EL MERCADO DE LAS CIBERARMAS HOYO NEGRO DE LA TECNOLOGÍA

Dr. Roberto Morales Estrella
Profesor Investigador de la UAEH

08 abril de 2024

En nuestra entrega de “la tecnología al servicio de los genocidas” (Morales, Estrella , OtecH, 2023) hablamos de cómo Israel realizó un ciberataque contaminando el agua para consumo humano de los palestinos, mientras que Hamás dañó páginas de internet israelíes; así mismo en nuestra entrega denominada “La nueva industria de ciberseguridad y la hegemonía global” (Morales, Estrella, 2023) se mencionó que la industria de la ciberseguridad es tan amplia como la vulnerabilidad, de todos los usuarios de la tecnología, es decir toda la sociedad.

El mercado de las ciberarmas, está determinado por los ciberdelinecuentes, hackers y mercenarios, es un mercado que representa el 1,5 del PIB Mundial, más de un billón de dólares (itDigitalSecurity, 2023) el doble de lo que se maneja por las drogas, la trata de personas, y el tráfico ilegal de armas de fuego; los conflictos geopolíticos, las innovaciones científico-tecnológicas, los genocidios (como el de Israel contra los Palestinos y el de Ruanda) y el ciberespionaje; son las condiciones que han propiciado la formación del mercado de ciberarmas, es un negocio de la muerte y la extinción.

La cibertecnología no es perfecta, ya que registran fallos y vulneravilidades, mismas que son identificadas por los hackers, quienes, según el Nuevo Diccionario de hackers (editors, 2002), son aquellas personas que enfrentan el desafío de superar las limitaciónes tecnológicas; por lo común los consideramos cibercriminales, que utilizan sus capacidades para hacer daño, o para ganar dinero, son los hackers de sombrero negro o mercenarios, que operan sin ética, pero también hay hackers de sombrero blanco.

Los documentos que divulgó Snowden, contenían entre otras cosas un listado de los hackers de la Agencia de Seguridad Nacional de los EEUU (NSA) con acceso a cualquier pieza de hardware comercial (Perlrot, 2022), tenían plenamente localizados los fallos y las vulnerabilidades, lo que les facilitó identificar los puntos de entrada, a cualquier dispositivo o sistema informático, esos puntos de entrada se denominan “día cero”, se les llama así porque cuando se identifican, se tienen día cero para solucionarlos.

Para Kaspersky (Kaspersky, 2024), día cero describe las vulnerabilidades de seguridad, con cero días para corregirlas; los cibercriminales se aprovechan, ya sea para secuestrar información o para venderlos, los días cero se convirtieron en una ciberarma y un producto de mercado, al mejor postor, su aplicación es sin duda con la menor regulación y obvio ningún tipo de ética.

Lo anterior se complementa con el descubrimiento del virus malware, llamado Stuxnet, por parte de la empresa bielorrusa VirusBlockAda (Silva, 2018), este software malicioso tiene la capacidad de superar las fronteras virtuales, para impactar en todo lo tangible, convirtiéndose en una ciberarma de alta letalidad por su capacidad de destrucción en los sectores industriales, puesto que opera a través de pendrive (memoria usb) y no internet, para infectar la infraestructura industrial, que usan programas fabricados por Siemens, sistemas operativos de windows llamados SCADA (Supervisory Control and Acquisition Data) como lo hizo en 2010 afectando a 100 mil industrias, el 60% de ellas de Irán, e Indonesia; este tipo de sistemas lo utilizan los equipos de naciones como Alemania, China y Finlandia, cabe precisar que ataca configuraciones con PLC (Controladores Lógicos Programables).

La infraestructura tecnológica global es ya objeto de una carrera, para ser parte de la hiperconectividad, el modo más fiable para insertarse, es mediante las virus, fallos y vulnerabilidades de día cero, tanto el gobierno de los EEUU, como Rusia, China, Israel, Corea del Norte, entre otros, hackers-espías y cibermercenarios, han hecho de la acumulación de días cero, como del software Pegasus (creado por la empresa israelí NSO-Group) un mercado, al servicio del crimen organizado, como de gobiernos dictatoriales, para aplicarlos en contra de sus disidentes y reprimirlos.

Más allá de los virus y troyanos, la tecnología transformada en ciberarmas, como las llamadas “Lavender y The Gospel” (Jalife Rahme, 2024) basadas en Inteligencia Artificial, las está aplicando, el Israel de Nentanyahu, masacrando a miles de niños y mujeres, con el propósito de extinguir a los palestinos, la primera arma es para marcar a los palestinos y la segunda para destruir sus inmuebles, todas éstas terroríficas ciberarmas, son la avanzada de una sociedad distópica.

Bibliografía

editors, V. (enero de 2002). Dominio Público. Obtenido de dominiopublico.gov.br: http://www.dominiopublico.gov.br/download/texto/gu003008.pdf

itDigitalSecurity. (2 de junio de 2023). itDigitalSecurity. Recuperado el abril de 2024, de itdigitalsecurity.es: https://www.itdigitalsecurity.es/actualidad/2023/06/el-valor-del-cibercrimen-se-aproxima-al-15-del-pib-mundial

Jalife Rahme, A. (7 de abril de 2024). Lavender: la Inteligencia Artificial de Israel para aniquilar a marcados palestinos civiles. La Jornada Internet, pág. https://www.jornada.com.mx/2024/04/07/opinion.

Kaspersky. (1° de abril de 2024). Kaspersky. Obtenido de latam.kaspersky.com: https://latam.kaspersky.com/resource-center/definitions/zero-day-exploit

M. R. (27 de noviembre de 2023). OtecH. Recuperado el abril de 2024, de otech.edu.mx: https://otech.uaeh.edu.mx/noti/index.php/articulo-otech/la-nueva-industria-de-la-ciberseguridad-y-la-hegemonia-global/

M. R. (17 de octubre de 2023). OtecH. Recuperado el abril de 2024, de otech.uaeh.edu.mx: https://otech.uaeh.edu.mx/noti/index.php/articulo-otech/la-tecnologia-al-servicio-de-genocidas-la-guerra-israel-hamas/

Perlrot, N. (2022). Así es como me dicen que acabará el mundo: La carrera armamentística cibernética. México, Cd de México , México : Ediciones Urano, S.A. U.

S. F. (21 de abril de 2018). Revista Pontificia Universidad Católica del Ecuador. Recuperado el abril de 2024, de revistapuce.edu.ec: https://www.revistapuce.edu.ec/index.php/revpuce/article/view/141