Publicado en Madrid el 04/08/2022

# [Nozomi Networks Labs reports: Wipers e IoT Botnets dominan el panorama de las amenazas OT/IoT](http://www.notasdeprensa.es)

## En el primer semestre de 2022, el conflicto entre Rusia y Ucrania ha aumentado el número de dispositivos conectados y las redes de bots IoT de los ciberdelincuentes han tenido un mayor impacto en el panorama de las amenazas a los Sistemas de Control Industrial (ICS)

 El último informe de seguridad OT/IoT de Nozomi Networks Labs destaca que el malware wiper, la actividad de redes de robots IoT y la guerra entre Rusia y Ucrania influyeron en el panorama de las amenazas en la primera mitad de 2022. Desde que Rusia comenzó su invasión de Ucrania en febrero de 2022, los investigadores de Nozomi Netwlorks Labs vieron actividad de diferentes tipos de actores de amenazas, incluyendo hacktivistas, amenazas avanzadas persistentes (APTs) de estados nación y cibercriminales. También observaron un gran uso del malware wiper y fueron testigos de una variante de Industroyer, denominada Industroyer 2, desarrollada para abusar del protocolo IEC-104, que se utiliza habitualmente en entornos industriales. Además, en la primera mitad del 2022, la actividad de la red de bot IoT maliciosos fue en aumento, tanto en número como en sofisticación. Nozomi Networks Labs Nozomi Networks Labs estableció una serie de honeypots o señuelos para atraer a estas redes de bots maliciosas y capturar su actividad con el fin de proporcionar información adicional sobre cómo los cibercriminales se dirigen a los entornos IoT.  En esta investigación, los analistas de Nozomi Networks Labs descubrieron la creciente preocupación por la seguridad tanto de las contraseñas codificadas como de las interfaces de Internet para las credenciales de los usuarios finales. Desde enero a junio de este año, los señuelos de Nozomi Networks detectaron que: Marzo fue el mes más activo con cerca de 5.000 direcciones IP de atacantes únicas recogidas. Las principales direcciones IP de los atacantes estaban asociadas a China y Estados Unidos. Las credenciales "root" y "admin" fueron el objetivo más frecuente y se utilizaron en múltiples variaciones para que los cibercriminales accedieran a todos los comandos del sistema y a las cuentas de usuario.  En el área de las vulnerabilidades, industria y energía continúan siendo los sectores más vulnerables, seguidos de salud e instalaciones comerciales. En el primer semestre de 2022: La CISA lanzó 560 notificaciones de Vulnerabilidades y Exposiciones Comunes (CVEs), un 14% menos que en el segundo semestre de 2021 El número de proveedores afectados aumentó un 27% Los productos afectados también aumentaron un 19% respecto al segundo semestre de 2021 "Este año el panorama de ciberamenazas es complejo", comenta Roya Gordon, evangelista investigador de Seguridad OT/ioT de Nozomi Networks. "Muchos factores como el número creciente de dispositivos conectados, la sofisticación de los actores maliciosas y los cambios en las motivaciones de los ataques, están aumentando el riesgo de una brecha o un ataque ciberfísico. Afortunadamente, las defensas de seguridad también están evolucionando. Ya hay soluciones disponibles para dar visibilidad de la red a las organizaciones de infraestructuras críticas; la detección dinámica de amenazas y la inteligencia accionable que necesitan para minimizar el riesgo y maximizar la resiliencia." El informe "OT/IoT Security Report" de Nozomi Networks ofrece a los profesionales de la seguridad los últimos conocimientos necesarios para reevaluar los modelos de riesgo y las iniciativas de seguridad, junto con recomendaciones prácticas para proteger las infraestructuras críticas. Este último informe incluye: Un análisis del estado actual de la ciberseguridad Las tendencias del panorama de amenazas y soluciones para afrontarlas Un resumen de la crisis Rusia/Ucrania, destacando las nuevas herramientas maliciosas y el malware relacionado con el conflicto Insights de las redes de bots IoT, sus correspondientes indicadores de compromiso (IoCs) y las técnicas, tácticas y procedimientos (TTPs) de los cibercriminales Recomendaciones y un análisis de previsiones.

**Datos de contacto:**

Axicom

91 661 17 37

Nota de prensa publicada en: [https://www.notasdeprensa.es/nozomi-networks-labs-reports-wipers-e-iot](http://www.notasdeprensa.es/educalivecom-disfruta-de-cursos-presenciales-y-clases-particulares-a-traves-de-internet)

Categorias: Telecomunicaciones Logística E-Commerce Ciberseguridad Otras Industrias



[**http://www.notasdeprensa.es**](http://www.notasdeprensa.es)