietet und der es ermöglicht, bestimmte Drittanbieter, die von der Kundenorganisation genutzt werden, kontinuierlich zu überwachen und, wenn sie entdeckt werden, entsprechende Warnungen zu automatisieren:

- Erwähnung von Namen von Supply Chain Vendoren in Darknet-Foren
- Erwähnung von Namen von Supply Chain-Anbietern bei Sicherheitsverletzungen
- Ein Anbieter, der von einem laufenden Ransomware-Angriff betroffen ist
- Aufkommende Phishing-Kampagne, die sich auf den Supply Chain Vendor bezieht
- Quellcode eines Anbieters für die Lieferkette wurde veröffentlicht
- Anbieter der Lieferkette wird zum Verkauf angeboten

Die kontinuierliche Überwachung von Drittanbietern ist unerlässlich, da ihre Systeme und Sicherheitspraktiken direkte Auswirkungen auf die Risikoexposition des Unternehmens haben können.

Diese Überwachung ist sowohl für aktuelle als auch für neu entstehende Cyber-Bedrohungslandschaften von großer Bedeutung, da Bedrohungsakteure zunehmend auf Anbieter in der Lieferkette abzielen, um in größere Unternehmen einzudringen. Durch die proaktive Identifizierung von Schwachstellen, Verstößen oder verdächtigen Aktivitäten innerhalb des Ökosystems des Anbieters kann man schnell auf potenzielle Bedrohungen reagieren und nachgelagerte Folgen für die Unternehmensumgebung verhindern.

Die Kombination aus der Sammlung umfassender Informationen und der kontinuierlichen Überwachung und Analyse durch einen engagierten Analysten trägt zu einem besseren Verständnis der externen Bedrohungslandschaft des Unternehmens bei.

SPEZIELLE ANALYSTENDIENSTE

Der Analyst bietet neben der täglichen Überwachung von Bedrohungen und der Alarmierung viele weitere Dienste an. Der engagierte Analyst gilt als Experte für die Cyberint-Lösung, der die Nutzung der Plattform maximieren und sicherstellen soll, dass alle Module effizient und wie vorgesehen laufen.

Zu den Aufgaben der Analysten, die für die laufende Feinabstimmung der Lösung sorgen, gehören

- **Asset-Konfiguration -** Der Analyst stellt sicher, dass jedes erhaltene Asset so konfiguriert ist, dass es den Anforderungen des Kunden entspricht.

- **Asset-Aktualisierung -** Der Analyst fordert schrittweise Aktualisierungen an, um eine aktuelle Abdeckung zu gewährleisten.

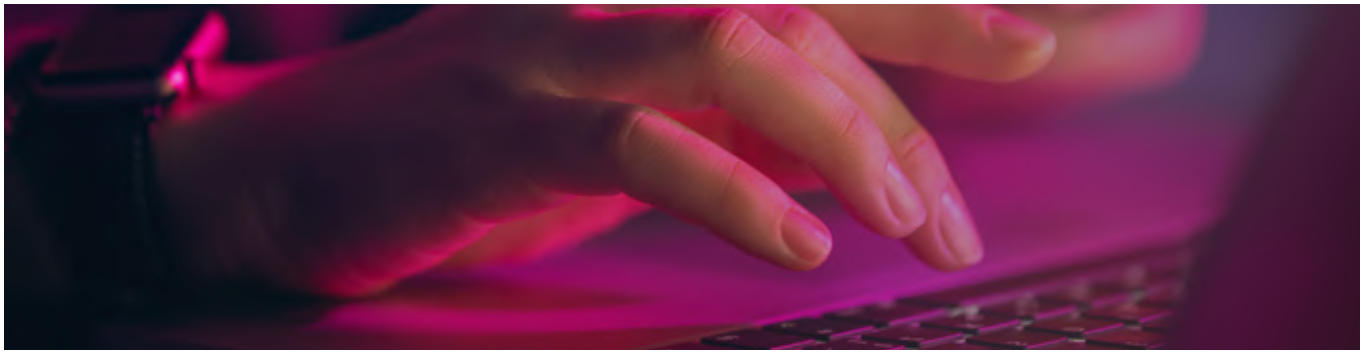
- **Überwachung der Umgebungsmetriken -** Die Analysten überwachen die Automatisierung und die Warnmeldungen, um Vorschläge zu machen, wie die Umgebung an die Bedürfnisse des Kunden angepasst werden kann.

- **Alarmkonfiguration -** Die Analysten überprüfen die Alarmierung, z. B. die Gründe für die Schließung und das Kundenfeedback, um Vorschläge für die Alarmkonfiguration zu machen (z. B. Deaktivierungen, Überschreiten des Schweregrads, Abstimmung der Kennwortrichtlinien des Unternehmens).

Die Aufgabe des Analysten besteht darin, Experte für die Plattform zu sein, aber auch in gewissem Maße als kooperatives Teammitglied zu fungieren. Der Analyst bietet auf Anfrage Schulungen an, um sicherzustellen, dass das Kundenteam mit der Lösung und all ihren Funktionen vertraut ist, unabhängig davon, ob der Kunde neu einsteigt oder nur einen Auffrischungskurs für die ständig aktualisierte Lösung wünscht.

Der engagierte Analyst hält außerdem regelmäßig - in der Regel monatlich - Meetings ab, in denen er die wichtigsten Warnungen und Diskussionspunkte vorstellt, um den Kunden einen klaren Einblick in die wichtigsten Erkenntnisse und den Gesamtwert der laufenden Bemühungen des Analysten zu geben.

Im Laufe der Zeit sehen die Analysten die gesammelten Rohdaten und werden zu Experten, die auf die Informationsanforderungen und die Strategie des Kunden zugeschnitten sind. Mit diesem Fachwissen können sie in strategischen Gesprächen, wie z. B. einem Priority Requirement Alignment (PIR), um die Übereinstimmung mit den strategischen Zielen des Unternehmens zu gewährleisten, oder in vierteljährlichen Geschäftsbesprechungen (Quarterly Business Review, QBR) weitere Intelligence-Vorschläge machen.



SCHLUSSFOLGERUNGEN UND EMPFEHLUNGEN

SCHLUSSFOLGERUNGEN

Die Reisebranche sieht sich mit einer sich entwickelnden externen Bedrohungslandschaft konfrontiert, die durch verstärkte DDoS-Angriffe, Phishing-Kampagnen, Cloud-Fehlkonfigurationen und Kompromittierungen der Lieferkette vorangetrieben wird. In dem Maße, wie sich die Angreifer anpassen, müssen auch die Verteidigungsstrategien der Reiseunternehmen angepasst werden, insbesondere in Bezug darauf, wie sie Bedrohungen außerhalb ihrer internen Grenzen verstehen und darauf reagieren.

Als wichtiger Partner für die Überwachung externer Bedrohungen ist Cyberint, jetzt ein Check Point Unternehmen, in der Lage, eine entscheidende Rolle bei der Stärkung der Cyber-Resilienz zu spielen, indem es zeitnahe, relevante und umsetzbare Erkenntnisse liefert.

Durch die Kombination von Echtzeit-Informationserfassung, Einblick in externe Angriffsflächen und analystengestützten Erkenntnissen hilft Cyberint, jetzt ein Check Point Unternehmen, Cyber-Bedrohungen zu antizipieren und zu entschärfen, bevor sie den Betrieb beeinträchtigen. In einem so zeitkritischen und kundenorientierten Sektor wie der Reisebranche ist ein Partner, der sich auf das konzentriert, was jenseits der Firewall des Unternehmens passiert, nicht länger optional, sondern unverzichtbar.

EMPFEHLUNGEN

Aufgrund der jüngsten Cyberangriffe auf die Reisebranche empfiehlt Cyberint, jetzt ein Unternehmen von Check Point, Folgendes:

1 VERTEIDIGUNG GEGEN DDOS-ANGRIFFE AUF BUCHUNGS- UND TICKETINGSYSTEME

Da wir eine Zunahme von KI-gesteuerten DDoS-Angriffen auf kritische Reiseplattformen in Zeiten hohen Verkehrsaufkommens erwarten, lauten unsere Empfehlungen wie folgt:

- Nutzen Sie Cyberint, um in Untergrundforen, Telegram-Kanälen und Botnet-Märkten, in denen DDoS-Kampagnen geplant oder beworben werden, auf Chatter im Vorfeld von Angriffen zu achten.
- Verfolgen Sie Erwähnungen Ihrer Kernplattformen und digitalen Infrastruktur, um Frühwarnzeichen für potenzielle Angriffe zu erkennen.
- Implementieren Sie DDoS-Präventionsmechanismen: Setzen Sie Cloud-basierten DDoS-Schutz ein, prüfen Sie die Sicherheit von Anbietern und führen Sie Stresstests für Buchungsplattformen durch.

2 VERHINDERUNG VON DATENVERSTÖSSEN DURCH FALSCH KONFIGURIERTEN CLOUD-SPEICHER

Cyberint, jetzt ein Unternehmen von Check Point, rechnet mit einer zunehmenden Ausnutzung offener Cloud-Buckets, die zu sensiblen Datenlecks in diesem Sektor führen. Unsere Empfehlungen lauten daher wie folgt:

- Verwenden Sie Cyberint, um in Foren für Sicherheitsverletzungen, auf Paste-Sites und in durchsuchbaren Repositories nach offenen Daten zu suchen, die mit Ihrer Marke oder Ihren Kunden in Verbindung stehen.
- Setzen Sie Cyberint ein, um die Überwachung auf konfigurationsbezogene Lecks durchzusetzen, z. B. .env-, .bak- oder Backup-Dateien, die in Dumps von Bedrohungsakteuren oder öffentlichen Buckets entdeckt werden.
- Nutzen Sie die ASM-Erkennung (Attack Surface Monitoring) von Cyberint, um kontinuierlich nach neu aufgedeckten Cloud-Assets, falsch konfiguriertem Speicher und nicht autorisierten Änderungen an Ihrem Cloud-Footprint zu suchen.

3 ENTSCHÄRFUNG VON KI-GESTÜTZTEM PHISHING UND AUSLESEN VON ZUGANGSDATEN

Cyberint, jetzt ein Unternehmen von Check Point, rechnet mit einer Zunahme von raffiniertem Phishing, das generative KI und Imitationen nutzt und auf Mitarbeiter des Sektors abzielt. Unsere Empfehlungen lauten daher wie folgt:

- Verstärken Sie die Überwachung auf Imitationen Ihrer Marke, Ihrer Führungskräfte oder Ihrer Kundensupport-Teams über soziale Medien, Domainregistrierungen und Phishing-Kits. Cyberint, jetzt ein Check Point-Unternehmen, bietet diesen Service an.
- Frühzeitige Überwachung der Phishing-Infrastruktur durch ähnlich aussehende Domains und geklonte Websites mit unserer Phishing-Erkennung. Cyberint, jetzt ein Unternehmen von Check Point, bietet diesen Service an.

4 ÜBERWACHUNG DES RISIKOS VON DRITTANBIETERN UND AUSNUTZUNG DER LIEFERKETTE

Cyberint, jetzt ein Check Point-Unternehmen, rechnet mit zunehmenden Angriffen durch anfällige Anbieter, Zahlungsplattformen und veraltete Tools von Drittanbietern. Daher lauten unsere Empfehlungen wie folgt:

- Überwachen Sie das Ökosystem von Anbietern kontinuierlich auf Indikatoren für eine Gefährdung, auf durchgesickerte Anmeldeinformationen oder auf Daten, die über Verbindungen von Drittanbietern an Ihr Unternehmen gelangen. Cyberint, jetzt ein Check Point-Unternehmen, bietet eine Lösung zur Überwachung von Drittanbietern.
- Verfolgen Sie branchenspezifische Verletzungen der Lieferkette und stellen Sie kontextbezogene Bedrohungsdaten bereit, um festzustellen, ob Ihre Umgebung indirekt betroffen ist.
- IOCs blockieren: Um Ihre internen Systeme zu schützen, empfehlen wir Ihnen, die bereitgestellte IOC-Liste in Ihre Endpunktschutzplattform zu importieren und sie so zu konfigurieren, dass alle passenden Bedrohungen blockiert oder unter Quarantäne gestellt werden. Wenden Sie außerdem die IPs und Domänen auf Ihre internen DNS- oder hostbasierten Firewall-Richtlinien an, um die Kommunikation mit bekannten bösartigen Infrastrukturen zu verhindern. Die IOC-Liste finden Sie auf den Seiten 20-27.

APPENDIX

KONSOLIDIERTE TTP-LISTE

Technique ID	Technique Name
T1003.003	Security Account Manager (SAM)
T1005	Data from Local System
T1012	Query Registry
T1016	System Network Configuration Discovery
T1018	Remote System Discovery
T1021	Remote Services
T1021.001	Remote Desktop Protocol
T1021.002	SMB/Windows Admin Shares
T1021.004	SSH
T1027	Obfuscated Files or Information
T1033	System Owner/User Discovery
T1047	Windows Management Instrumentation
T1048.003	Exfiltration Over Alternative Protocol: SMB/Windows Admin Shares
T1055	Process Injection
T1055.002	Portable Executable Injection
T1056	Input Capture
T1056.004	Credential API Hooking
T1057	Process Discovery
T1059	Command and Scripting Interpreter
T1059.001	PowerShell
T1059.003	Windows Command Shell
T1069.001	Permission Groups Discovery: Local Groups
T1069.002	Permission Groups Discovery: Global Groups
T1070.001	Indicator Removal from Tools: File Deletion
T1070.004	Indicator Removal from Tools: File System Metadata Deletion
T1071	Application Layer Protocol
T1078	Valid Accounts
T1087.002	T1087.002

Technique ID	Technique Name
T1110	Brute Force
T1112	Modify Registry
T1190	Exploit Public-Facing Application
T1210	Exploitation for Privilege Escalation
T1213	Data from Information Repositories
T1219	Remote Access Tools
T1482	Domain Trust Discovery
T1486	Data Encrypted for Impact
T1497	Virtualization/Sandbox Evasion
T1530	Data from Cloud Storage Object
T1547.001	Boot or Logon Autostart Execution: Registry Run Keys / Startup Folder
T1548	Abuse Elevation Control Mechanism
T1564.003	Hide Artifacts: Hidden Files and Directories
T1566	Phishing
T1567	Exfiltration Over Web Service
T1567.002	Exfiltration Over Web Service: Web Shell
T1580	Data from Local System
T1587	Acquire Infrastructure
T1589	Gather Victim Identity Information
T1595	Active Scanning
T1596.001	Gather Victim Host Information: System Information Discovery
T1657	Application Layer Protocol: Web Protocols

IOCS NACH BEDROHUNGSAKTEUREN

Rhysida

IOC Type	Technique Name	Hash / Email / IP	Description
C2 IP Address	5.39.222[.]67	N/A	Command and Control Server
C2 IP Address	5.255.99[.]59	N/A	Command and Control Server
C2 IP Address	51.77.102[.]106	N/A	Command and Control Server
C2 IP Address	108.62.118[.]136	N/A	Command and Control Server
C2 IP Address	108.62.141[.]161	N/A	Command and Control Server
C2 IP Address	146.70.104[.]249	N/A	Command and Control Server
C2 IP Address	156.96.62[.]58	N/A	Command and Control Server
C2 IP Address	157.154.194[.]6	N/A	Command and Control Server
Email Address	rhysidaeverywhere@onionmail[.]org	N/A	Email associated with Rhysida
Email Address	rhysidaofficial@onionmail[.]org	N/A	Email associated with Rhysida
SHA256 Hash	48f559e00c472d9ffe3965ab92c6d298f8fb3a3f0d6d203cd2069bfca4bf3a57	Sock5.sh	File used in Rhysida operations
SHA256 Hash	edfae1a69522f87b12c6dac3225d930e4848832e3c551ee1e7d31736bf4525ef	PsExec64.exe	File used in Rhysida operations
SHA256 Hash	078163d5c16f64caa5a14784323fd51451b8c831c73396b967b4e35e6879937b	PsExec.exe	File used in Rhysida operations

IOC Type	Technique Name	Hash / Email / IP	Description
SHA256 Hash	201d8e77ccc2575d910d47042a98648 0b1da28cf0033e7ee726ad9d45ccf4daa	PsGetsid64.exe	File used in Rhysida operations
SHA256 Hash	a48ac157609888471bf8578fb8b2aef6 b0068f7e0742fccf2e0e288b0b2cfdfb	PsGetsid.exe	File used in Rhysida operations
SHA256 Hash	de73b73eeb156f877de61f4a6975d06 759292ed69f31aaf06c9811f3311e03e7	PsInfo64.exe	File used in Rhysida operations
SHA256 Hash	951b1b5fd5cb13cde159cebc7c604655 87e2061363d1d8847ab78b6c4fba7501	PsInfo.exe	File used in Rhysida operations
SHA256 Hash	fdadb6e15c52c41a31e3c22659dd490d 5b616e017d1b1aa6070008ce09ed27ea	PsLoggedon64.exe	File used in Rhysida operations
SHA256 Hash	d689cb1dbd2e4c06cd15e51a6871c406 c595790ddcdcd7dc8d0401c7183720ef	PsLoggedon.exe	File used in Rhysida operations
SHA256 Hash	554f523914cdbaed8b17527170502199 c185bd69a41c81102c50dbb0e5e5a78d	PsService64.exe	File used in Rhysida operations
SHA256 Hash	d3a816fe5d545a80e4639b34b90d92d 1039eb71ef59e6e81b3c0e043a45b751c	PsService.exe	File used in Rhysida operations
SHA256 Hash	8329bcbadc7f81539a4969ca13f0be5b8 eb7652b912324a1926fc9bfb6ec005a	Eula.txt	File used in Rhysida operations
SHA256 Hash	be922312978a53c92a49fefd2c9f9cc09 8767b36f0e4d2e829d24725df65bc21	psfile64.exe	File used in Rhysida operations
SHA256 Hash	4243dc8b991f5f8b3c0f233ca2110a1e0 3a1d716c3f51e88faf1d59b8242d329	psfile.exe	File used in Rhysida operations
SHA256 Hash	7ba47558c99e18c2c6449be804b5e765 c48d3a70ceaa04c1e0fae67ff1d7178d	pskill64.exe	File used in Rhysida operations
SHA256 Hash	5ef168f83b55d2cbd2426afc5e6fa8161 270fa6a2a312831332dc472c95dfa42	pskill.exe	File used in Rhysida operations
SHA256 Hash	d3247f03dcd7b9335344ebba76a0b923 70f32f1cb0e480c734da52db2bd8df60	pslist64.exe	File used in Rhysida operations
SHA256 Hash	ed05f5d462767b3986583188000143f0 eb24f7d89605523a28950e72e6b9039a	pslist.exe	File used in Rhysida operations

IOC Type	Technique Name	Hash / Email / IP	Description
SHA256 Hash	5e55b4caf47a248a10abd009617684e969dbe5c448d087ee8178262aaab68636	psloglist64.exe	File used in Rhysida operations
SHA256 Hash	dcdb9bd39b6014434190a9949dedf633726fdb470e95cc47cdaa47c1964b969f	psloglist.exe	File used in Rhysida operations
SHA256 Hash	8d950068f46a04e77ad6637c680cccf5d703a1828fbd6bdca513268af4f2170f	pspasswd64.exe	File used in Rhysida operations
SHA256 Hash	6ed5d50cf9d07db73eaa92c5405f6b1bf670028c602c605dfa7d4fcb80ef0801	pspasswd.exe	File used in Rhysida operations
SHA256 Hash	d1f718d219930e57794bdadf9dda61406294b0759038cef282f7544b44b92285	psping64.exe	File used in Rhysida operations
SHA256 Hash	355b4a82313074999bd8fa1332b1ed00034e63bd2a0d0367e2622f35d75cf140	psping.exe	File used in Rhysida operations
SHA256 Hash	4226738489c2a67852d51dbf96574f33e44e509bc265b950d495da79bb457400	psshutdown64.exe	File used in Rhysida operations
SHA256 Hash	13fd3ad690c73cf0ad26c6716d4e9d1581b47c22fb7518b1d3bf9cfb8f9e9123	psshutdown.exe	File used in Rhysida operations
SHA256 Hash	4bf8fbb7db583e1aacbf36c5f740d012c8321f221066cc68107031bd8b6bc1ee	pssuspend64.exe	File used in Rhysida operations
SHA256 Hash	95a922e178075fb771066db4ab1bd70c7016f794709d514ab1c7f11500f016cd	pssuspend.exe	File used in Rhysida operations
SHA256 Hash	a9ca77dfe03ce15004157727bb43ba66f00ceb215362c9b3d199f000edaa8d61	PSTools.zip	File used in Rhysida operations
SHA256 Hash	2813b6c07d17d25670163e0f66453b42d2f157bf2e42007806ebc6bb9d114acc	Pstools.chm	File used in Rhysida operations
SHA256 Hash	8e43d1ddbd5c129055528a93f1e3fab0ecdf73a8a7ba9713dc4c3e216d7e5db4	pversion.txt	File used in Rhysida operations

Lockbit

IOC Type	Indicator
C2 IP Address	185.215.229[.]44
C2 IP Address	185.215.229[.]45
C2 IP Address	185.215.229[.]46
C2 IP Address	185.215.229[.]47
C2 IP Address	185.215.229[.]48
Domain Name	lockbit[.]pro
Domain Name	lockbit[.]info
Domain Name	lockbit[.]com
Domain Name	lockbit[.]org
Email Address	lockbit@protonmail[.]com
Email Address	support@lockbit[.]pro
File Name	lockbit.exe
SHA256 Hash	23e742dc0f0ec5953993d8f2e5e4399b21353600042d1b9ef95fc9ad26811d729
File Name	lockbit-ransomware.exe
SHA256 Hash	2d96d8315e46517a6d61f93b774951af41b0621c240fd1a315c458aa77978fd99
File Name	lockbit.txt
SHA256 Hash	ccd9da93ab1c6fc3005b72c8a105ffdeeea0e7c9e5b6ec30a100907bc7fe773cf
File Name	ransom_note.txt
SHA256 Hash	292c2717ed5863497f34ad0715455191e4a567f24ff78870b517c2922dcd58e9
File Name	lockbit_6341d6e5844c8289.exe
SHA256 Hash	f3a1576837ed56bcf79ff486aadf36e78d624853e9409ec1823a6f46fd0143ea
File Name	Salary_Lockheed_Martin_job_opportunities_confidential[.]doc
MD5 Hash	18a352d33c8c01b6a196adce176c5a96
MD5 Hash	9661c01af31a41caef2ccd3b6be06e60
MD5 Hash	3c9e550d41f3de930e678776a6e018ed
MD5 Hash	b354eaf3061b4099aecac523eb5466a3
SHA1 Hash	7e303af8c686a0c98fa87a34de1ffcf08f64a093
SHA1 Hash	e09dae6d33cffd7f6f38b62b71c484e5b12b4b79
SHA1 Hash	a118e1e110e285fb82495defe7d1c570d922ee0d

IOC Type	Indicator
SHA1 Hash	774e4e11015b6ff9f3f79aa43770c057d98fbc24
URL	hxxps://temp[.]sh/AErDa/LockBit_6341D6E5844C8289[.]exe
Registry Key	HKCU\Software\LockBit
Registry Key	HKLM\Software\LockBit
Mutex	LockBitMutex
Process Name	lockbit.exe
Process Name	lockbit-ransomware.exe
File Extension	lockbit
File Extension	lockbit_ransomware

IncRansom

Type	Indicator	Description
File Artifact	.INC	File extension used
File Artifact	INC-README.txt	Ransom note filename
File Artifact	INC-README.html	Alternate ransom note filename
Registry Artifact	C:\source\INC Encryptor\Release\ INC Encryptor.pdb	Debugger path in binary
Wallpaper Change	Desktop wallpaper	Modified to display ransom note
Tool	NetScan.exe	Network scanning
Tool	Advanced IP Scanner	Network discovery
Tool	AnyDesk.exe	Remote desktop access
Tool	TightVNC	Remote desktop access

Type	Indicator	Description
Tool	.PsExec	Remote command execution
Tool	Mimikatz	Credential dumping
Tool	HackTool.Win32.ProcTerminator.A	Process termination
Tool	HackTool.PS1.VeeamCreds.A	Credential dumping from Veeam
Tool	7-Zip	Archiving data
Tool	MEGAsync	Cloud-based exfiltration
Encryption	AES	Encryption algorithm
Encryption	Fast, Medium, Slow	Modes used for data skipping/encryption
Encryption	Shadow Copy Deletion	Deletes Volume Shadow Copies
Email	gansbronz[at]gmail[.]com	Ransomware contact email
Onion URL	lynxblogxstgzsarfyk2pvhdv45igghb4zmthnzmsipzeoduruz3xwqd[.]onion	Dark web leak site
SHA-256	ecbfea3e7869166dd418f15387bc33ce46f2c72168f571071916b5054d7f6e49	Lynx Encryptor
SHA-256	571f5de9dd0d509ed7e5242b9b7473c2b2cbb36ba64d38b32122a0a337d6cf8b	Lynx Encryptor
SHA-256	eaa0e773eb593b0046452f420b6db8a47178c09e6db0fa68f6a2d42c3f48e3bc	Lynx Encryptor

Fancy Bear

IOC Type	Indicator
C2 IP Address	185.215.229[.]44
C2 IP Address	185.215.229[.]45
C2 IP Address	185.215.229[.]46
C2 IP Address	185.215.229[.]47
C2 IP Address	185.215.229[.]48
Domain Name	lockbit[.]pro
Domain Name	lockbit[.]info
Domain Name	lockbit[.]com
Domain Name	lockbit[.]org
Email Address	lockbit@protonmail[.]com
Email Address	support@lockbit[.]pro
File Name	lockbit.exe
SHA256 Hash	23e742dc0f0ec5953993d8f2e5e4399b21353600042d1b9ef95fc9ad26811d729
File Name	lockbit-ransomware.exe
SHA256 Hash	2d96d8315e46517a6d61f93b774951af41b0621c240fd1a315c458aa77978fd99
File Name	lockbit.txt
SHA256 Hash	ccd9da93ab1c6fc3005b72c8a105ffdeeea0e7c9e5b6ec30a100907bc7fe773cf
File Name	ransom_note.txt
SHA256 Hash	292c2717ed5863497f34ad0715455191e4a567f24ff78870b517c2922dcd58e9
File Name	lockbit_6341d6e5844c8289.exe
SHA256 Hash	f3a1576837ed56bcf79ff486aadf36e78d624853e9409ec1823a6f46fd0143ea
File Name	Salary_Lockheed_Martin_job_opportunities_confidential[.]doc
MD5 Hash	18a352d33c8c01b6a196adce176c5a96
MD5 Hash	9661c01af31a41caef2ccd3b6be06e60
MD5 Hash	3c9e550d41f3de930e678776a6e018ed
MD5 Hash	b354eaf3061b4099aecac523eb5466a3
SHA1 Hash	7e303af8c686a0c98fa87a34de1ffcf08f64a093
SHA1 Hash	e09dae6d33cffd7f6f38b62b71c484e5b12b4b79
SHA1 Hash	a118e1e110e285fb82495defe7d1c570d922ee0d

IOC Type	Indicator
SHA1 Hash	774e4e11015b6ff9f3f79aa43770c057d98fbc24
URL	hxxps://temp[.]sh/AErDa/LockBit_6341D6E5844C8289[.]exe
Registry Key	HKCU\Software\LockBit
Registry Key	HKLM\Software\LockBit
Mutex	LockBitMutex
Process Name	lockbit.exe
Process Name	lockbit-ransomware.exe
File Extension	.lockbit
File Extension	.lockbit_ransomware

ALPHV

IOC Type	Value	Description	File Name (if any)
MD5	944153fb9692634d6c70899b83676575	ALPHV Windows Encryptor	7O3cCX9YcHMV2.exe
MD5	341d43d4d5c2e526cadd88ae8da70c1c	Anti Virus Tools Killer	File used in Rhysida operations
MD5	34aac5719824e5f13b80d6fe23cbfa07	CobaltStrike BEACON	LMtool.exe
MD5	eea9ab1f36394769d65909f6ae81834b	CobaltStrike BEACON	Info.exe / ConnectivityDiagnos.exe
MD5	379bf8c60b091974f856f08475a03b04	ALPHV Linux Encryptor	him
MD5	ebca4398e949286cb7f7f6c68c28e838	SimpleHelp Remote Management tool	first.exe
MD5	c04c386b945ccc04627d1a885b500edf	Tunneler Tool	conhost.exe
MD5	824d0e31fd08220a25c06baee1044818	Anti Virus Tools Killer	ibmModule.dll

IOC Type	Value	Description	File Name (if any)
MD5	61804a029e9b1753d58a6bf0274c25a6	MeshCentral Agent	WPEHOSTSVC64.exe
MD5	83deea3b61b6a734e7e4a566dbb6bffa	ScreenConnect & attacker tools installer	deployService.exe
MD5	8738b8637a20fa65c6e64d84d1cfe570	Suspected Proxy Tool	socks32.exe
SHA256	c64300cf8bacc4e42e74715edf3f8c32 87a780c9c0a38b0d9675d01e7e231f16	ALPHV Windows Encryptor	—
SHA256	1f5e4e2c78451623cfbf32cf517a92253 b7abfe0243297c5ddf7dd1448e460d5	Anti Virus Tools Killer	—
SHA256	3670dd4663adca40f168f3450fa9e7e8 4bc1a612d78830004020b73bd40fcd71	CobaltStrike BEACON	—
SHA256	af28b78c64a9effe3de0e5ccc77852742 8953837948d913d64dbd0fa45942021	CobaltStrike BEACON	—
SHA256	bbfe7289de6ab1f374d0bcbeecf31cad 2333b0928ea883ca13b9e733b58e27b1	ALPHV Linux Encryptor	—
SHA256	5d1df950b238825a36fa6204d1a2935a 5fbcfe2a5991a7fc69c74f476df67905	SimpleHelp Remote Management tool	—
SHA256	bd9edc3bf3d45e3cdf5236e8f8cd57a9 5ca3b41f61e4cd5c6c0404a83519058e	Tunneler Tool	—
SHA256	732e24cb5d7ab558effc6dc88854f7560 16352c923ff5155dcb2eece35c19bc0	Anti Virus Tools Killer	—
SHA1	3dd0f674526f30729bced4271e6b7eb0 bb890c52	ALPHV Windows Encryptor	—
SHA1	d6d442e8b3b0aef856ac86391e4a57bc b93c19ad	Anti Virus Tools Killer	—
SHA1	6b52543e4097f7c39cc913d55c0044fcf 673f6fc	CobaltStrike BEACON	—
SHA1	004ba0454feb2c4033ff0bdb2ff67388a f0c41b6	CobaltStrike BEACON	—

IOC Type	Value	Description	File Name (if any)
SHA1	430bd437162d4c60227288fa6a82cde8a5f87100	SimpleHelp Remote Management tool	—
SHA1	1376ac8b5a126bb163423948bd1c7f861b4bfe32	Tunneler Tool	—
SHA1	380f941f8047904607210add4c6da2da8f8cd398	Anti Virus Tools Killer	—
Domain	resources.docusong[.]com	Command and Control Server	—
Domain	Fisa99.screenconnect[.]com	ScreenConnect Remote Access	—
Domain	pcrendal[.]com	Command and Control Server	—
Domain	instance-qqemas-relay[.]screenconnect[.]com	ScreenConnect Remote Access	—
Domain	instance-rbjvws-relay.screenconnect[.]com	ScreenConnect Remote Access	—
IP Address	5.199.168.24	Command and Control Server	—
IP Address	91.92.254.193	SimpleHelp Remote Access	—
IP Address	5.199.168[.]233	IP used by Threat Actor	—
IP Address	92.223.89[.]55	IP used by Threat Actor	—
IP Address	185.195.59[.]218	IP used by Threat Actor	—
IP Address	51.159.103[.]112	IP used by Threat Actor	—
IP Address	45.32.141[.]168	Command and Control Server	—
IP Address	45.77.0[.]92	Command and Control Server	—

Fancy Bear

Type	Indicator	Description
File Extension	.exe	Common malware payload
File Extension	.dll	Common malware payload
File Extension	.ps1	Used in PowerShell scripts for exploitation
Malware Hash	ecbfea3e7869166dd418f15387bc33ce4 6f2c72168f571071916b5054d7f6e49	Known malware sample
Registry Key	HKCU\Software\Microsoft\Windows\ CurrentVersion\Run*	Persistence
Mutex	Global\ScatteredSpiderMutex	Avoid multiple instances
Tool	AnyDesk	Remote desktop access
Tool	ScreenConnect	Remote desktop access
Tool	Mimikatz	Credential dumping
Tool	secretdump	Credential dumping
Tool	PsExec	Remote execution
Tool	7-Zip	File compression and archiving
Tool	MEGAsync	Cloud-based data exfiltration
Encryption	AES	Encryption algorithm
Email	gansbronz[at]gmail[.]com	Ransomware contact
Domain	lynxblog[.]net	Phishing or C2 domain
Domain	transfer[.]sh	Exfiltration hosting service
Domain	linkedinsso[.]com	Phishing domain
Domain	mgmresorts-okta[.]com	Phishing domain
IP	99.25.84[.]9	Observed IP in campaigns
IP	144.76.136[.]153	Observed IP in campaigns
Ransomware	BlackCat/ALPHV	Used by group
Ransomware	RansomHub	Used by group
Ransomware	Qilin	Used by group

EXTERNAL REFERENCES OUTSIDE OF CYBERINT

1. https://blog.netwrix.com/mgm-cyber-attack
2. https://www.reuters.com/technology/cybersecurity/iag-flags-air-europas-customers-personal-data-leak-wsj-reports-2024-03-21/
3. https://apnews.com/article/japan-jal-cyberattack-flights-travel-04fbd4848f3015a77057339a5c90ca32
4. https://apnews.com/article/seattle-airport-cyberattack-ransomware-rhysida-95cd980a9f45112f0fdce488233eec9c
5. https://www.theguardian.com/uk-news/article/2024/sep/02/transport-for-london-dealing-with-cyber-attack
6. https://www.voyageursdumonde.fr/voyage-sur-mesure/Img/institutionnel/info-fi/data/2023/PR_Voyageurs_du_Monde_17.5.2023.pdf
7. https://www.skynews.com.au/australia-news/australian-travel-agency-hit-by-data-breach-leaking-passport-and-travel-details-of-thousands-of-customers/news-story/73072684e13a253e315d326b916280c1
8. https://icsstrive.com/incident/aerticket-suffers-cyberattack-causing-technical-failures/
9. https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-319a
10. https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-075a
11. https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-108
12. https://www.cisa.gov/news-events/cybersecurity-advisories/aa22-110a
13. https://www.sentinelone.com/anthology/inc-ransom/
14. https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-353a

CONTACT US

ISRAEL

Tel: +972-73-226-4555
5 Shlomo Kaplan Street
Tel Aviv 6789159

USA

Tel: 1-800-429-4391
100 Oracle Parkway, Suite 800
Redwood City, CA 94065

SINGAPORE

Tel: +65-6435-1318
78 Shenton Way, #09-01 Tower 1,
Singapore 079120

PHILIPPINES

Tel: +63 2 8465 9200
Unit 2005, 20th Floor, Zuellig Building,
Makati Avenue, corner Paseo de Roxas
Makati City 1223, Metro Manila

UK AND IRELAND

Tel: +44 20 7628 4211
85 London Wall, 4th Floor,
London, EC2M 7AD

JAPAN

Tel: +81-3-6205-8340
Toranomon Kotohira Tower 25F,
1-2-8, Toranomon Minato-ku, Tokyo 105-0001

ÜBER CYBERINT

Cyberint, jetzt ein Unternehmen von Check Point, reduziert Risiken, indem es Unternehmen hilft, externe Cyber-Bedrohungen zu erkennen und zu entschärfen, bevor sie negative Auswirkungen haben. Die Check Point External Risk Management-Lösung bietet eine überragende Transparenz durch die kontinuierliche Erkennung der sich entwickelnden Angriffsoberfläche, kombiniert mit der automatisierten Sammlung und Analyse großer Mengen von Informationen aus dem offenen, tiefen und dunklen Web. Ein Team globaler Cybersecurity-Experten auf militärischem Niveau arbeitet mit den Kunden zusammen, um relevante Bedrohungen schnell zu erkennen, zu untersuchen und zu entschärfen - bevor sie die Chance haben, sich zu größeren Vorfällen zu entwickeln. Globale Kunden, darunter Fortune-500-Unternehmen aus allen wichtigen Branchen, verlassen sich auf Check Point External Risk Management, um sich vor einer Vielzahl externer Risiken zu schützen, darunter Schwachstellen, Fehlkonfigurationen, Phishing, Impersonation-Attacken, Malware-Infektionen, offengelegte Anmeldeinformationen, Datenlecks, Betrug und Risiken durch Dritte.

For more information visit: https://cyberint.com / checkpoint.com/erm