**ESET publica su Informe de actividad de APT, que destaca la guerra cibernética de grupos alineados con Rusia, China e Irán**

*ESET comparte un panorama general de las actividades de distintos grupos APT (amenazas persistentes avanzadas) analizados en el cuarto trimestre de 2023 y el primer trimestre de 2024.*

[ESET](https://www.eset.com/latam/), compañía líder en detección proactiva de amenazas, publicó su Informe de actividad de APT, que resume las actividades de grupos notables de amenazas persistentes avanzadas (APT) desde octubre de 2023 hasta finales de marzo de 2024. Las operaciones destacadas son representativas del panorama más amplio de amenazas que el equipo de investigación de ESET siguió durante este período, ilustrando tendencias y desarrollos clave.

**Información destacada:**

* ***Los grupos alineados con Irán aumentaron su actividad contra Israel después del ataque liderado por Hamás contra Israel en octubre de 2023 y durante la guerra en curso en Gaza.***
* ***Grupos alineados con Rusia se centraron en el espionaje dentro de la Unión Europea y en continuos ataques contra Ucrania.***
* ***Los actores de amenazas alineados con China explotaron vulnerabilidades en dispositivos de acceso público, como VPN, firewalls y software.***
* ***Los principales objetivos de la mayoría de las campañas fueron las organizaciones gubernamentales.***

Después del ataque liderado por Hamás contra Israel en octubre de 2023, y durante la guerra en curso en Gaza, ESET detectó un aumento significativo en la actividad de los grupos amenazantes alineados con Irán. Los grupos alineados con Rusia han centrado sus actividades en el espionaje dentro de la Unión Europea y los ataques contra Ucrania. Por otro lado, varios actores de amenazas alineados con China explotaron vulnerabilidades en dispositivos públicos, como VPN y firewalls, y software, como Confluence y Microsoft Exchange Server, para obtener acceso inicial a objetivos en múltiples verticales. Los grupos alineados con Corea del Norte continuaron apuntando a las empresas aeroespaciales y de defensa y a la industria de las criptomonedas.



Pie de imagen: Países y sectores objetivo

“*Los objetivos de la mayoría de las campañas fueron organizaciones gubernamentales y ciertos sectores verticales: por ejemplo, aquellos que fueron objeto de continuos e implacables ataques a la infraestructura ucraniana. Europa experimentó una gama más diversa de ataques por parte de diversos actores de amenazas. Los grupos alineados con Rusia reforzaron su enfoque en el espionaje en la Unión Europea, donde los actores de amenazas alineados con China también mantienen una presencia constante, lo que indica un interés continuo en los asuntos europeos por parte de los grupos alineados tanto con Rusia como con China*”, dice Jean-Ian Boutin, Director de Investigación de Amenazas de ESET.

Basándose en la filtración de datos de la empresa china de servicios de seguridad I-SOON (Anxun), el equipo de investigación de ESET puede confirmar que este contratista chino efectivamente se dedica al ciberespionaje. ESET rastrea una parte de las actividades de la empresa bajo el grupo FishMonger. En este último informe, ESET también presenta un nuevo grupo APT alineado con China, CeranaKeeper, que se distingue por características únicas pero posiblemente conectado por la huella digital con el grupo Mustang Panda.

En el caso de los grupos de amenazas alineados con Irán, MuddyWater y Agrius pasaron de su enfoque anterior en ciberespionaje y ransomware, respectivamente, a estrategias más agresivas que involucran intermediación de acceso y ataques de impacto. Mientras tanto, las actividades de OilRig y Ballistic Bobcat experimentaron una desaceleración, lo que sugiere un cambio estratégico hacia operaciones más notorias y “más ruidosas” dirigidas a Israel.

En cuanto a la actividad alineada con Rusia, la campaña Operación Texonto, una operación psicológica y de desinformación (PSYOP) descubierta por el equipo de investigación de ESET, difundió información falsa sobre las protestas rusas relacionadas con las elecciones y la situación en la metrópolis del este de Ucrania, Kharkiv, fomentando la incertidumbre entre los ucranianos a nivel nacional y en el extranjero.

El informe también describe la explotación de una vulnerabilidad de día cero en Roundcube por parte de Winter Vivern, un grupo que ESET considera alineado con los intereses de Bielorrusia. Además, se destaca una campaña en Medio Oriente llevada a cabo por SturgeonPhisher, un grupo que el equipo de ESET cree que está alineado con los intereses de Kazajstán.



Pie de imagen: Fuentes de ataque

*“Los productos de ESET protegen los sistemas de sus clientes de las actividades maliciosas descritas en el informe. La inteligencia recolectada se basa principalmente en datos de telemetría patentados de ESET y ha sido verificada por el equipo de investigación, quienes preparan informes técnicos detallados y actualizaciones frecuentes de actividades que detallan las actividades de grupos APT específicos. Estos análisis de inteligencia de amenazas, conocidos como ESET APT Reports PREMIUM, ayudan a las organizaciones encargadas de proteger a los ciudadanos, la infraestructura nacional crítica y los activos de alto valor de ataques cibernéticos criminales y dirigidos por estados-nación.”,* concluye Jean-Ian Boutin, Director de Investigación de Amenazas de ESET.

Los [**Informes de Actividad APT de ESET**](https://www.welivesecurity.com/es/informes/reporte-actividad-apt-cuarto-trimestre-2023-primer-trimestre-2024/) contienen sólo una fracción de los datos de inteligencia de ciberseguridad proporcionados en los Informes APT PREMIUM de ESET. Para obtener más información, visite el sitio web [de ESET Threat Intelligence](https://www.eset.com/int/business/services/threat-intelligence/?utm_source=welivesecurity.com&utm_medium=referral&utm_campaign=wls-research&utm_content=eset-apt-activity-report-q4-2023-q1-2024&sfdccampaignid=7011n0000017htTAAQ).

Para conocer más sobre seguridad informática visite el portal de noticias de ESET: <https://www.welivesecurity.com/es/informes/reporte-actividad-apt-cuarto-trimestre-2023-primer-trimestre-2024/>

Por otro lado, ESET invita a conocer [**Conexión Segura**](https://www.eset.com/latam/podcast/), su podcast para saber qué está ocurriendo en el mundo de la seguridad informática. Para escucharlo ingrese a: <https://open.spotify.com/show/0Q32tisjNy7eCYwUNHphcw>

**Visítanos en:**

  [@ESETLA](https://twitter.com/ESETLA)  [/compay/eset-latinoamerica](https://www.linkedin.com/company/eset-latinoamerica/)  [/esetla](https://www.instagram.com/esetla/)  [/ESETLA](https://www.facebook.com/ESETLA)  [/@esetla](https://www.youtube.com/%40esetla)

**Acerca de ESET**

ESET® proporciona seguridad digital de vanguardia para prevenir ataques antes de que ocurran. Al combinar el poder de la IA y la experiencia humana, ESET® se anticipa a las ciberamenazas conocidas y emergentes, asegurando empresas, infraestructuras críticas e individuos. Ya sea protección de endpoints, nube o dispositivos móviles, sus soluciones y servicios nativos de IA y basados en la nube son altamente efectivos y fáciles de usar. La tecnología de ESET incluye detección y respuesta sólidas, cifrado ultraseguro y autenticación multifactor. Con defensa en tiempo real las 24 horas, los 7 días de la semana y un sólido soporte local, mantiene a los usuarios seguros y a las empresas funcionando sin interrupciones. Un panorama digital en constante evolución exige un enfoque progresivo de la seguridad: ESET® está comprometido con una investigación de clase mundial y una potente inteligencia sobre amenazas, respaldada por centros de I+D y una sólida red global de socios. Para obtener más información, visite <https://www.eset.com/latam> o síganos en [LinkedIn](https://www.linkedin.com/company/eset-latinoamerica), [Facebook](https://www.facebook.com/ESETLA) y [Twitter](https://twitter.com/ESETLA).

**Datos de Contacto de Comunicación y Prensa**

*Para más información se puede poner en contacto a través de* ***prensa@eset-la.com*** *o al +54 11 2150-3700.*

*Copyright © 1992 – 2024. Todos los derechos reservados. ESET y NOD32 son marcas registradas de ESET. Otros nombres y marcas son marcas registradas de sus respectivas empresas.*