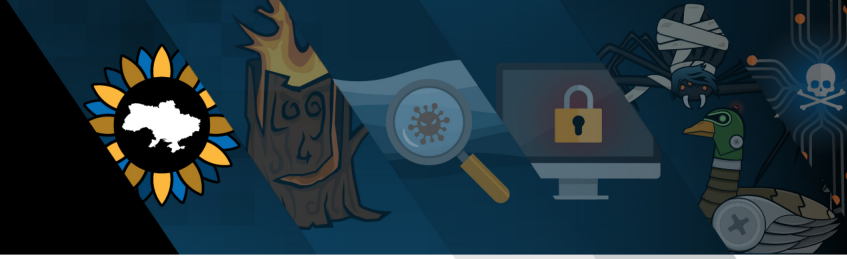
Talos

REVISIÓN DEL AÑO 2022

UCRANIA



DESCARGA EL INFORME COMPLETO EN INGLÉS AQUÍ

El soporte continuo de Talos para Ucrania ha sido un gran enfoque de nuestros esfuerzos operativos este año. Impulsado por nuestra misión principal de proteger a la gente y la infraestructura de Ucrania, Talos lanzó un grupo de trabajo de más de 40 voluntarios dedicados a defender a nuestros clientes y partners. Este equipo de expertos monitorea a los clientes de infraestructura crítica para identificar amenazas, corregir ataques y recopilar información.

PRINCIPALES ADVERSARIOS Y AMENAZAS

La siguiente lista representa una instantánea de los adversarios y las amenazas que Talos observó que apuntaban a las entidades ucranianas y sus aliados en 2022:

- Antes y después de la invasión, vimos una variedad de limpiadores destructivos y otro malware contra objetivos ucranianos, incluidos WhisperGate, HermeticWiper, CaddyWiper, DoubleZero y CyclopsBlink.
- Los delincuentes cibernéticos aprovecharon la situación al anunciar herramientas cibernéticas ofensivas que en realidad eran malware para apuntar a entidades rusas y utilizaron señuelos de correo electrónico con temas relacionados con la crisis para realizar estafas financieras y entregar troyanos de acceso remoto.
- El grupo patrocinado por el estado ruso Gamaredon distribuyó malware de robo de información y un presunto actor patrocinado por el estado intentó un intento de ataque a la cadena de suministro denominado GoMet.
- El actor de amenazas con sede en China, Mustang Panda, llevó a cabo campañas de suplantación de identidad contra entidades en Europa y Rusia utilizando documentos “oficiales” falsos como señuelos.
- El grupo hacktivista alineado con Rusia, Killnet, lanzó ataques de denegación de servicio contra sitios web dentro de países pro-Ucrania.

TENDENCIAS DE COMPORTAMIENTO

Según los datos que hemos recopilado desde principios de 2022, hemos visto las siguientes tendencias indicativas de comportamientos del adversario activos en Ucrania:

- Las utilidades comunes, como PowerShell y Windows Management Instrumentation (WMI), siguen siendo el principal objetivo de los adversarios que buscan la “consecución del negocio” y evadir la detección.
- Se observaron en mayor número técnicas tales como el uso de ejecutables de Google Chrome y el uso de claves de políticas de Windows para establecer la persistencia.

Figura 1: *Principales ataques cibernéticos contra Ucrania.*

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

UCRANIA

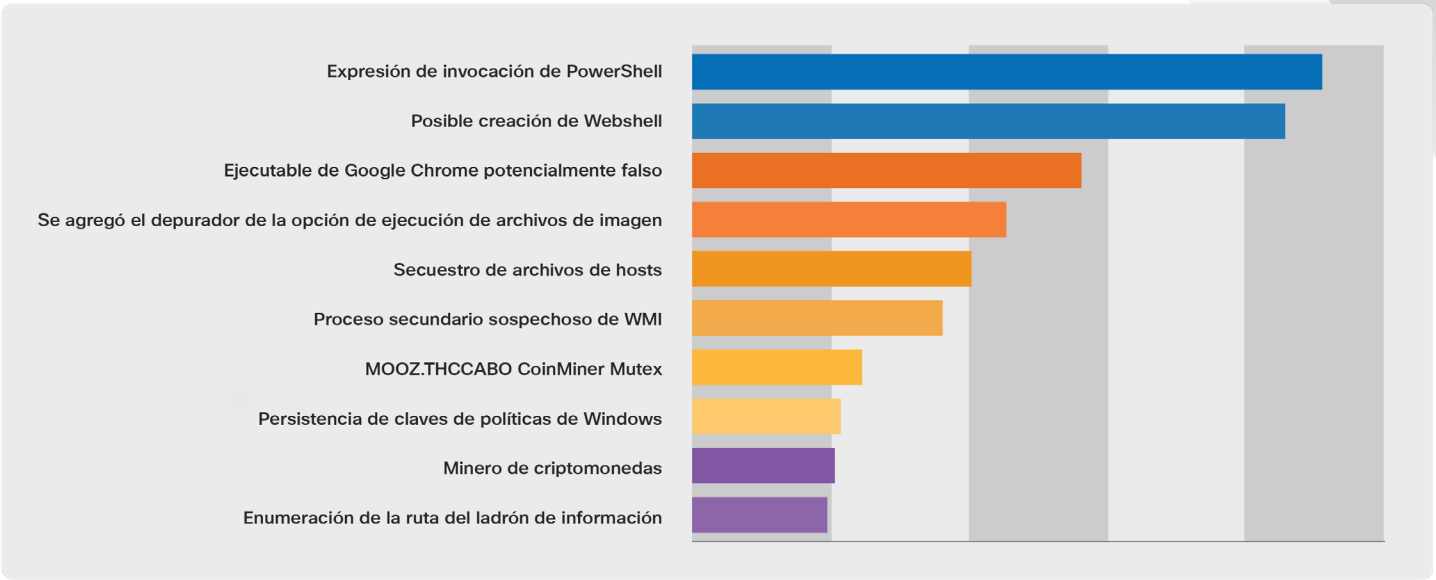


Figura 2: *La mayoría de las reglas de protección de comportamiento activas de Cisco Secure Endpoint en los clientes ucranianos donde se ha implementado Cisco Secure Endpoint.*

- Se observó un aumento en las detecciones de ladrones de información y mineros de criptomonedas. Sin embargo, vemos actores de todo el espectro de la sofisticación con la actividad destructiva como objetivo principal.
- Hemos observado un aumento en las alertas de "ejecución del proxy binario firmado mediante rundll32" en Ucrania, pero también a nivel global. Esta técnica abusa de la biblioteca de enlaces dinámicos (DLL) para ejecutar código malicioso.

A pesar del aumento de la actividad contra los objetivos en Ucrania, nuestro equipo de respuesta ante incidentes observó menos amenazas contra los clientes de Cisco en general durante la primera mitad de 2022. Es posible que el conflicto haya atraído a agentes de amenazas que, de lo contrario, estarían realizando ataques en otros lugares.

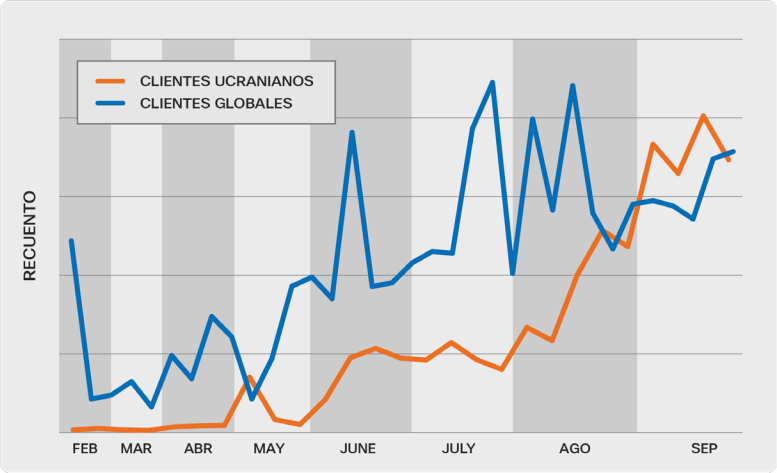


Figura 3: *Detecciones de prevención de exploits para la "ejecución del proxy binario firmado mediante rundll32" en clientes ucranianos y clientes globales, de febrero a septiembre 2022.*

CONCLUSIÓN

No hay indicios de que la cadencia de los ataques cibernéticos contra Ucrania se esté ralentizando ni el conflicto cibernético terminará necesariamente con el cese de las hostilidades. Las tensiones regionales y la diversidad de los agentes de amenazas involucrados en el conflicto sugieren que los ataques contra Ucrania probablemente continuarán. Además, evaluamos que los agentes de amenazas cibernéticas rusas probablemente llevarán a cabo ataques destructivos según sea necesario para afectar el resultado de la guerra.

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