Cyberint
A Check Point Company

PANORAMA DE LAS AMENAZAS PARA EL SECTOR DE VIAJES Y CIRCUITOS TURÍSTICOS

By Josh Puentes, Manasa Pisipati and Ben Johnathan Neeman

May 2025

TABLE OF CONTENTS

RESUMEN EJECUTIVO

Cyberint, ahora una empresa de Check Point, realizó un informe sobre el panorama de las amenazas centrado en el sector de los viajes y las operaciones turísticas. El siguiente informe describe los recientes eventos cibernéticos, las predicciones de amenazas cibernéticas y una visión general de los servicios de Cyberint, ahora una empresa de Check Point, como una solución para mitigar las amenazas digitales.

De 2023 a 2025, el sector mundial de los viajes se enfrentó a un aumento de los ciberataques dirigidos, incluidas las interrupciones DDoS, los incidentes de ransomware, las violaciones de datos a través del almacenamiento en la nube mal configurado y los compromisos de la cadena de suministro de terceros. El informe incluye un resumen de los sucesos ocurridos en todo el mundo. También incluye una lista de las TTP (herramientas y técnicas) destacadas relacionadas con los atacantes y una lista de las IOC relacionadas que deben tenerse en cuenta y bloquearse.

A continuación se presentan las predicciones de tendencias que Cyberint prevé, basándose en los incidentes relacionados:

Ataques DDoS que perturban los sistemas de reservas

Estos ataques suelen coincidir con los periodos punta de los viajes y se aprovechan de la dependencia del sector de los servicios en línea en tiempo real. Se espera que los grupos de actores de amenazas sigan aprovechando las redes de bots para paralizar las operaciones, lo que podría dar lugar a demandas de extorsión para restablecer el servicio

Filtraciones de datos a través de almacenamiento en la nube mal configurado

Los atacantes utilizan cada vez más herramientas avanzadas y secuencias de comandos automatizadas para identificar y extraer datos del almacenamiento en la nube expuesto. Las pequeñas y medianas empresas de viajes sin sólidas prácticas DevSecOps siguen siendo muy vulnerables.

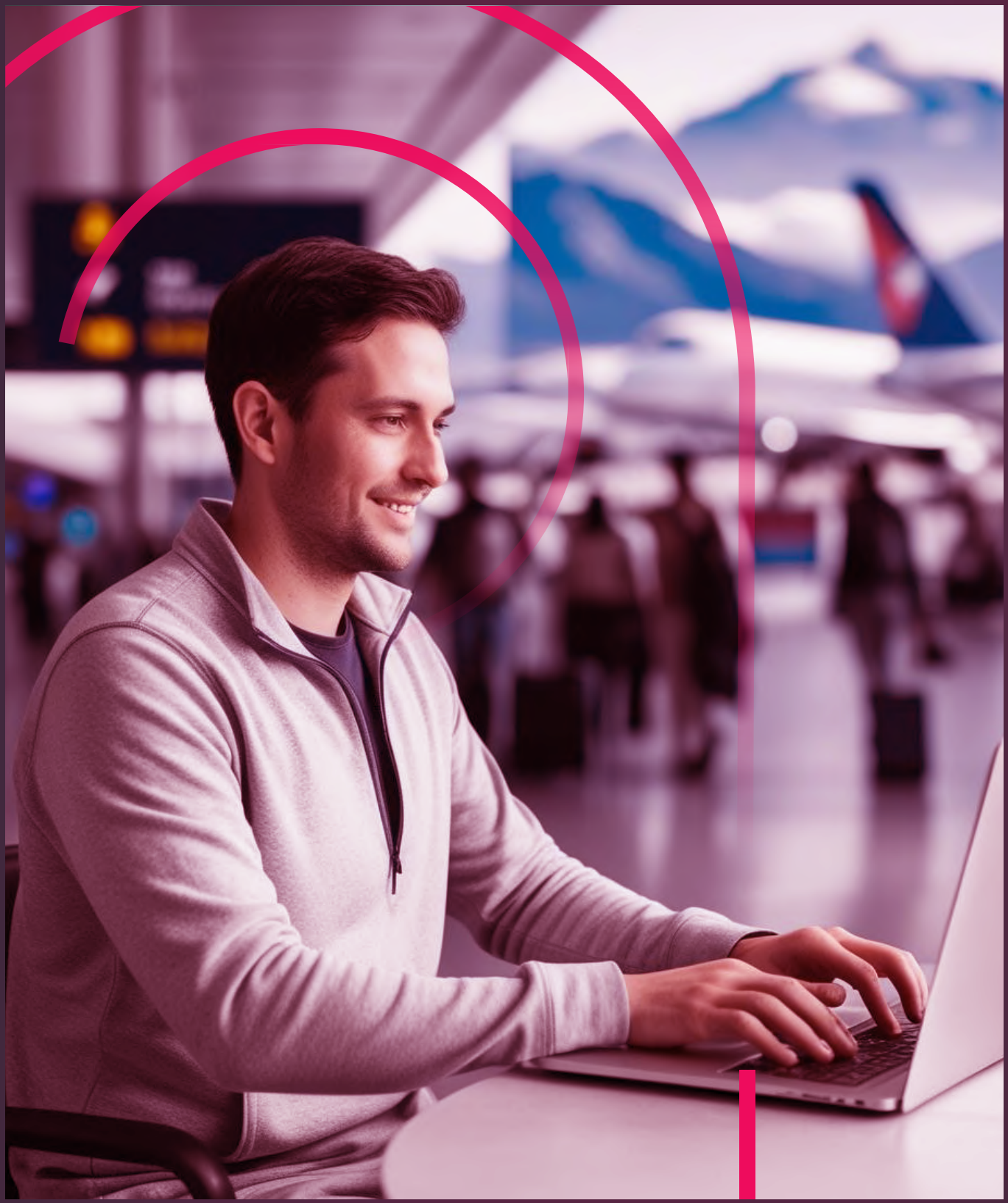
Phishing y Explotación de Credenciales

Los atacantes están utilizando técnicas avanzadas de ingeniería social, incluyendo la suplantación de identidad y señuelos de phishing generados por IA, para obtener las credenciales de los empleados. Estos ataques permiten el despliegue de ransomware, la exfiltración de datos internos y la persistencia del sistema.

Compromiso de la cadena de suministro y riesgos de terceros

Los atacantes están eludiendo los perímetros reforzados dirigiéndose a proveedores de procesamiento de pagos, autenticación e infraestructura en la nube, a menudo aprovechando aplicaciones obsoletas o inseguras para infiltrarse en los sistemas centrales y exfiltrar datos confidenciales.

Para mitigar estas amenazas en evolución, Cyberint proporciona Inteligencia sobre Amenazas (TI) y Supervisión de la Superficie de Ataque (ASM) continuas y adaptadas al entorno de riesgo externo del sector de los viajes. Detectamos indicadores tempranos de compromiso, activos expuestos y actividad de actores de amenazas a través de una supervisión exhaustiva de un amplio conjunto de fuentes. Este enfoque de inteligencia proactiva permite a las organizaciones de viajes anticiparse a las amenazas específicas y minimizar el impacto operativo y en la reputación.



INCIDENTES CIBERNÉTICOS

CRONOLOGÍA DE ACONTECIMIENTOS DESTACADOS

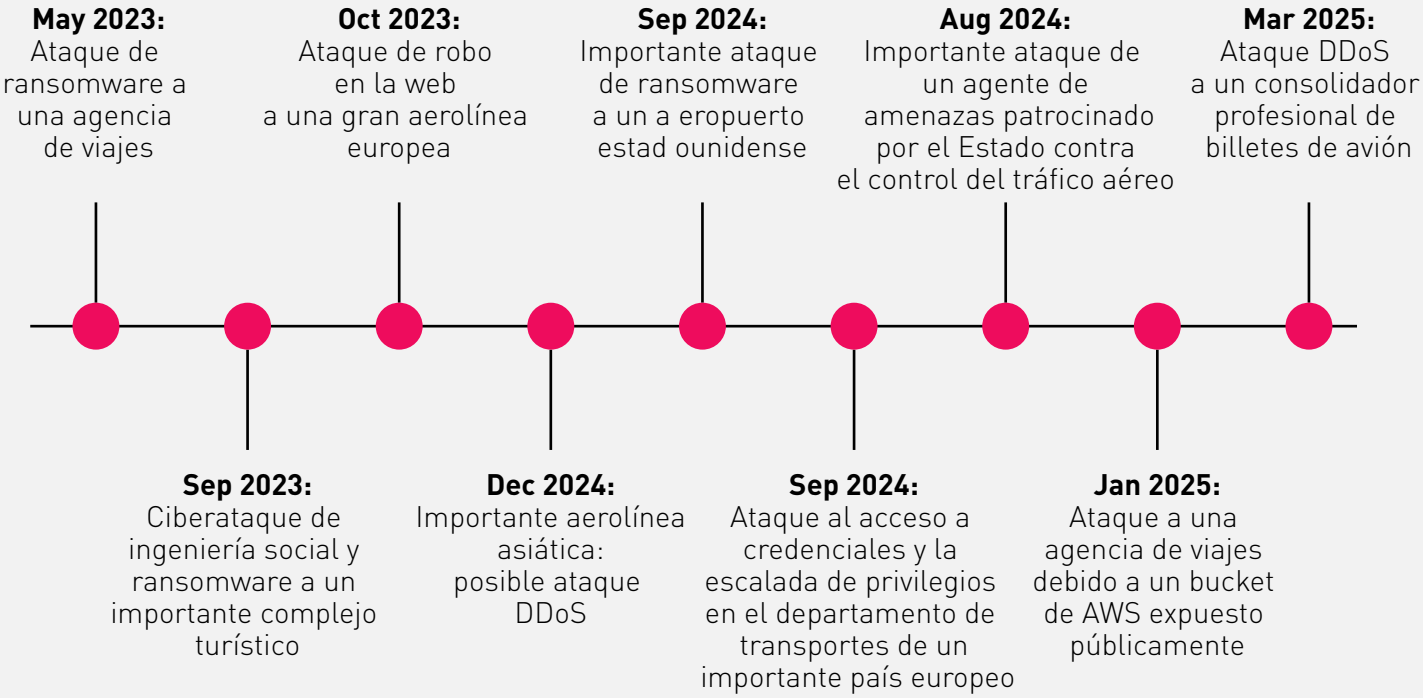


Figure 1: Timeline of Cyber Attacks Covered in this Report

DETALLES DE LOS INCIDENTES CIBERNÉTICOS

Ataque DDoS a un consolidador profesional de billetes de avión

En marzo de 2025, un ciberataque interrumpió las operaciones de un consolidador profesional de billetes de avión, afectando a sus clientes en Alemania, Austria, Suiza y en todo el mundo. Su sistema de reservas, se vio afectado debido a un posible ataque «DDOS»..

Ataque a una agencia de viajes debido a un bucket de AWS expuesto públicamente

En enero de 2025, una agencia de viajes australiana sufrió un ataque que provocó la filtración de 112.000 registros de la base de datos de la empresa, no protegida con contraseña y con un tamaño de 26,8 GB, incluidos detalles como imágenes de pasaportes, visados de viaje, itinerarios y billetes de viaje, y números parciales de tarjetas de crédito de clientes. Se descubrió que se habían filtrado hojas de cálculo con información detallada de más de 13.000 clientes, que incluía sus nombres, direcciones de correo electrónico, gastos de viaje y destinos. Aunque la mayoría de los viajeros afectados son australianos, también se han visto afectados clientes de Nueva Zelanda, Irlanda y Gran Bretaña.

La brecha se debió a un cubo de almacenamiento en la nube de Amazon AWS expuesto públicamente que estaba mal configurado. Estos ataques suelen comenzar con la búsqueda de sistemas expuestos o almacenamiento en la nube mal configurado. Se utilizaron herramientas o scripts para buscar cubos S3 abiertos o servicios de almacenamiento en la nube (por ejemplo, Bucket Finder, S3Scanner, Shodan, Censys o Grayhat Warfare). Los actores de amenazas también aprovechan las automatizaciones basadas en palabras clave para buscar archivos como passwords.txt, .env, db_backup.sql, etc.

Importante ataque de un agente de amenazas patrocinado por el Estado contra el control del tráfico aéreo

En agosto de 2024, una infraestructura informática administrativa, que gestiona las comunicaciones internas de las oficinas, sufrió un ataque. Esto permitió el acceso no autorizado a datos sensibles. Se atribuyó este ataque a Fancy Bear (alias APT28), un actor de amenazas supuestamente atribuido al servicio de inteligencia militar de Rusia.

Ataque al acceso a credenciales y la escalada de privilegios en el departamento de transportes de un importante país europeo

En septiembre de 2024, el departamento de transportes de un importante país europeo sufrió un ciberataque que les obligó a suspender temporalmente las solicitudes de tarjetas de acceso debido a la preocupación por la seguridad del sistema.

Esto también afectó a la capacidad de registrar nuevas tarjetas, emitir reembolsos por viajes de pago por uso incompletos realizados con tarjetas sin contacto y mejorar el sistema de reservas para el servicio Dial-a-Ride. También se vio afectada la alimentación de datos de viajes en directo. Aunque se respetaron las reservas anteriores, las nuevas sólo pudieron hacerse por teléfono hasta que se restableció el sistema. Se accedió a los datos de 5.000 personas, incluidos nombres, datos de contacto y datos de reembolso de tarjetas de acceso. Esto incluía números de cuentas bancarias y códigos de clasificación.

Al parecer, los atacantes utilizaron LicensingUI.exe (un binario firmado de Windows) para ejecutar las cargas útiles. TfL tuvo que restablecer 30.000 contraseñas de empleados en persona, lo que indica la magnitud de la brecha. El autor de la amenaza puede haber establecido persistencia y privilegios elevados, posiblemente utilizando tareas programadas o tokens de administrador.

Importante ataque de ransomware a un aeropuerto estadounidense

En septiembre de 2024, varios sistemas críticos de un importante aeropuerto estadounidense se vieron afectados debido a un ciberataque atribuido a afiliados de Rhysida.

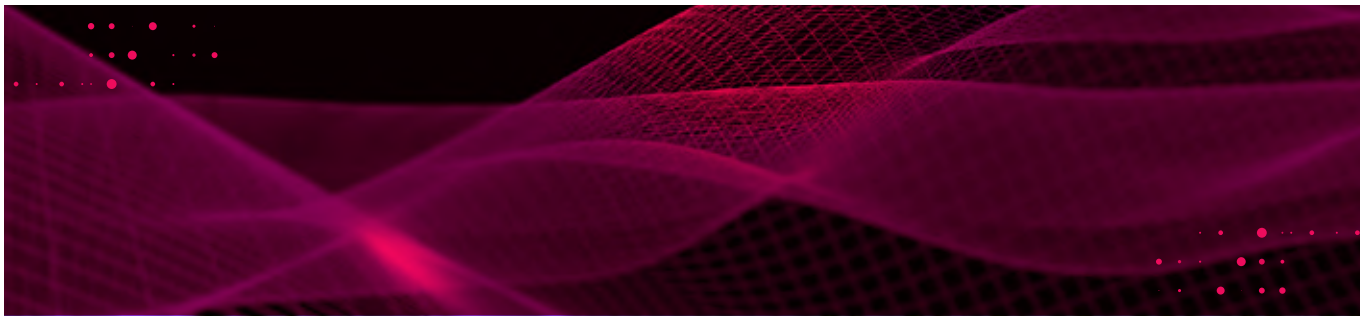
Los retrasos en el procesamiento del equipaje provocaron que las maletas se entregaran a los viajeros mucho después de su llegada. Debido a las caídas del sistema, los pasajeros tuvieron que utilizar tarjetas de embarque manuscritas. Los sistemas portuarios internos estaban encriptados, lo que dificultó el proceso de restablecimiento.

Los autores de la amenaza accedieron y descargaron cierta información personal de sistemas portuarios utilizados anteriormente para datos de empleados, contratistas y aparcamientos (90000 personas). La información descargada incluía nombres, fechas de nacimiento, números de la Seguridad Social (o los cuatro últimos dígitos de los números de la Seguridad Social), números de carné de conducir o de otras tarjetas de identificación gubernamentales, e información médica.

Los actores de Rhysida operan como ransomware-as-a-service (RaaS), donde las herramientas y la infraestructura de ransomware se alquilan en un modelo de reparto de beneficios. Se ha observado que los actores de Rhysida utilizan servicios remotos externos para acceder a una red y permanecer en ella inicialmente. También se les ha observado autenticándose en puntos de acceso VPN internos con credenciales válidas comprometidas, sobre todo porque las organizaciones no tienen activada la AMF por defecto. Además, se les ha observado explotando Zerologon -una vulnerabilidad crítica de elevación de privilegios en el protocolo remoto Netlogon de Microsoft- y llevando a cabo intentos de phishing con éxito.

Importante aerolínea asiática: posible ataque DDoS

En diciembre de 2024, una importante aerolínea asiática fue víctima de un ciberataque que provocó retrasos en los vuelos. Aunque no identificaron públicamente al actor específico de la amenaza, confirmaron que no se filtraron datos de clientes ni se detectaron virus informáticos. El incidente consistió en un aumento del tráfico, lo que sugiere un ataque DDoS, que interrumpió los sistemas de la aerolínea y la venta de billetes.



Ataque de robo en la web a una gran aerolínea europea

En octubre de 2023, IncRansom (un grupo ruso de piratas informáticos) obtuvo acceso no autorizado al sistema de pago de la aerolínea. Aunque no se ha confirmado el método del ataque, lo más probable es que se produjera a través de la web.

La brecha expuso datos confidenciales de los clientes, incluida información sobre tarjetas de crédito como números de tarjeta, fechas de caducidad y códigos CVV. La aerolínea notificó rápidamente a los clientes afectados y les aconsejó que cancelaran sus tarjetas para evitar posibles usos fraudulentos. En marzo de 2024, la aerolínea actualizó su información, revelando que se había expuesto información personal adicional, como nombres, números de DNI o pasaporte, fechas de nacimiento, números de teléfono, direcciones de correo electrónico y nacionalidades.

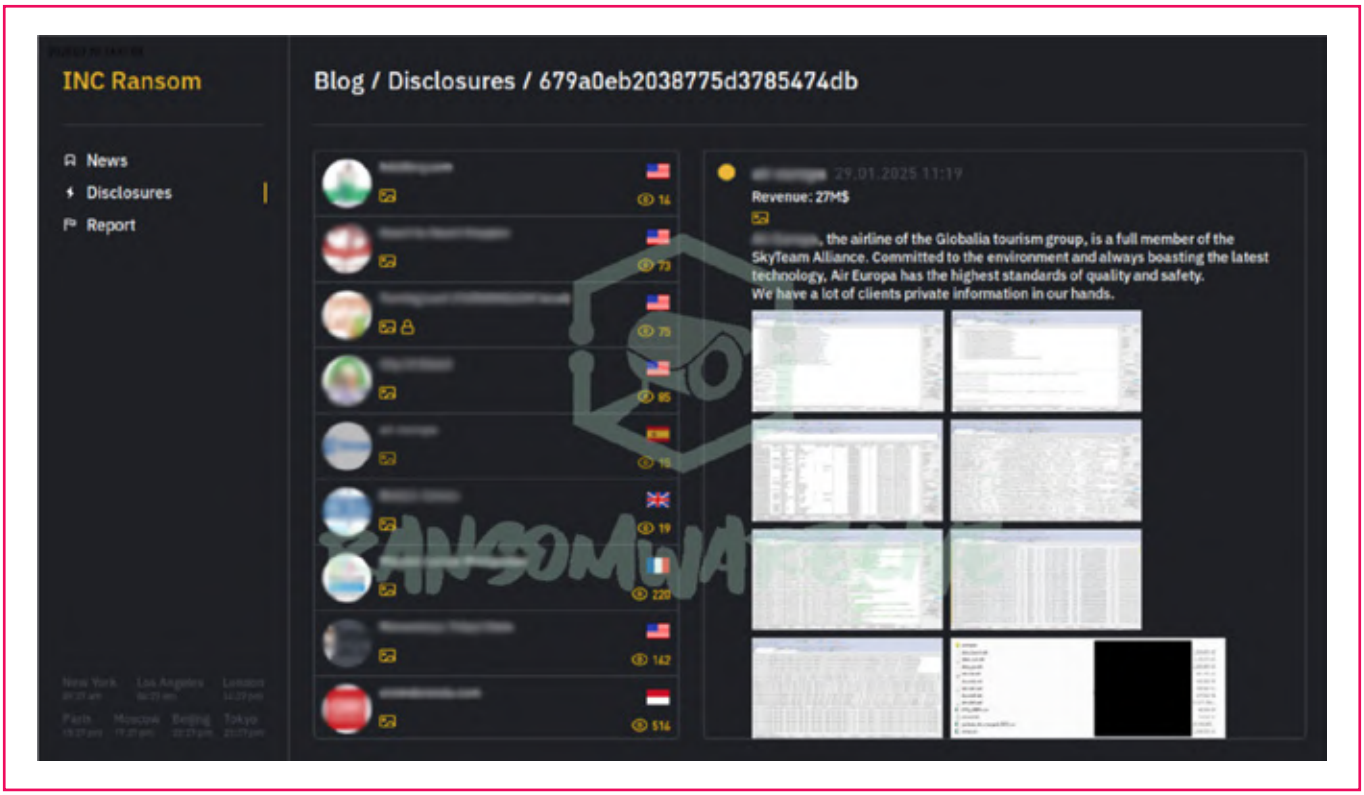


Figure 2: Screenshot from INCRansomware DLS affecting European Airline

Ciberataque de ingeniería social y ransomware a un importante complejo turístico

En septiembre de 2023, una importante cadena de complejos turísticos de Estados Unidos se vio afectada por un ciberataque, un esfuerzo combinado de Scattered Spider y ALPHV.

Los miembros de Scattered Spider investigaron a los empleados de la empresa en LinkedIn para recabar información. Se hicieron pasar por un empleado y convencieron al servicio de asistencia informática para que les proporcionara credenciales de inicio de sesión. Con ellas, los atacantes obtuvieron acceso de administrador a los entornos Okta y Azure de The resort, lo que les permitió moverse lateralmente dentro de los sistemas. A continuación, ALPHV desplegó el ransomware en varios servidores de hipervisor VMware ESXi.

Estos servidores alojaban miles de máquinas virtuales que soportaban sistemas críticos de la hostelería como máquinas de juego, sistemas de reservas online, llaves digitales de habitaciones y sitios web. ALPHV también afirma haber exfiltrado 6 TB de información de clientes durante este tiempo, tras lo cual iniciaron negociaciones con la cadena de complejos turísticos para evitar la divulgación pública de los datos robados.

Ataque de ransomware a una agencia de viajes

En mayo de 2023, Lockbit atacó una agencia de viajes francesa. Tras la negativa de la agencia a pagar el rescate, LockBit publicó aproximadamente entre 7.000 y 10.000 fotocopias de pasaportes en la dark web. Estos documentos se obtuvieron de clientes que participaban en viajes en grupo, lo que constituye alrededor del 2% de la base de clientes de la agencia. Lockbit funciona a través de un modelo RaaS (Ransomware as a Service). Por favor, consulte el apéndice para sus TTPs.

(Para más información sobre TTPs y COIs basados en The Appendix)

LAS 10 TTPS MÁS CRÍTICAS EN ESTE SECTOR

Las TTPs que aparecen a continuación se han clasificado como graves en función de su impacto, frecuencia en incidentes del mundo real y dificultad para detectarlas o mitigarlas.

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

PREDICCIONES DE TENDENCIAS

Las siguientes predicciones se derivan del análisis de incidentes cibernéticos recientes dirigidos al sector de los viajes y a las operaciones de las empresas de viajes, incluidos ataques DDoS, almacenamiento en la nube mal configurado, ingeniería social y ransomware.

Cada predicción se centra en vectores de ataque específicos observados en incidentes entre 2023-2025, proyectando cómo estas amenazas podrían evolucionar y afectar a las empresas y operaciones de viajes en el futuro.

1 AUMENTO DE LOS ATAQUES DDOS CONTRA SISTEMAS DE RESERVA Y VENTA DE BILLETES

Los principales ataques de marzo de 2025 y diciembre de 2024 ponen de relieve los ataques críticos que implicaron campañas DDoS que interrumpieron sistemas cruciales de reservas y emisión de billetes, causando retrasos operativos e insatisfacción de los clientes. Estos ataques se aprovecharon de la dependencia del sector de los viajes de plataformas y sistemas en línea en tiempo real.

En el futuro, es probable que los actores de amenazas sigan desplegando ataques DDoS para saturar los sistemas de reservas o las plataformas de emisión de billetes de avión con el objetivo de perturbar las temporadas altas de viajes (por ejemplo, las vacaciones). Además de las crecientes tensiones geopolíticas, es probable que los ciberataques patrocinados por estados-nación también se vuelvan más frecuentes y sofisticados con el objetivo de perturbar las infraestructuras críticas y los sistemas financieros destinados a desestabilizar las economías.

Es probable que los atacantes utilicen redes de bots mejoradas por la amplificación del tráfico impulsada por la IA para eludir las defensas DDoS tradicionales. En el sector de la aviación, alrededor de 1/4 de los incidentes tienen su origen en vulnerabilidades de proveedores, lo que ofrece a los actores de amenazas vías para amplificar los picos de tráfico utilizando redes de bots impulsadas por IA. Las agencias de viajes más pequeñas, con presupuestos de ciberseguridad limitados, podrían ser especialmente vulnerables, enfrentándose a tiempos de inactividad y pérdidas de ingresos.

Si esta tendencia continúa, podría haber un aumento de los esquemas de extorsión en los que los atacantes exigen rescates para detener las campañas DDoS, explotando la necesidad del sector de un servicio ininterrumpido. Esta táctica se observó en otro sector: un ataque de ransomware sanitario en 2024, en el que BlackCat/ALPHV exigió millones para restaurar los sistemas críticos, lo que pone de manifiesto la rentabilidad de atacar operaciones sensibles al tiempo. En última instancia, esto exigiría que el sector invirtiera en protección DDoS basada en la nube, auditara la seguridad de los proveedores y sometiera a pruebas de estrés las plataformas de reserva.

2 AUMENTO DE LAS FILTRACIONES DE DATOS A TRAVÉS DE UN ALMACENAMIENTO EN LA NUBE MAL CONFIGURADO

En 2025, una empresa de viajes australiana sufrió una filtración de datos importante cuando un cubo de almacenamiento en la nube de AWS quedó accesible al público sin contraseña. Como resultado, quedaron expuestos más de 112.000 registros de clientes, incluidos pasaportes escaneados y números parciales de tarjetas de crédito. Este incidente ilustra una importante vulnerabilidad que afecta al sector de los viajes y el turismo en general: los sistemas de almacenamiento en la nube mal configurados.

Las amenazas automatizan cada vez más el descubrimiento y la explotación del almacenamiento en la nube mal configurado, especialmente en plataformas como AWS y Azure. Herramientas como Bucket Finder, S3Scanner y motores de búsqueda como Shodan y Censys permiten a los agresores localizar fácilmente buckets de acceso público. Una vez identificados, se aprovechan los permisos excesivamente permisivos (por ejemplo, READ, LIST o WRITE) para acceder de forma anónima a los datos almacenados o alterarlos. A continuación, los atacantes despliegan scripts basados en palabras clave utilizando AWS CLI o boto3 para buscar archivos confidenciales como .env, passwords.txt o db_backup.sql. Si no se aplica HTTPS, los datos pueden incluso filtrarse a través de canales no cifrados.

A medida que la industria de los viajes y el turismo continúa su cambio a la infraestructura en la nube, especialmente entre los operadores pequeños y medianos que carecen de controles sólidos de ciberseguridad, el almacenamiento en la nube mal configurado seguirá siendo una de las vulnerabilidades más explotadas. El uso de herramientas de análisis automatizadas y tácticas de búsqueda basadas en IA no hará sino acelerarse, permitiendo a los atacantes identificar y extraer datos valiosos a escala. Podemos esperar un aumento de la extorsión selectiva y el fraude basado en la fuga de datos, lo que empujará a los organismos reguladores a endurecer las normas de cumplimiento y obligará a las empresas a implementar auditorías de configuración continuas, controles de acceso estrictos y políticas de cifrado de extremo a extremo.

3 CAMPAÑAS DE PHISHING QUE SE APROVECHAN DE LAS CREDENCIALES DE LOS EMPLEADOS

El ataque de 2023 a un importante complejo turístico estadounidense reveló un patrón de amenaza creciente: los ataques de phishing y suplantación de identidad se están utilizando como punto de entrada para comprometer los sistemas internos. El actor de la amenaza Scattered Spider se hizo pasar por un empleado tras investigar los perfiles de LinkedIn, convencer al personal del servicio de asistencia de TI para que le entregara sus credenciales y desplegar un ransomware que paralizó los sistemas operativos.

En 2025, podemos esperar un aumento de las campañas de phishing impulsadas por IA dirigidas específicamente al personal de primera línea y de asistencia de agencias de viajes, aerolíneas y operadores aeroportuarios. Esto es especialmente crítico, ya que más del 70% de los ataques en el sector de la aviación se centran en el robo de datos de inicio de sesión y el acceso no autorizado a la infraestructura de TI. Los atacantes utilizarán correos electrónicos generados por IA imitando a proveedores o ejecutivos de confianza, como se ha visto en el caso anterior, para engañar al personal y conseguir que facilite el acceso a sistemas como plataformas de reservas o pasarelas de pago. La alta rotación de empleados del sector de los viajes y las tendencias de trabajo a distancia aumentarán las vulnerabilidades. Podrían aumentar las tácticas de doble extorsión, en las que los datos robados de los clientes (por ejemplo, pasaportes o tarjetas de crédito) se filtran si no se pagan los rescates.

Los ataques de phishing han sido durante mucho tiempo una de las tácticas favoritas de los ciberdelincuentes y, con la integración de la IA generativa, estos ataques están a punto de volverse mucho más sofisticados. Los atacantes utilizarán la IA para crear correos electrónicos, mensajes de texto o mensajes de redes sociales de phishing altamente personalizados.

4 ATAQUES A LA CADENA DE SUMINISTRO A TRAVÉS DE TERCEROS

La brecha de una importante aerolínea europea en 2024 probablemente implicó el robo de datos a través de un sistema de pago comprometido, exponiendo datos de tarjetas de crédito e información personal. Del mismo modo, el ataque al aeropuerto estadounidense de 2024 puso de manifiesto la vulnerabilidad de los sistemas de terceros, ya que las filiales de Rhysida accedieron a los datos de empleados y contratistas. Estos incidentes reflejan una tendencia más amplia: la explotación de aplicaciones de cara al público (T1190) y las debilidades de la cadena de suministro que dejan al descubierto sistemas de gran valor en el sector de los viajes.

Con la creciente dependencia de los servicios en la nube y los ecosistemas de múltiples proveedores, es probable que los atacantes sigan explotando los eslabones más débiles de las cadenas de suministro digitales. En 2025, los ataques a la cadena de suministro dirigidos a terceros proveedores, como procesadores de pagos, plataformas de reservas y servicios de verificación de identidad, podrían intensificarse. Los agresores pueden centrarse en infiltrarse en proveedores más pequeños y menos seguros como puntos de entrada para comprometer a organizaciones de viajes más grandes. Una vez dentro, los atacantes a menudo capturan datos de entrada (T1056), extraen información financiera o de clientes sensible de los sistemas y repositorios internos (T1213) y la filtran a través de servicios web de confianza o plataformas en la nube (T1048.003), lo que les ayuda a evadir la detección de seguridad tradicional.

Estos ataques pueden dar lugar a filtraciones de datos a gran escala, fraudes financieros e interrupciones operativas, especialmente en el caso de las empresas que utilizan software de proveedores obsoletos, lo que aumenta su exposición a las vulnerabilidades de día cero. También se espera que los actores de las amenazas sigan atacando de forma oportunista a las organizaciones con defensas débiles en la cadena de suministro, aprovechando la falta de control de las empresas sobre sus socios externos.

La Agencia Europea de Seguridad de las Redes y de la Información (ENISA) ha señalado los riesgos de la cadena de suministro como una preocupación creciente, destacando su naturaleza sigilosa, su complejidad y sus amplias consecuencias. Muchas organizaciones de todos los sectores siguen sin estar suficientemente preparadas para hacer frente a estas amenazas. El sector de los viajes es especialmente vulnerable debido a su gran dependencia de las plataformas en la nube y los intrincados ecosistemas de proveedores.

Además, cada vez más organizaciones están adoptando modelos de IA de gran tamaño (LLM) a un ritmo cada vez mayor durante 2024, y se espera que se unan más a lo largo de 2025. Los actores de amenazas son conscientes de esta nueva tendencia y tratan de explotarla llevando a cabo ataques de envenenamiento de datos en los modelos de entrenamiento en los que se basan los LLM.

CYBERINT, AHORA UNA COMPAÑÍA DE CHECK POINT SOLUCIONES

Dadas las recientes tendencias de amenazas emergentes, es esencial entender la gama de servicios que Cyberint ofrece para ayudar a protegerse contra estos riesgos.

Cyberint, ahora una compañía de Check Point, monitoriza varios activos, incluyendo dominios, correos electrónicos, direcciones IP externas, empleados de alto impacto y más. Cada activo se configura cuidadosamente para satisfacer las necesidades cruciales a medida que los equipos de seguridad maniobran los numerosos retos a los que se enfrentan a lo largo del año.

Estos activos se supervisan diariamente en la solución Cyberint mediante la automatización de la supervisión de la superficie de ataque (ASM), la recopilación de información sobre amenazas, la detección de phishing y la colaboración de analistas especializados.

ATTACK SURFACE MONITORING

El módulo Attack Surface Monitoring de la solución Cyberint realiza escaneos no intrusivos, diarios y semanales, de las siguientes categorías de activos:

- **Dominios**
- **Subdominios**
- **Direcciones IP**
- **Azure Data Lake / Blobs de almacenamiento**
- **Almacenamiento en la nube de Google**
- **Amazon S3 Buckets**

Los análisis de exposición diarios automatizados supervisan continuamente las tecnologías vulnerables, las configuraciones erróneas, los puertos explotables o abiertos y otros elementos de exposición potenciales. Cuando se detecta un problema, se genera automáticamente una alerta y se envía al módulo de alertas, donde el equipo puede revisarla y determinar los siguientes pasos apropiados.

Este análisis diario es imprescindible para supervisar las posibles vulnerabilidades de los activos externos, especialmente los buckets de Amazon S3, ya que está directamente relacionado con el ciberataque al sistema de tickets mencionado anteriormente, en el que los actores de la amenaza accedieron a un bucket de almacenamiento en la nube configurado de forma incorrecta.

El módulo Attack Surface Monitoring (ASM) proporciona visibilidad continua de una amplia gama de activos digitales a través de análisis diarios y semanales no intrusivos. Identifica vulnerabilidades, configuraciones incorrectas y servicios expuestos en dominios, IP y almacenamiento en la nube, al tiempo que aprovecha los datos públicos y las integraciones opcionales en la nube para descubrir activos asociados que pueden no proporcionarse directamente.

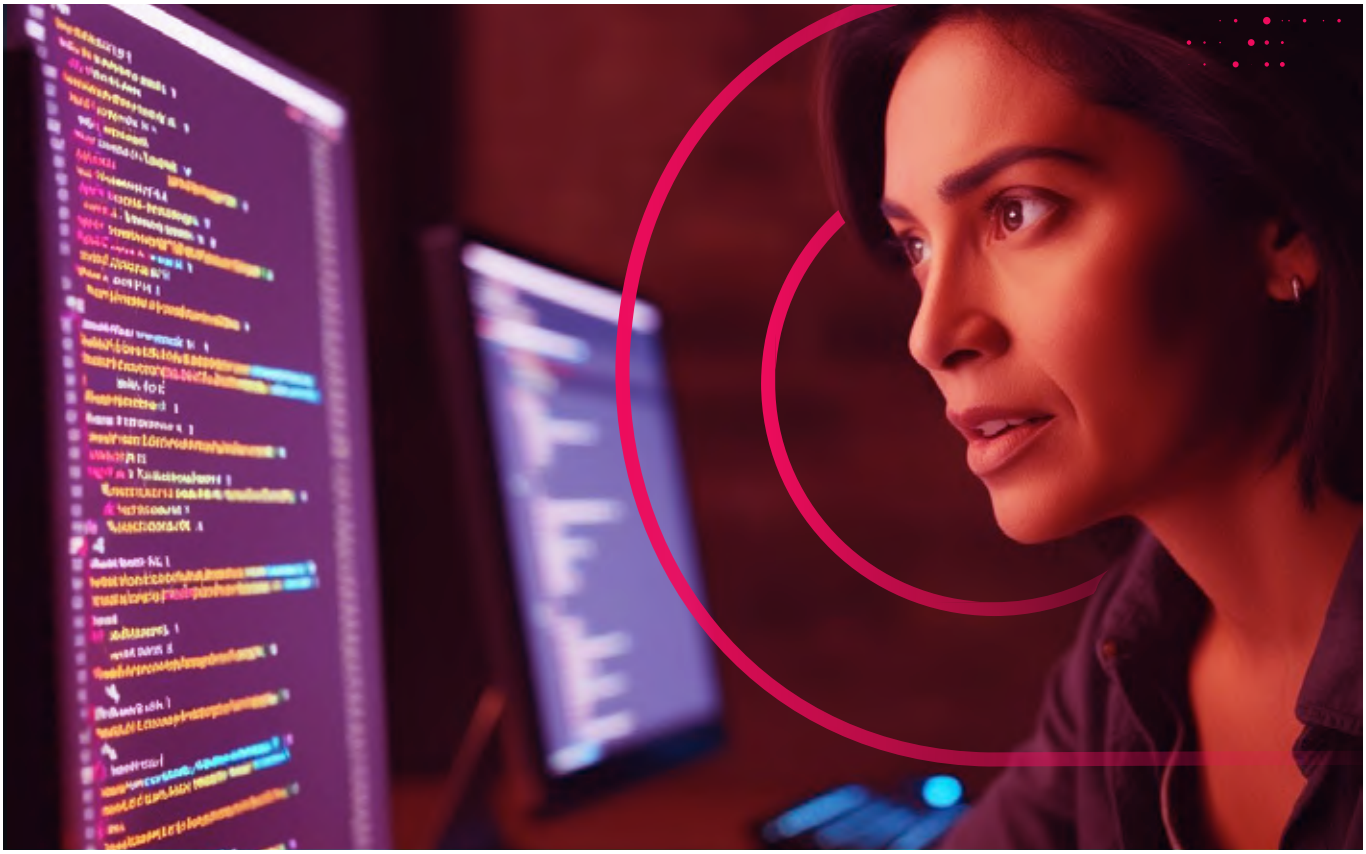
Este enfoque integral garantiza que las organizaciones estén al tanto de su exposición externa y puedan tomar medidas oportunas ante cualquier problema detectado.

MONITORIZACIÓN DE THREAT INTELLIGENCE

Detección de Phishing

Bajo la protección de phishing de Cyberint, los activos de dominio principales pueden ser marcados tanto para Inteligencia de Amenazas como para Monitorización de Superficie de Ataque, permitiendo la detección automática de dominios sospechosos de semejanza.

Para complementar la automatización, el Phishing Beacon de Cyberint, ahora una empresa de Check Point, identifica proactivamente los sitios de phishing incrustando un script no intrusivo dentro del sitio web protegido. Nos alerta cuando los actores maliciosos intentan clonar ese mismo sitio en dominios no autorizados.



Threat Hunting

La supervisión de la inteligencia sobre amenazas se refuerza mediante la designación estratégica de activos clave. Una vez identificados, estos activos se supervisan continuamente a través de una amplia gama de fuentes de inteligencia, incluidos foros clandestinos, repositorios de código y redes sociales, para sacar a la luz posibles riesgos. El analista especializado revisa diariamente la inteligencia recopilada y notifica a los equipos de seguridad pertinentes cualquier amenaza relevante.

Además, el equipo de analistas de Cyberint, ahora una empresa de Check Point, consume constantemente una variedad de informes que nos permiten adaptarnos continuamente al panorama de amenazas en constante evolución en lo que respecta a sectores específicos y hace recomendaciones sobre las mejores prácticas para mitigar las amenazas emergentes.

Supervisión de la cadena de suministro

Además, la supervisión de la cadena de suministro es un servicio que ofrece Cyberint, ahora una empresa de Check Point, que permitiría añadir proveedores externos específicos utilizados por la organización del cliente para supervisarlos continuamente y, si se detectan, automatizar las alertas correspondientes:

- Menciones del nombre del proveedor de la cadena de suministro en foros de la Darknet
- Menciones del nombre del proveedor de la cadena de suministro en filtraciones.
- Un proveedor que sufra un ataque de ransomware en curso
- Campaña de phishing emergente relacionada con el proveedor de la cadena de suministro
- Filtración del código fuente de un proveedor de la cadena de suministro
- Proveedor de la cadena de suministro puesto a la venta

La supervisión continua de los proveedores externos es esencial porque sus sistemas y prácticas de seguridad pueden repercutir directamente en la exposición al riesgo de la organización.

Esta supervisión sigue siendo muy importante en los entornos de ciberamenazas actuales y emergentes, ya que los actores de las amenazas se dirigen cada vez más a los proveedores de la cadena de suministro como punto de entrada para comprometer a las grandes organizaciones. Mediante la identificación proactiva de vulnerabilidades, brechas o actividades sospechosas dentro del ecosistema del proveedor, se puede responder rápidamente a las amenazas potenciales y evitar consecuencias posteriores en el entorno de la empresa.

La combinación de una amplia recopilación de inteligencia y la supervisión y el análisis continuos por parte del analista especializado ayuda a comprender mejor el panorama de amenazas externas de la organización.

DEDICATED ANALYST SERVICES

El analista proporciona muchos servicios además de la supervisión diaria de amenazas y alertas. El analista dedicado se considera el experto de la solución Cyberint, que busca maximizar el uso de la plataforma y garantizar que todos los módulos funcionen de forma eficiente y según lo previsto.

Algunas de las tareas que realizan los analistas para perfeccionar la solución de forma continua incluyen:

- **Configuración de activos:** El analista se asegura de que cada activo recibido está configurado para satisfacer las necesidades del cliente.

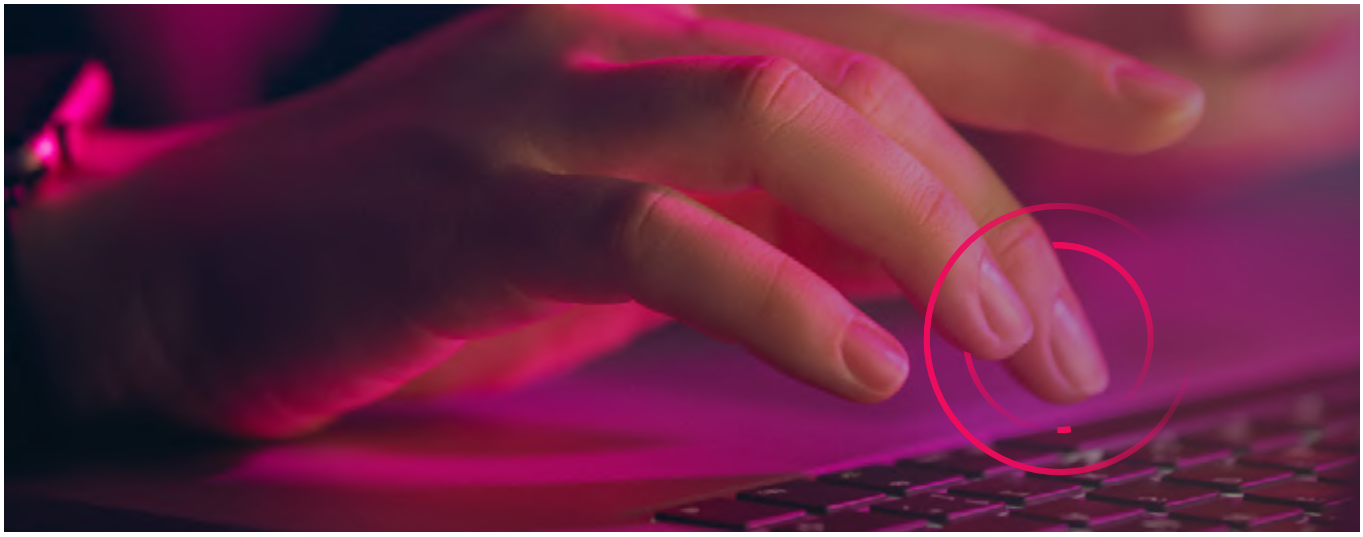
- **Actualización de activos:** de forma incremental, el analista solicita actualizaciones para garantizar una cobertura actualizada.

- **Supervisión de métricas del entorno:** los analistas supervisan la automatización y las alertas para sugerir formas de ajustar el entorno a las necesidades del cliente.

- **Configuración de alertas:** los analistas revisan las alertas, como los motivos de cierre y los comentarios de los clientes, para hacer sugerencias sobre configuraciones de alertas (es decir, desactivaciones, anulaciones de gravedad, ajuste de la política de contraseñas corporativa)

El analista dedicado también celebra reuniones periódicas -típicamente mensuales- para presentar las alertas clave y los puntos de debate, proporcionando a los clientes una visión clara de los hallazgos más impactantes y del valor global de los esfuerzos continuos del analista.

Con el tiempo, los analistas ven a diario la inteligencia bruta recopilada que menciona los activos del cliente, y se convierten en expertos a la medida de los requisitos de inteligencia y la estrategia del cliente. Con esta experiencia, pueden hacer más sugerencias de inteligencia en llamadas estratégicas como una Priority Requirement Alignment (PIR) para garantizar la alineación con los objetivos estratégicos de la empresa, o reuniones de Quarterly Business Review (QBR).



CONCLUSIONES Y RECOMENDACIONES

CONCLUSIONES

El sector de los viajes se enfrenta a un panorama de amenazas externas en constante evolución, impulsado por el aumento de los ataques DDoS, las campañas de phishing, las desconfiguraciones de la nube y los compromisos de la cadena de suministro. A medida que los atacantes se adaptan, también deben hacerlo las estrategias defensivas de las organizaciones de viajes, sobre todo en lo que respecta a la forma en que entienden y responden a las amenazas más allá de sus perímetros internos.

Como un importante socio de monitoreo de inteligencia de amenazas externas, Cyberint, ahora una compañía de Check Point, está posicionada para desempeñar un papel crítico en el fortalecimiento de la resiliencia cibernética mediante la entrega de información oportuna, relevante y procesable.

Mediante la combinación de la recopilación de inteligencia en tiempo real, la visibilidad de la superficie de ataque externa y los conocimientos de los analistas, Cyberint, ahora una empresa de Check Point, ayuda a anticipar y mitigar las amenazas cibernéticas antes de que afecten a las operaciones. En un sector tan sensible al tiempo y orientado al cliente como el de los viajes, contar con un socio centrado en lo que ocurre más allá del cortafuegos de la empresa ya no es opcional, sino esencial.

RECOMENDACIONES

Basándose en los recientes ciberataques dirigidos al sector de los viajes, Cyberint, ahora una empresa de Check Point, recomienda lo siguiente:

1 DEFENSA CONTRA ATAQUES DDOS EN SISTEMAS DE RESERVAS Y EMISIÓN DE BILLETES

Como prevemos un aumento de los ataques DDoS basados en IA dirigidos a plataformas de viajes críticas durante periodos de mucho tráfico, nuestras recomendaciones son las siguientes:

- Utiliza Cyberint para monitorizar las conversaciones previas a los ataques en foros clandestinos, canales de Telegram y mercados de botnets donde se planifican o anuncian campañas DDoS.
- Rastree las menciones a sus principales plataformas e infraestructura digital para detectar señales de alerta temprana de posibles ataques.
- mplemente un mecanismo de prevención de DDoS: aplique la protección DDoS basada en la nube, audite la seguridad de los proveedores y realice pruebas de estrés de las plataformas de reserva.

2 PREVENCIÓN DE FUGAS DE DATOS POR ALMACENAMIENTO EN LA NUBE MAL CONFIGURADO

Cyberint, ahora una empresa de Check Point, prevé un aumento de la explotación de los buckets de nube abiertos, lo que provocará fugas de datos confidenciales en el sector. Por ello, nuestras recomendaciones son las siguientes

- Utilice Cyberint para Monitorizar los datos expuestos vinculados a su marca o clientes a través de foros de brechas, sitios de pasta y repositorios de búsqueda.
- Utilice Cyberint para reforzar la supervisión de fugas relacionadas con la configuración, como archivos .env, .bak o de copia de seguridad detectados en volcados de actores de amenazas o buckets públicos.
- Utilice la detección ASM (Attack Surface Monitoring) de Cyberint para buscar continuamente activos en la nube recién expuestos, almacenamiento mal configurado y cambios no autorizados en su huella en la nube.

3 CÓMO MITIGAR EL PHISHING Y LA SUPLANTACIÓN DE CREDENCIALES BASADOS EN IA

Cyberint, ahora una empresa de Check Point, prevé un aumento del phishing sofisticado mediante IA generativa y suplantación de identidad dirigido al personal de primera línea del sector. Por ello, nuestras recomendaciones son las siguientes

- Implemente la monitorización de suplantación de su marca, ejecutivos o equipos de atención al cliente a través de redes sociales, registros de dominios y kits de phishing. Cyberint, ahora una empresa de Check Point, ofrece este servicio.
- Enforce Supervisión temprana de la infraestructura de phishing a través de dominios parecidos y sitios clonados utilizando nuestra detección de phishing. Cyberint, ahora una empresa de Check Point, proporciona este servicio.

4 SUPERVISIÓN DE RIESGOS DE TERCEROS Y EXPLOTACIÓN DE LA CADENA DE SUMINISTRO

Cyberint, ahora una empresa de Check Point, prevé un aumento de los ataques a través de proveedores vulnerables, plataformas de pago y herramientas de terceros obsoletas. Por ello, nuestras recomendaciones son las siguientes

- Supervise continuamente los ecosistemas de proveedores en busca de indicadores de compromiso, credenciales filtradas o datos que mencionen a su organización a través de conexiones de terceros. Cyberint, ahora una empresa de Check Point, ofrece una solución de supervisión de proveedores externos.
- Rastree las violaciones de la cadena de suministro de sectores específicos y proporcione inteligencia contextual sobre amenazas para evaluar si su entorno se ve indirectamente afectado.
- Bloquee los IOC: Para proteger sus sistemas internos, recomendamos importar la lista de IOC proporcionada a su plataforma de protección de endpoints y configurarla para bloquear o poner en cuarentena cualquier amenaza que coincida. Además, aplique las IP y los dominios a su DNS interno o a las políticas de cortafuegos basadas en host para evitar la comunicación con infraestructuras maliciosas conocidas. Consulte la lista de IOC en las páginas 26-37.

APPENDIX

CONSOLIDATED TTP LIST

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 BY THREAT ACTOR

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

ABOUT CYBERINT

Cyberint, now a Check Point company, reduces risk by helping organizations detect and mitigate external cyber threats before they have an adverse impact. The Check Point External Risk Management solution provides superior visibility through continuous discovery of the evolving attack surface, combined with the automated collection and analysis of vast quantities of intelligence from across the open, deep and dark web. A team of global military-grade cybersecurity experts work alongside customers to rapidly detect, investigate, and disrupt relevant threats – before they have the chance to develop into major incidents. Global customers, including Fortune 500 leaders across all major market verticals, rely on Check Point External Risk Management to protect themselves from an array of external risks, including vulnerabilities, misconfigurations, phishing, impersonation attacks, malware infections, exposed credentials, data leaks, fraud, and 3rd party risks.

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