Cisco | Talos

REVISIÓN DEL AÑO 2022

AMENAZAS PERSISTENTES AVANZADAS

DESCARGA EL INFORME COMPLETO EN INGLÉS AQUÍ

Amenazas avanzadas persistentes (APT) patrocinadas o alineadas por el estado, adaptadas al cambiante panorama geopolítico en 2022. Cisco Talos observó varias campañas cibernéticas ofensivas vinculadas a varios grupos provenientes de Rusia, Irán, China, Corea del Norte y países del subcontinente indio. Estos grupos participaron en diversas actividades maliciosas, que incluyen espionaje, robo de propiedad intelectual e implementación de malware destructivo. Las principales tendencias observadas incluyen lo siguiente:

- Entrega de malware nuevo y personalizado y variantes actualizadas de malware conocido anteriormente.
- Aprovechamiento de vulnerabilidades conocidas públicamente, como las utilidades de Log4j.
- Actualización de herramientas y patrones de comportamiento para evadir la detección.
- Aumento de la actividad de APT en nuestros compromisos de Cisco Talos Incident Response (CTIR), incluido el grupo MuddyWater patrocinado por el estado de Irán y varias APT afiliadas a China.

Rusia

Los grupos patrocinados por el estado más activos que observó Talos en 2022, particularmente antes de que Rusia invadiera Ucrania en febrero.

Fancy Bear

Una sospechosa unidad de la agencia de inteligencia militar de Rusia, la Dirección del Estado Mayor (GRU).

- Ha utilizado tácticas, técnicas y procedimientos (TTP) similares a los observados en "WhisperGate", un ataque destructivo limpiador, varias semanas antes de la invasión.

Gamaredon

Se sospecha que es un equipo de actores apoyados por el gobierno ruso en Crimea.

- Se lanzó una campaña masiva de suplantación de identidad focalizada (spear phishing) diseñada para infectar a los usuarios del gobierno ucraniano con malware de robo de información para exfiltrar datos confidenciales.

Turla

Origen ruso, atribuido por algunos al Servicio Federal de Seguridad de Rusia (FSB).

- Sigue participando en operaciones altamente específicas contra entidades del sector público y privado en países de la OTAN y estados postsoviéticos mediante ataques a sitios web, campañas de suplantación de identidad focalizada (spear phishing), técnicas de ingeniería social, explotación de vulnerabilidades conocidas y puertas traseras personalizadas, como Crutch y Gazer.

Irán

Estos grupos realizan ataques cibernéticos a nivel mundial con el objetivo principal de robar propiedad intelectual y recopilar inteligencia. Es probable que conserven los medios técnicos para implementar ransomware y otro malware destructivo.

MuddyWater

Tras una revisión exhaustiva, creemos que MuddyWater consta de varios subgrupos encargados de dirigirse a un país o región específicos.

- Si bien cada subgrupo de MuddyWater utiliza TTP únicos para comprometer a sus objetivos designados, también comparte malware, herramientas y procedimientos que se consideran eficaces en otras campañas regionales.
- Este año, MuddyWater intentó comprometer a las entidades gubernamentales turcas e implementó un nuevo implante denominado SloughRAT en el Medio Oriente.
- En función de las interacciones de CTIR, observamos una gran cantidad de herramientas de puerta trasera y posteriores a la explotación en uso. Incluso después de la corrección, encontramos la presencia de puertas traseras adicionales en la infraestructura del servidor y el uso de Impacket para la ejecución de servicios remotos y herramientas de ataque.

© 2023 Cisco y/o sus filiales. Todos los derechos reservados.

AMENAZAS PERSISTENTES AVANZADAS

China

Los agentes de APT vinculados a China se centraron en entidades de una amplia variedad de mercados verticales de la industria, y roban propiedad intelectual y datos confidenciales de industrias clave y sectores de infraestructura crítica que se alinean con los objetivos estratégicos de China.

Mustang Panda

Conocido por aprovechar los eventos actuales para comprometer a las víctimas, particularmente en los EE. UU. y Asia.

- Aprovechó la guerra entre Rusia y Ucrania para atacar a las organizaciones europeas, incluidas las entidades rusas, en una campaña de espionaje generalizada.

Deep Panda

Un grupo independiente de ciberespionaje patrocinado por el estado que está dirigido a gobiernos, ejércitos, servicios públicos y organizaciones financieras.

- Aprovechó la vulnerabilidad de Log4j para comprometer una entidad de servicios de salud y, luego, implementó una puerta trasera personalizada para establecer la persistencia.

Corea del Norte

Talos observó una prolífica actividad de los agentes de amenazas vinculados al gobierno de Corea del Norte, en particular el grupo Lazarus, que respalda los objetivos políticos y de seguridad nacional a través del espionaje, el robo de datos y los ataques disruptivos.

Grupo Lazarus

Conocido por utilizar malware personalizado y cometer robos monetarios generalizados.

- Aprovechó las vulnerabilidades de Log4j en los servidores públicos de VMware Horizon para atacar a las empresas de energía ubicadas en los Estados Unidos, Canadá y Japón.
- Talos descubrió un nuevo troyano de acceso remoto, al que denominamos MagicRAT, así como otros implantes personalizados utilizados para el reconocimiento interno y el robo de datos.

Sur de Asia

Talos rastreó numerosas campañas dirigidas principalmente a entidades en la India, la mayoría de las cuales parece provenir de actores vinculados al estado en Pakistán, un adversario regional desde hace mucho tiempo.

Transparent Tribe

- Se dirige principalmente a entidades gubernamentales y militares, y a organizaciones afiliadas en Afganistán e India. El grupo comenzó a apuntar a estudiantes e instituciones educativas en la India, en lo que parece ser una expansión de su victimología estándar.

APT Bitter

- El espionaje parece ser el principal objetivo de este grupo. En una campaña de larga duración, sus ataques se dirigieron a los gobiernos y entidades del sur y el este de Asia en los sectores de energía e ingeniería.

Otras APT

- A principios de este año, Talos publicó una investigación que sugiere que varios agentes de APT que operan en el sur de Asia habían reutilizado el código de VBA escrito por diferentes grupos de amenazas, posiblemente sin intención.

© 2023 Cisco y/o sus filiales. Todos los derechos reservados.