Guatemala - El Salvador - Honduras - República Dominicana

Devel
CYBERSECURITY REDEFINED

CYBER SECURITY NEWS

SECURITY OPERATIONS CENTER

ATACANTES AFECTAN A ORANGE Y CROWDSTRIKE: ¿COINCIDENCIA O REPRESALIA CIBERNÉTICA?

26/ 02 / 2025

CONTENIDO

INTRODUCCIÓN

El reciente ataque cibernético que afectó a Orange y CrowdStrike ha despertado preocupaciones en la comunidad de seguridad informática, planteando interrogantes sobre si se trata de una coincidencia o una represalia premeditada. Tras la brecha de seguridad en Orange, la empresa recurrió a CrowdStrike, reconocida por su experiencia en respuesta a incidentes, para mitigar el impacto del ataque y fortalecer sus defensas. Sin embargo, poco después, CrowdStrike se convirtió en el blanco de un ciberataque, lo que ha llevado a especulaciones sobre una posible represalia por parte de actores malintencionados.

ATACANTES AFECTAN A ORANGE Y CROWDSTRIKE: ¿COINCIDENCIA O REPRESALIA CIBERNÉTICA?

A continuación, se encuentra en cuadro de identificación de la amenaza.

ID de alerta:	DSOC-CERT_2025_02_26_1
Clasificación de alerta:	Noticia
Tipo de Impacto:	Alta
TLP (Clasificación de información):	**CLEAR**
Fecha de publicación:	26/02/2025
Es día cero (0 day):	No

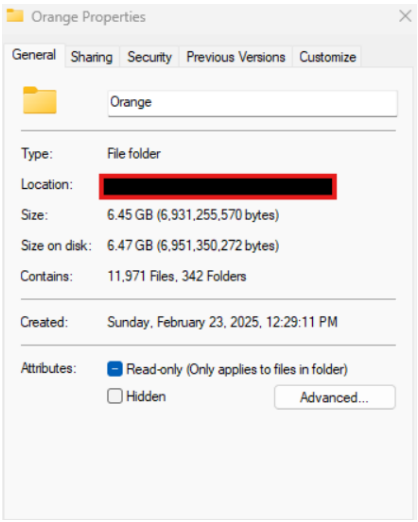
RESUMEN

El mundo digital ha sido testigo de una nueva serie de ciberataques dirigidos contra grandes corporaciones. En febrero de 2025, Orange Group, una de las principales empresas de telecomunicaciones, confirmó una brecha de seguridad tras la filtración de documentos internos por parte de hackers. Lo que parecía ser un incidente aislado tomó un giro inesperado cuando, poco después, CrowdStrike, la reconocida empresa de ciberseguridad, también se convirtió en blanco de los atacantes.

La filtración en Orange

El incidente que afectó a Orange Group fue mucho más que un simple ataque cibernético; representó una grave vulnerabilidad en su infraestructura de seguridad. El actor de amenazas Rey afirmó que esta filtración no está relacionada con la operación de ransomware HellCat, lo que indica que el enfoque del ataque fue diferente y más sutil.

Los atacantes afirmaron haber tenido acceso a los sistemas de Orange durante más de un mes, lo que sugiere que la empresa no detectó a tiempo la intrusión o no aplicó medidas efectivas para su contención. Durante este periodo, lograron extraer cerca de 12,000 archivos, con un peso total de aproximadamente 6.5 GB.



Los datos robados proceden en su mayoría de la sucursal rumana de la empresa e incluyen 380,000 direcciones de correo electrónico únicas, así como código fuente, facturas, contratos e información de clientes y empleados. Además, algunos de los datos verificados eran bastante antiguos, con direcciones de correo electrónico asociadas a personas que trabajaron o colaboraron con Orange Romania hace más de cinco años.

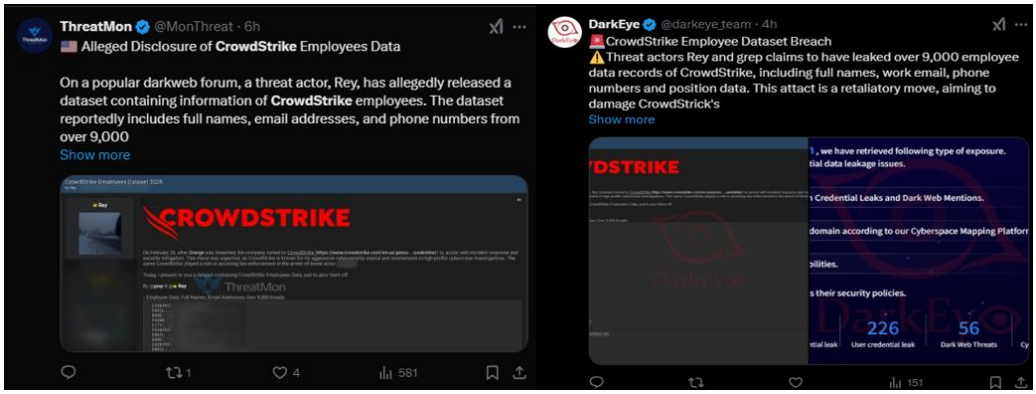
Un representante de Orange confirmó: “Orange puede confirmar que nuestras operaciones en Rumanía han sido objeto de un ciberataque. Tomamos medidas inmediatas y nuestra principal prioridad sigue siendo proteger los datos y los intereses de nuestros empleados, clientes y socios. No ha habido ningún impacto en las operaciones de los clientes, y se descubrió que la violación se produjo en una aplicación de back office no crítica”.

Orange ignoró la nota de rescate

A pesar de haber dejado una nota de rescate en los sistemas comprometidos, el grupo de atacantes indicó que Orange nunca intentó negociar. Esto sugiere que la empresa optó por una estrategia de contención y respuesta en lugar de ceder a las demandas de los atacantes, una práctica alineada con las recomendaciones de expertos en ciberseguridad para evitar incentivar este tipo de crímenes.

La filtración en CrowdStrike

La reciente violación de datos en CrowdStrike ha dejado al descubierto información sensible de más de 9,000 empleados de la compañía. Fuentes confiables han confirmado que los datos filtrados incluyen información sensible de empleados, como nombres completos, correos electrónicos corporativos, números de teléfono, puestos y ubicación dentro de la empresa. Además, se ha corroborado que el ataque resultó en la filtración de datos exclusivamente de empleados, sin que se viera afectado el producto o la operación de la empresa.



Datos Comprometidos

Los datos comprometidos incluyen información de empleados de más de 71 países, distribuidos de la siguiente manera:

País	Datos Filtrados	País	Datos Filtrados	País	Datos Filtrados	País	Datos Filtrados
Desconocido	239	Reino Unido	17	Perú	5	Sierra Leona	2
India	179	Nueva Zelanda	16	Canadá	5	Malta	2
EE. UU.	117	Arabia Saudita	14	Kenia	5	Grecia	2
Brasil	78	Colombia	14	Uruguay	5	Bolivia	2
Sri Lanka	71	Singapur	14	Eslovaquia	5	Botsuana	2
México	67	Sudáfrica	12	Jamaica	5	Burundi	1
Indonesia	65	Países Bajos	12	Polonia	4	Etiopía	1
Filipinas	50	Malasia	11	Nepal	4	Dinamarca	1

Turquía	41	Portugal	11	Mongolia	4	China	1
Camboya	38	Bangladesh	11	Bélgica	4	Suiza	1
Tailandia	34	Austria	10	Alemania	3	Hong Kong	1
Kuwait	31	Líbano	10	Mauricio	3	Bulgaria	1
España	31	Chequia	8	Nigeria	3	Argelia	1
Egipto	31	Hungría	8	Pakistán	3	Serbia	1
Chile	27	Guatemala	7	Vietnam	3	Omán	1
Israel	27	Qatar	7	Australia	3	Japón	1
Emiratos Árabes Unidos	26	Francia	6	Taiwán	2	Rumanía	1
Italia	23	Zambia	6	Birmania	2		

Motivo del ataque

Los ciberdelincuentes Rey y Grep han declarado que la publicación de estos datos es una represalia directa contra CrowdStrike, debido a su activa participación en la investigación y arresto de cibercriminales. En su mensaje, afirman que la intención es “molestar” a la empresa, dejando en claro que no buscan beneficios económicos, sino afectar su imagen y la seguridad de su equipo interno.

Asociación con Orange y posible relación con la filtración

Se cree que existe una relación entre el ataque a Orange y CrowdStrike. Después de la brecha de seguridad en Orange, la empresa buscó la ayuda de CrowdStrike, una firma reconocida por su experiencia en ciberseguridad y respuesta a incidentes, para gestionar la mitigación del incidente. La rápida intervención de CrowdStrike permitió a Orange mitigar parte de los daños y comenzar la investigación sobre cómo se llevó a cabo la intrusión. Sin embargo, esta acción parece haber atraído la atención de ciertos grupos cibercriminales, lo que resultó en un ataque dirigido contra la propia empresa de ciberseguridad.

El historial de CrowdStrike como un actor clave en la respuesta a incidentes de alto perfil la ha convertido en un objetivo frecuente de grupos de amenazas. Esto refuerza la teoría de que el ataque a CrowdStrike fue un acto de represalia, motivado por su participación en investigaciones y arrestos de ciberdelincuentes.

Recomendaciones

- **Capacitación y Concientización:** Implementar programas regulares para educar a los empleados sobre los riesgos de la ingeniería social, centrándose en cómo identificar correos de phishing y señales de advertencia.
- **Verificación de Comunicaciones:** Fomentar la práctica de verificar la autenticidad de correos electrónicos o mensajes antes de actuar, como confirmar solicitudes de información a través de números conocidos.

- **Filtros de Correo:** Utilizar herramientas de filtrado para detectar y bloquear correos sospechosos, disminuyendo el riesgo de ataques de phishing.
- **Autenticación de Dos Factores (2FA):** Implementar 2FA en cuentas sensibles para añadir una capa extra de seguridad, protegiendo las credenciales incluso si son comprometidas.
- **Simulacros de Phishing:** Realizar simulacros de phishing para evaluar la preparación de los empleados y reforzar su capacidad de respuesta ante ataques.

NOTICIA COMPLETA

https://devel.group/blog/atacantes-afectan-a-orange-y-crowdstrike-coincidencia-o-represalia-cibernetica/

CONTACTOS DE SOPORTE

Correo electrónico: info@develsecurity.com

Teléfonos directos:

Guatemala: +(502) 2307 5757

El Salvador: +(503) 2249 4252

Honduras: +(504) 2283 5904

República Dominicana: +1 829 734 2040

WhatsApp: +(502) 5124 9536

Sitio Web: https://www.devel.group/