DIARIO INDEPENDIENTE DE INFORMACIÓN GENERAL
LA RAZÓN
EDICIÓN NACIONAL

Fecha: 26/01/2024 Audiencia: 262.545 Sección: CULTURA
Vpe: 22.656 € Tirada: 75.013 Frecuencia: DIARIO
Vpe pág: 24.929 € Difusión: 51.373
Vpe portada: 45.460 € Ocupación: 90,88%

Ciencia

La Inteligencia Artificial y las guerras disparan los ciberataques

En 2023 los ataques de hackers no solo crecieron, también han cambiado los objetivos. Se abre una nueva era en la que todo vale. No basta el dinero, ahora se ataca estructuras críticas como hospitales para generar el caos

Eva M. Rull. MADRID

Vamos a ver cada vez más fraudes relacionados con las deep fakes y con la IA generativa. Con la inteligencia artificial crecen los ciberataques y aumenta su sofisticación y los costes en ciberseguridad aumentarán tanto en ámbito empresarial como público», Con estas palabras Dorit Dor, directora de tecnología de Check Point Software Technologies se expresaba en una entrevista retransmitida durante el reciente Foro Económico de Davos (Suiza). La ciberseguridad ha centrado un año más parte de las conversaciones de esta reunión anual en un momento en el que los ciberataques crecen en todo el mundo.

«En 2023 ha habido un boom de ataques; ha sido un año muy caótico también debido a los conflictos (de hecho, el ataque de Hamas se explica por un ciberataque anterior que tumbó los sistemas de seguridad de Israel, la llamada cúpula de hierro). Lo importante de 2023 es que hasta este año los delitos se cometían contra empresas o contra la administración. Ahora se ha saltado una línea roja y se empiezan a producir ataques a estructuras críticas como los hospitales. Un ejemplo es el ataque que sufrió en Hospital Clínic de Barcelona; muchos pacientes no pudieron ser operados y cientos de datos privados aparecieron en la dark web. Se ha publicado algún informe que apunta a que han aumentado hasta un 78% los ataques en el sector sanitario. Ahora todo vale. Lo hemos visto también con el ataque a Air Europa. La compañía tuvo que pedir a 100.000 clientes que cancelaran sus tarjetas», comenta Óscar Quero, director del Máster de Ciberseguridad de OBS Business School.

Números de 2023

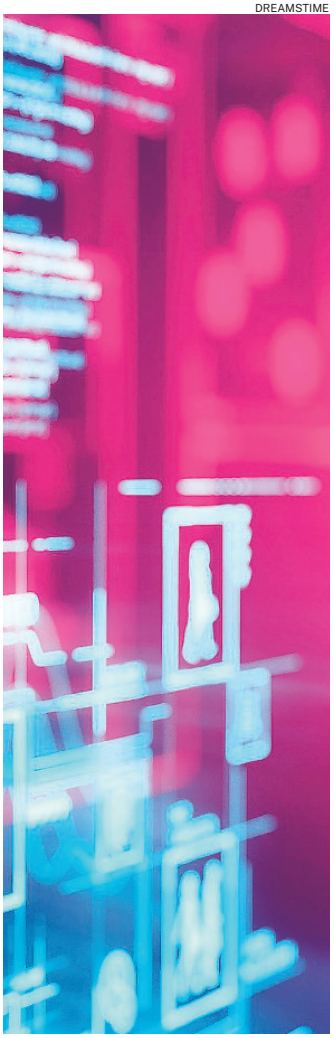
A nivel global se calcula que «hay entre 90 y 100 millones de ciberataques al año. En España según nuestros datos, en 2021 hubo 109.000 incidencias, en 2022 estas subieron un 10% hasta alcanzar las 118.000 y la previsión es que en 2023 hayan aumentado. En cuanto a las tipologías de delitos, un tercio lo que buscan es dinero a través de la extorsión para la recuperación de datos o a través de la venta en la dark web. En esta categoría está el phishing o las suplantaciones, pero también el malware, que es el software malicioso, supone entre el 20 y el 25% de los delitos», detalla Marcos Gómez Hidalgo, subdirector del Centro de Respuesta a Incidentes de Seguridad del Instituto Nacional de Ciberseguridad (INCIBE, centro que trabaja con el sector privado y la ciudadanía).

Basta echar una ojeada por Google para darse cuenta de que los hackeos con robos de identidad, datos, estafas y fraudes están a la orden del día. Microsoft empezó el año con un ataque de hackers rusos que han accedido a emails corporativos, algunos del personal de ciberseguridad En 2023 ha habido casos de todo tipo como el de la British Library que perdió el acceso público a todos sus fondos digitales. En España, «han sido atacados muchos ayuntamientos, quizás el caso más sonado ha sido el de Sevilla. También intrusiones en ministerios, el robo de información del Registro de Mascotas,

DIARIO INDEPENDIENTE DE INFORMACIÓN GENERAL
LA RAZÓN
EDICIÓN NACIONAL

Fecha: 26/01/2024 Audiencia: 262.545 Sección: CULTURA
Vpe: 22.581 € Tirada: 75.013 Frecuencia: DIARIO
Vpe pág: 24.929 € Difusión: 51.373
Vpe portada: 45.460 € Ocupación: 90,58%

DREAMSTIME



ChatGPT se ha convertido en la plataforma que más rápido ha crecido. En cinco días alcanzó el millón de usuarios

Si el cibercrimen fuera un país, sería la tercera economía más grande del mundo, dice Forbes

Tras la aparición de ChatGPT han salido dos herramientas de IA generativa para cometer delitos

En detalle

Los grupos de hackers más peligrosos

NoName057, de origen ruso, ha sido uno de los grupos más activos en 2023. Entre los ataques más destacados que se les asigna está el que sufrió el Ministerio del Interior de España durante la jornada electoral.
Revil, también rusos, desde 2019 se centran en cifrar archivos e información y piratear sistemas para luego pedir un rescate. Se les acusa de haber robado planos de productos de Apple antes de su lanzamiento, datos de Lady Gaga e información al ejército de los EE UU.
Dark Side, especializado en ataques ransomware, protagonizó el ataque a la red Colonial en 2021 y dejó a EE UU sin poder suministrar hasta un 31% de gasolina a coches y aviones. Se definen como apolíticos y dicen tener un código ético por el que les impide atacar hospitales, universidades, etc. Además, hacen donaciones con lo que recaudan.
Lazarus, de Corea del Norte. Se les ha vinculado con el famoso ataque WannaCry. El caso, ocurrido en 2017, ha sido considerado el mayor ataque informático del mundo. Infectó más de 230.000 ordenadores en 180 países. Se calcula que los estafadores ingresaron unos 100.000 dólares de más de 300 transacciones, pero provocaron pérdidas de más de 100 millones de euros, según Deloitte.

medios de comunicación, y empresas», cuenta Rafael Palacios, jefe de estudios de Ingeniería de Telecomunicación de ICAI y del Máster en Ciberseguridad de la Universidad Pontificia Comillas.

Fraud GPT

La IA ha venido a complicar aún más las cosas y ya hay quien considera que va a aumentar el número de hackers. Y lo cierto es que desde la aparición de herramientas como Chat GPT, la mención al uso de IA generativa con fines oscuros se ha disparado en la dark web (como se ve en el gráfico). La IA generativa es capaz de escribir código malicioso y convertirse en el compañero silencioso de cualquier hacker. De hecho, a la popular herramienta para crear textos le ha salido un gemelo perverso: el FraudGPT, capaz de crear correos electrónicos falsos pero muy convincentes o páginas web para phishing (es decir, para obtener datos a través del engaño). Otra aplicación de IA generativa es WormGPT que sirve también para crear correos de phishing de forma sencilla. También pueden servir para crear malware, es decir, software que provoca infecciones y fallos en los dispositivos o ayudar a crear documentos, facturas o solicitudes de pago fraudulentas.

Teniendo esto en cuenta no es de extrañar que la revista Forbes indique que los costes de ciberseguridad de las empresas aumentarán de 8.000 millones de dólares a 10.500 millones para 2025. «La ciberseguridad ya representa el 12% de los presupuestos en TI».

Activismo e ingeniería social

Los expertos consultados coinciden en señalar varios motivos por los que los ciberatques aumentan cada año. El primero es tan simple como que a mayor número de dispositivos, más vulnerabilidad. Solo en el ámbito empresarial y siguiendo Forbes. «La cantidad de dispositivos de las redes corporativas está creciendo exponencialmente y se espera que alcancen los 27.000 millones en 2025».

La misma publicación asegura que si el cibercrimen fuera un país, ya sería la tercera economía más grande del mundo, superada por Estados Unidos y China y es que otro de los motivos por los que el cibercrimen aumenta es el económico. Se monetiza la venta de información en la dark web o se pide dinero saboteando redes. Aunque, como señala el profesor de la OBS, Óscar Quero, pagar un rescate no siempre asegura que se eviten los daños ni que los delincuentes no vendan igualmente los datos. Existe, además, un tipo de rescate que sale especialmente rentable y que tiene que ver con las llamadas «vulnerabilidades tipo cero», aquellas fragilidades de los sistemas, los dispositivos o las redes que todavía no han sido detectadas por el fabricante. Por ejemplo, cuando sale al mercado un nuevo móvil puede que haya algún fallo de seguridad que no ha sido detectado en las pruebas. Por eso se llama de día cero porque no está cubierta por el fabricante. Para estos casos existen hasta grupos de investigadores y de hackers éticos que se dedican a detectar estos problemas y ayudar a las empresa a subsanarlos antes de que caigan en malas manos.

Con el aumento de los conflictos armados (se considera que estamos en el momento histórico con más conflictos abiertos desde la Segunda Guerra Mundial) también aumenta el hacking relacionado con el activismo político (que se convierte en la otra gran tendencia en ciberseguridad para los próximos 10 años, junto a la IA). Los hackers optan, en este caso por ataques híbridos centrados en parar servicios y crear caos bancario o en el transporte, además de obtener dinero. Una última causa es la falta de técnicos cualificados. «El 70% de los encuestados dijo que sus organizaciones no tienen suficiente personal , lo que provoca una aplicación de parches más lenta en sistemas críticos», señalaba un informe publicado en la web de Davos del año pasado.

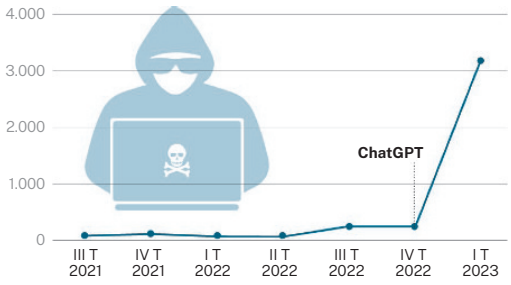
¿Es posible protegerse?

Además de phishing y malware, cada vez es más habitual «el uso de la ingeniería social. El ser humano es social. Si consigues la confianza de una persona empiezas a obtener información gratis. Es un problema que se da también en las compañías. Si recibes un mail de Recursos Humanos que parece real y pides a la gente que rellene datos, hay un porcentaje que lo hará. Esto se evita con formaciones y hacking ético, por ejemplo contratando un phishing para ver quién cae. La ingeniería social provoca mucho sentimiento de urgencia. Lo que quieren es que no pienses y actúes, te crean alarmas como que te han robado en tu cuenta, pero sabemos que un banco nunca te va a mandar un SMS. Hay que ser conscientes de que no tenemos que regalar nuestra información ni datos. Hay gente que te llama para conseguir ciertas palabras y con tu voz puede cometer un delito de suplantación de identidad», dice Quero de la OBS. Otra clave de actuación nos la da Rafael Palacios de Comillas: «Los ciudadanos nos debemos proteger aplicando las actualizaciones en nuestros ordenadores y móviles. Por ejemplo, iPhone ha publicado la versión 17.3 de iOS hace días, ¿cuántos usuarios la han instalado ya? El segundo punto es tener copias de seguridad».

EL USO DE IA GENERATIVA CON FINES NEFASTOS

Es un tema cada vez más popular en la web oscura después del lanzamiento de ChatGPT.

Número de menciones de la IA generativa en la web oscura



Fuente: Rapid7, Bain & Company

Infografía LA RAZÓN

120
número de incidentes críticos en España en 2023 (fueron 75 en 2022), según el CCN-CERT

27.000
millones de dispositivos estarán conectados a las redes corporativas en 2025 según Forbes

25%
de los delitos tienen que ver con el malware, es decir, con software malicioso