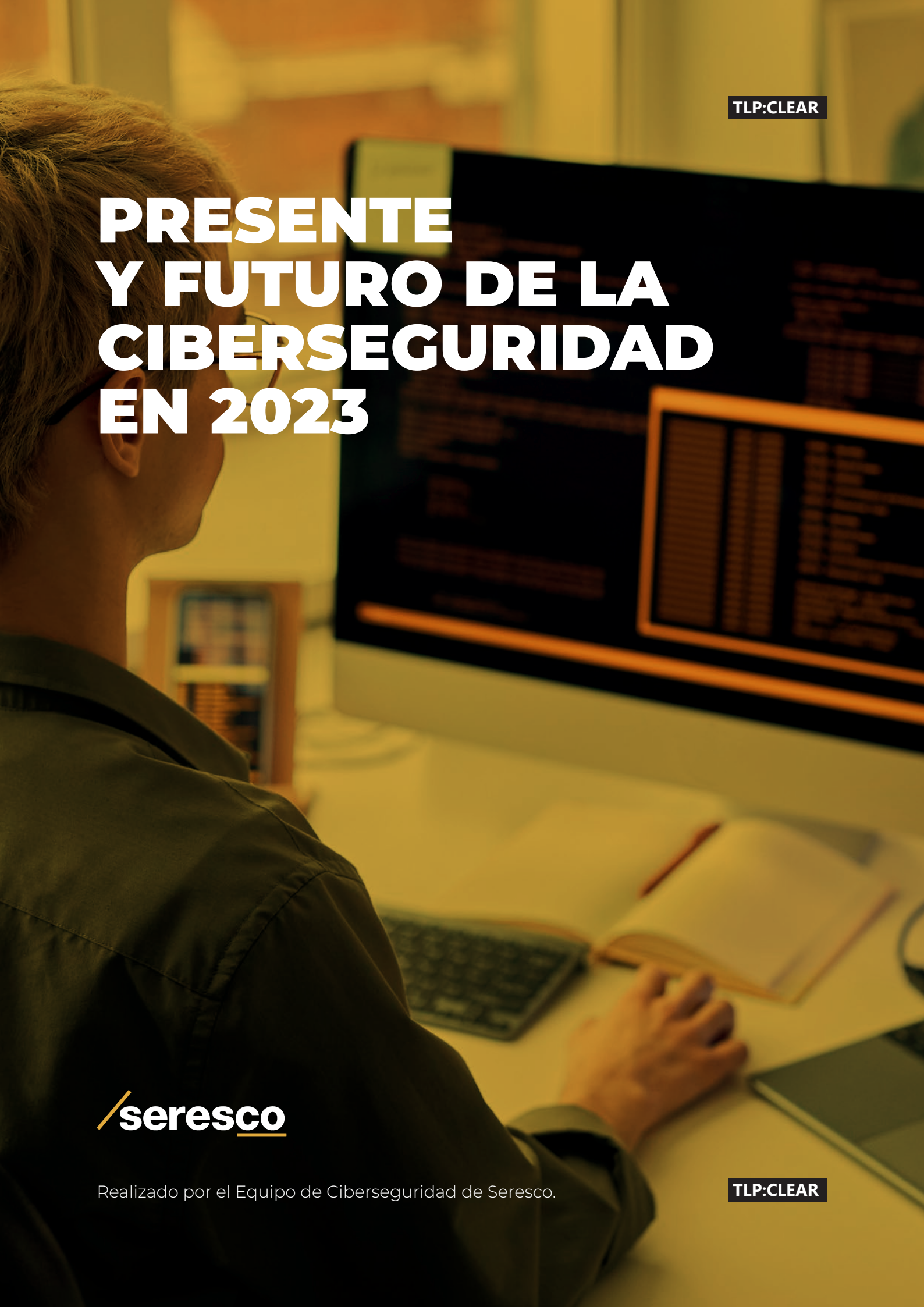
TLP:CLEAR

PRESENTE Y FUTURO DE LA CIBERSEGURIDAD EN 2023



seresco

Realizado por el Equipo de Ciberseguridad de Seresco.

TLP:CLEAR

ÍNDICE

CONSIDERACIONES INICIALES

El presente informe pretende, en primer lugar, resumir de la forma más breve —pero completa— posible el **panorama de amenazas que hemos vivido en el año 2022,** analizando sus sucesos y tendencias y comparándolas con lo que veníamos observando en años anteriores. Así, desde una visión general e histórica, podemos destacar aquellas novedades, cambios y variaciones que hemos visto respecto al 2021, al igual que tendencias y aspectos clave que se han ido desprendiendo en este último año.

En segundo lugar, y teniendo en cuenta dichas líneas y tendencias detectadas a lo largo de 2022, se tratarán de combinar con el contexto social en el que vivimos para tratar de lanzar ciertas **previsiones para el 2023.** En todos los casos se realiza una exposición de previsiones con el mayor grado de certeza posible, siendo todos ellos puntos de vista realmente interesantes para tener en consideración en los próximos meses y siempre desde el punto de vista y experiencia de Seresco de acuerdo con las observaciones realizadas por el equipo de ciberseguridad.

Se ha de tener en cuenta que, tanto las valoraciones como las previsiones, están totalmente fundamentadas en la evidencia recopilada por fuentes propias y de terceros. Una vez realizado un metaanálisis de diferentes estudios acerca del panorama de amenazas en el 2022, de lo observado y recopilado internamente en este periodo, de las predicciones de expertos en la materia para el 2023 e, igualmente, de lo que desde Seresco consideramos particularmente más probable, se ha elaborado el informe reuniendo lo más reseñable.

¿QUÉ HA OCURRIDO EN EL 2022?

CRECIENTE IMPACTO DE LA GEOPOLÍTICA EN EL PANORAMA DE AMENAZAS DE CIBERSEGURIDAD

EL CONFLICTO ENTRE RUSIA Y UCRANIA

La guerra en la frontera oriental de Europa ha remodelado el panorama de amenazas de ciberseguridad. Se ha observado una notoria concentración de **ciberactividad en torno a acciones militares cinéticas,** como preparación o complemento a ataques físicos de corte militar.

En la cara opuesta de la moneda, se ha notado un **creciente papel defensivo de las empresas tecnológicas** en las operaciones cibernéticas durante los conflictos con algunas grandes empresas de tecnología tomando partido y apoyando a Ucrania en el frente de la guerra cibernética, destacando Microsoft y AWS.

ATAQUES CONTRA LA DISPONIBILIDAD Y CON FINES DESTRUCTIVOS

Han sido ampliamente implementados **ataques contra la disponibilidad** —tanto DDoS como disruptivos— y de desinformación, utilizados antes del contacto físico como actividad preparatoria a la invasión. Estos recursos se han convertido en una faceta más de los conflictos geopolíticos, utilizados directamente como herramientas de guerra cibernética.

Según avanzaba el conflicto entre Rusia y Ucrania ha sido tónica habitual la sucesión de **ciberataques con fines destructivos apuntando a Infraestructuras Críticas,** concretamente del sector energético. Han sido ampliamente utilizados, con este fin, toda una ramificación de malware de tipo wiper con la intención de destruir datos y afectar su operativa.

MOVILIZACIÓN DEL CIBERCRIMEN Y NUEVA OLA DE HACKTIVISMO

Gran presencia y actuación de **grupos organizados, de todas las partes del mundo,** tomando partido en el conflicto según los intereses geopolíticos de alguna de las partes, así como la proliferación de toda clase de acciones de grupos hacktivistas. La coordinación de estos grupos ha tenido lugar, sobre todo, vía Telegram, donde han podido, de forma fácil, unirse, participar y descargar herramientas.

Si bien tenemos el ejemplo perfecto en el contexto de Rusia y Ucrania, no es aquí el único conflicto en el que ha habido una **gran movilización** de ejércitos de voluntarios cibernéticos, de grupos hacktivistas, de cibercriminales y de grupos patrocinados por Estados.

GRUPOS DE CIBERDELINCUENTES PATROCINADOS POR ESTADOS PARTICIPAN EN LOS CONFLICTOS

Ha habido una gran presencia de **ataques y actores patrocinados por Estados.** Muchos Estados, para poder realizar ciertos ataques desvinculándose de su autoría, han recurrido a la promoción de una larga serie de grupos ATP para llevarlos a cabo. Hay gran prominencia de **ataques destructivos** producto de estas operaciones estatales.

A medida que crecen las tensiones geopolíticas entre Estados han ido aumentando las operaciones cibernéticas, pero no sólo en Europa. Se ha producido un incremento de ataques a entidades en **Israel, EEUU, Oriente Medio y África del Norte,** adoptando ransomware y operaciones de información 'lock-and-leak'. La búsqueda de Inteligencia de las distintas organizaciones gubernamentales ha sido una nota predominante.

DESINFORMACIÓN A GRAN ESCALA

La desinformación es omnipresente en muchas áreas habituales de la sociedad, pero es en el plano geopolítico en el que más repunta. En los llamados ***social media*** se prioriza más el tráfico y el volumen de usuarios que mueven datos, antes que la fiabilidad o rigurosidad de la información. Es por esto por lo que se promociona la información que más espectadores genere, muchas veces sin ningún tipo de contrastación de esta.

Los conflictos geopolíticos, ya nombrados previamente, han traído a escena nuevas formas del uso de esta amenaza, **moldeando la percepción de la gente** sobre la evolución y las responsabilidades de sus partes.

AUMENTO DE LAS CAPACIDADES DE LOS ACTORES DE AMENAZAS

APROVECHAMIENTO DE EXPLOITS 0-DAY Y VULNERABILIDADES CRÍTICAS

La utilización y aprovechamiento de **exploits de 0-day** cada vez son más frecuentes, siendo, de hecho, la explotación de vulnerabilidades el vector de intrusiones identificadas con mayor frecuencia en los ataques perpetrados por grupos patrocinados por Estados. Grupos de hackers éticos han descubierto este año 65K vulnerabilidades de software, suponiendo esto un incremento del 21 % respecto al 2021.

Concretamente, no se puede dejar de mencionar a ***ProxyNotShell,*** las dos nuevas vulnerabilidades de Microsoft Exchange Server que han estado siendo activamente explotadas por los ciberdelincuentes éste último año, en ataques de acceso a servidores y ejecución remota de código. Presentan similitudes con ProxyShell, de 2021, de ahí su denominación.

Los ciberdelincuentes se valen de la **divulgación de CVE para encontrar debilidades adicionales,** convertirlas en armas y explotarlas. Durante los últimos meses, la explotación de vulnerabilidades fue documentada como la **causa más común de incidentes de seguridad,** la cual se ha visto aumentada un 33 % desde 2020. Se estima que este incremento se vincula principalmente a fallos introducidos en procesos de transformación digital, sobre todo fallos de configuración (+150 %) y autorizaciones incorrectas (+45 %).

Se observaron **altos volúmenes de compra y venta** dentro del mercado clandestino de exploits, orientados a vulnerabilidades de *ProxyLogon, ProxyShell, PrintNightmare* y *Log4Shell.*

EL NEGOCIO DEL CYBERCRIME AS A SERVICE (CaaS)

Se ha producido el asentamiento del modelo de negocio del ***Cybercrime as a Service (CaaS),*** siendo ya habitual la presencia de grupos o individuos que toman la figura de cibercriminal mercenario al servicio de quien necesite algún tipo recurso, bien o servicio, ya sea acceso (AaaS), hacking (HaaS), malware (MaaS), ransomware (RaaS) o phishing (PhaaS). Igualmente, los ciberdelincuentes recurren directamente a material listo para usar, ofrecido por otros ciberdelincuentes mediante kits de malware.

Especial relevancia tiene aquí el servicio de ***Initial Access Brokers (IAB),*** mercado el cual ha florecido aún más en los últimos años, principalmente debido a la constante demanda, por parte de las organizaciones criminales, de fácil acceso a las organizaciones objetivo. Este mercado *AaaS* continúa **habilitando actores estatales,** compuesto principalmente por compañías que ofrecen capacidades cibernéticas ofensivas.

ATAQUES A LA CADENA DE SUMINISTRO

Se ha percibido un creciente interés y capacidad en **ataques a cadenas de suministro** y contra MSPs (Managed Services Providers). Los actores acuden cada vez más a este recurso, viendo un aumento constante desde la revelación de la campaña de cadena de suministro de SolarWinds, en diciembre de 2020.

Esta amenaza **combina, al menos, dos ataques distintos:** uno a un proveedor y otro a su cliente. Cada vez más, los actores maliciosos explotan este método para llevar a cabo sus operaciones, debido a su conectividad de red de confianza y acceso privilegiado a sus clientes.

Hay una creciente interconexión de esta tendencia con **la implementación de ransomware, coin mining, robo de criptomoneda y robo de credenciales,** facilitando otro tipo de actividades.

USO DE CERTIFICADOS DE FIRMA DE CÓDIGO COMPROMETIDOS

Cada vez más en los últimos meses se está constatando el **uso de certificados de firma de código comprometidos,** robados y comprados ilícitamente para firmar malware. Este método está siendo utilizado por los atacantes para entregar drivers maliciosos, lo cual les permite eludir las medidas de seguridad cruciales que requieren que los drivers estén firmados para que el sistema cargue el paquete.

LOS ATAQUES CONTRA LA DISPONIBILIDAD SE SITÚAN, JUNTO CON LOS ATAQUES DE RANSOMWARE, EN LA CIMA EN CUANTO A VOLUMEN DE EVENTOS

AUMENTO SIGNIFICATIVO DE ATAQUES DDoS

Los ataques DDoS se están **volviendo cada vez más grandes y complejos,** moviéndose hacia redes móviles e IoT *(Internet of Things)* y aumentando de forma constante a lo largo de todo el 2022, especialmente los realizados por ciberdelincuentes profesionales. Igualmente, tal como hemos avanzado anteriormente, están siendo ampliamente utilizados en contextos de guerra cibernética.

Es importante remarcar que el **volumen de ataques de DoS se ha situado en lo más alto,** acompañando a los incidentes de ransomware, lo cual es un cambio notable respecto a años anteriores, cuando el ransomware despuntaba claramente respecto a todas las demás amenazas. De hecho, en el último trimestre de 2022, con respecto al del año anterior, el número de ataques DDoS se ha visto duplicado.

EL RANSOMWARE SE MANTIENE EN VOLUMEN, PERO EVOLUCIONA EN FORMA

Se ha notado cierta evolución, tanto en tipos como en sofisticación, de técnicas de extorsión. Cada vez es más frecuente observar la utilización de la llamada **doble, triple e, incluso, cuádruple extorsión,** en la cual el atacante extiende el rango del ataque a clientes y socios comerciales de la víctima para incrementar la presión, bajo la amenaza y la posibilidad de interrupciones en el negocio causados por ataques de ransomware.

Tal es así la evolución de las técnicas de extorsión que los ciberdelincuentes se han dado cuenta de que podían **solicitar rescates sin el despliegue de ransomware** y así crear mercados dedicados donde anunciar y vender datos robados. Los ciberdelincuentes también han usado el concepto de **pólizas de seguro cibernético** durante la fase de negociación.

Como caso particular ha llamado la atención el **primer ransomware hacktivista** del cual se ha tenido noticia. Las ciberoperaciones en las cuales ha tomado partido han sido organizadas por el grupo hacktivista Cyber Partisans, las cuales han sido notables y han dado a conocer el primer ransomware de su clase.

POPULARIZACIÓN DE LOS *LEAK SITES*

Los llamados ***leak sites,*** o sitios de filtración, han ganado gran popularidad. Cada vez es más frecuente acudir a esta figura del leak seat para apuntar, directamente, a daños reputacionales por la filtración de la información, lo cual, en muchas ocasiones, los atacantes han comprobado que implica mucha mayor presión para la víctima que la simple amenaza de pérdida de datos.

INGENIERÍA SOCIAL Y PHISHING: UNA VEZ MÁS, VECTOR MÁS COMÚN PARA ACCESO INICIAL

PHISHING CADA VEZ MÁS SOFISTICADO

El elevado volumen de casos de ingeniería social va a la par con el nivel de sofisticación, en concreto en lo referente al *phishing.* Al igual que ocurre con cualquier estafa tradicional, cada vez son **más sofisticados los métodos para conseguir engañar a las víctimas,** y cada vez es más complejo estar lo suficientemente alerta para no convertirse en una de ellas.

Esta sofisticación ha conseguido que importantes grupos, como por ejemplo Lapsus$, **atacaran con éxito a grandes compañías tecnológicas** como NVIDIA, Samsung, Microsoft, Okta o T-Mobile, así como a otras entidades como Uber o el Ministerio de Salud de Brasil.

USO EXTENDIDO DEL PHISHING CONTEXTUAL

Desde hace ya un tiempo atrás es habitual el uso **de phishing en referencia a determinados contextos.** Esto vendría ligado al habitual impacto general del panorama geopolítico ya comentado, de lo cual se derivaría la adaptación de los ataques de phishing al contexto social que estamos viviendo, en este caso, con gran prevalencia de todo lo relacionado con la guerra entre Rusia y Ucrania.

En este sentido, por tanto, encontramos muchas similitudes con lo ocurrido éstos últimos años con el contexto de la pandemia de COVID-19.

MAYOR SELECCIÓN DE OBJETIVOS

La evolución del phishing no sólo afecta a sus técnicas de implementación, sino también a las de **selección de objetivos.** Cada vez es más habitual hablar, en mayor o menor grado, de ataques de *spearphishing* en lugar del tradicional phishing genérico, dado que suelen mostrar cierto grado de adaptación a víctimas o entornos concretos, presentando **mayor carga de customización, individualización y personalización.** Esto los hace más creíbles y los aleja del phishing general e indiscriminado —por supuesto, sin dejar éste de estar presente—.

ABUSO DE CUENTAS CONOCIDAS Y DE BEC

Muchos atacantes han dejado de apuntar a buzones individuales y han optado por **abusar de la infraestructura legítima** para ejecutar sus operaciones.

Cada vez es más común el **compromiso de cuentas corporativas o de servidores de Microsoft Exchange** —a través de ProxyShell o ProxyLogin— para distribuir correos a cuentas de usuario tanto internas como externas. También se implementan ataques de ***hijacking,*** modificando tipografía e idioma de los mensajes de respuesta para cada ataque.

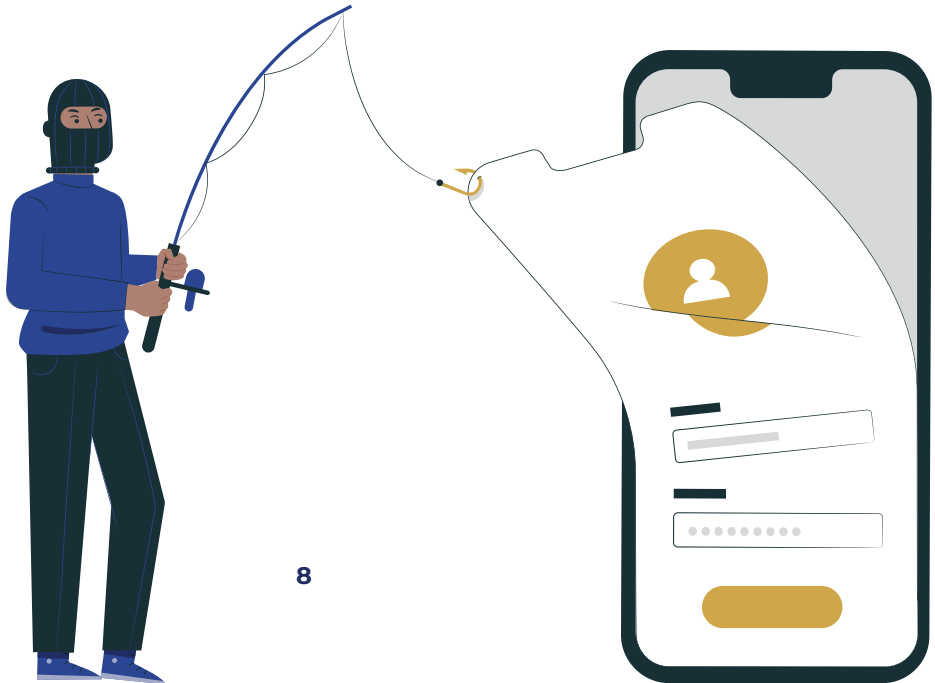
UTILIZACIÓN DEL VISHING COMO MEDIO DE ESTAFA FINANCIERA

Se ha hecho habitual el modus operandi de vishing, por medio del cual **el estafador contacta por vía telefónica a la víctima para convencerla** de transferir fondos a una 'cuenta segura', contándole que su cuenta del banco se ha visto comprometida. También suelen avisar de una retirada fraudulenta de efectivo al usuario, apremiando para facilitar credenciales de acceso para manejar la situación. Suelen hacerse pasar por policías o personal de la institución financiera.

Este tipo de casos se han incrementado sustancialmente, no menos de un **550 % respecto al año anterior.**

CAMPAÑAS DE PHISHING APT

Muchos grupos APT emplean **campañas de ingeniería social de larga duración** para operaciones de ciberespionaje y obtención de información. Estas campañas utilizan una amplia gama de métodos, tales como la construcción elaborada de perfiles en redes sociales, la creación de webs, conferencias e identidades fraudulentas, la recopilación de información de las víctimas mediante investigación OSINT, y un largo etcétera.



FUERTE REGRESO DEL MALWARE

LA UE ALBERGA LA MAYOR PARTE DE ACTIVIDAD

El malware vuelve a escena, aumentando otra vez su presencia tras un detrimento temporal a lo largo de la pandemia por COVID-19, esta vez asociado principalmente al **crypto-jacking** y al malware de **IoT.**

En lo referente a la presencia de malware en términos generales, se han observado un gran número de ataques involucrando software malicioso, principalmente focalizados en el **entorno de la UE.** No obstante, éste fenómeno no sólo se circunscribe a la UE, sino que se estima que, **en todo el mundo, más del 15 %** de computadoras de usuarios de internet sufrió uno o más ataques de tipo malware durante el último año.

RETIREMENT Y REBRANDING

Continuas **retiradas y *rebranding* de grupos de malware,** los cuales permutan integrantes, códigos base y campañas, adaptando malware con variantes que se entrelazan unas con otras y son utilizadas por diferentes actores. Algunas familias de ransomware han desaparecido, tales como Egregor, REvil, BlackMatter y Doppelpaymer, mientras que algunas de las nuevas familias aparecidas presentan similitudes con aquellas.

Se ha visto un potente desarrollo de malware en los ataques dirigidos a la industria, concretamente ataques a sus **sistemas de control industrial** (ICS).

ATAQUES A IoT CASI DUPLICADOS

Sólo en la primera mitad de 2022 fueron cuantificados **más de 12M de ataques de malware dirigido a IoT,** y esto sólo si contabilizamos los producidos por las principales Botnet: Mirai y Mozi.

Esto supone **el mayor de todos los registros de los últimos 4 años,** siendo los objetivos IoT más comunes algunos dispositivos de red como Netgear, D-Link y Dasan.

ADOPCIÓN DE ALTERNATIVAS A LAS MACROS DE OFFICE

Tras el anuncio de Microsoft acerca del bloqueo de macros de archivos provenientes de Internet por parte de Office, se ha ido confirmando un cambio hacia el uso de **archivos contenedores (ISO, ZIP, RAR) y archivos de acceso directo de Windows (LNK)** en las campañas de distribución de malware. Según algunos estudios se confirmaría que, efectivamente, los **archivos comprimidos han superado, por primera vez en 3 años, a los documentos de Office** como tipo de archivo más común.

Explicado en datos concretos, el número de campañas de malware que usan macros VBA han caído del 70 al 20 %, mientras que aquellas que usan LNK se han visto incrementadas del 5 a más del 70 %.

Se han identificado igualmente campañas de uso combinado de archivos comprimidos con nuevas técnicas de **contrabando de HTML** con las que eludir las soluciones de seguridad de correo electrónico.

DISTRIBUCIÓN DE MALWARE MÓVIL

Sólo en junio de 2022 se descargaron unos **10M de troyanos** *adware.* Por otro lado, a los anteriores casos de spyware Pegasus y NSO se suman nuevos ataques dirigidos por otras organizaciones, como Predator, de los desarrolladores del spyware Cytrox.

AUMENTA EL RIESGO PARA LAS REDES ICS/OT

AMPLIA GAMA DE ATAQUES A REDES OT

Las amenazas cibernéticas contra **Infraestructuras Críticas (IC) y redes OT** aumentan en escala, alcance y sofisticación a medida que han ido aumentando las tensiones geopolíticas. Se han observado ataques, principalmente, para recopilar **Inteligencia,** desplegar **malware de ICS e interrumpir servicios.**

En este ámbito tienen gran presencia los ataques provenientes de grupos patrocinados por Estados, los cuales implementan elaborados **ataques destructivos** como un componente prominente de sus operaciones. En este sentido se ha registrado un uso generalizado de wiper malware para destruir e interrumpir redes de agencias gubernamentales y de ICs.

El **ransomware** fue la principal causa de compromisos en el sector industrial por parte de la generalidad de cibercriminales, siendo la industria manufacturera el sector más atacado, con diferencia. Concretamente, los ataques de ransomware y extorsión contra organizaciones industriales aumentaron en más del 500 %. Algunos de los malware más catastróficos han mostrado módulos OT específicos.

EVOLUCIÓN DE AMENAZAS EN EL SECTOR ENERGÉTICO: INFRAESTRUCTURAS DE GAS Y PETRÓLEO

Del aumento del 500 % de ransomware señalado en el punto anterior, cabe especificar que el **5 % de esos ataques afectaron a infraestructuras de gas y petróleo,** debido a su prevalencia en el panorama de amenazas, a la baja barrera de entrada para implementar y a la facilidad para realizar campañas de orientación masiva.

La creciente **conectividad remota** desde la pandemia es otra área de preocupación y riesgo potencial para este sector, donde las tradicionales conexiones analógicas aisladas de monitoreo y control básico están dando paso a nuevos modelos que impulsan la transformación digital y la eficiencia operativa, aumentando la conectividad y, por tanto, los vectores de entrada.

ALTO IMPACTO DE AMENAZAS NOVEDOSAS, HÍBRIDAS Y EMERGENTES

AUMENTO DE ATAQUES CONTRA SOCIEDAD CIVIL

Ha habido un aumento de casos relacionados con **vigilancia y selección de ataques contra sociedad civil.** Por ejemplo, el caso Pegasus tuvo graves repercusiones, con amplia cobertura e impacto en los medios y con acciones gubernamentales. Este caso supuso un gran escándalo, producido por el Grupo NSO, con sede en Israel, donde más de 30.000 activistas de derechos humanos, periodistas y abogados de todo el mundo fueron atacados, así como 14 líderes mundiales.

En este aspecto destacan las acciones llevadas a cabo por **grupos de AaaS,** los cuales tienen como objetivo, cada vez más, disidentes, activistas, abogados civiles, periodistas y otros ciudadanos privados.

USO EXTENDIDO DEL *CONSENT PHISHING*

Uso extendido del ***consent phishing,*** o phishing de consentimiento. Los atacantes envían un link a la víctima y la engañan para que haga click en él. Hecho esto, brindan al actor malicioso acceso y permisos a aplicaciones y servicios.

IA Y ML COMO VECTORES DE ENTRADA

Los modelos de ***machine learning*** **(ML)** se convierten, cada vez más, en objetivo de ciberataques. Esto es particularmente amenazante, dado que los ML se encuentran en el núcleo de los sistemas modernos.

El **mal uso de la IA** (Inteligencia Artificial) y la expansión de los ***deepfakes*** alimentan la desinformación, con la proliferación de bots que modelan personas y la perturbación de los procesos de 'notificación y comentario', así como de la interacción de la comunidad. Se sucede la inundación de agencias gubernamentales con información y comentarios *fake*.

INTERCEPCIÓN DE TRÁFICO HTTPS

Las **Autoridades Certificadas (CA) estatales** facilitan la intercepción de tráfico HTTPS y de ataques *man-in-the-middle* contra sus ciudadanos, poniendo en riesgo la seguridad y privacidad de Internet.

NUEVAS OPORTUNIDADES DE ATAQUE EN LA NUBE

Se han generalizado los servicios basados en la nube para respaldar los procesos de negocio de las organizaciones, los cuales brindan **una falsa sensación de seguridad, reduciendo el esfuerzo empleado por las organizaciones** en monitorizar las infraestructuras y plataformas de la nube. Como resultado, los cibercriminales se focalizan en estos servicios y están tomando ventaja de las deficiencias en la administración de activos y configuraciones.

En este terreno, los cibercriminales se benefician de **infraestructuras y botnets *command-and-control* (C2),** altamente escalables y fiables. Las APIs públicas, por su parte, pueden ser usadas como vectores de ataque para obtener acceso a dispositivos individuales.

PROXIMIDAD CON EUROPA DE LAS PRINCIPALES AMENAZAS DEL CIBERESPACIO

A lo largo de este año, en todo el mundo, se ha visto un número de incidentes menor al sufrido en 2021. No obstante, en concreto, aquellos que han tenido lugar **en el entorno de la UE han mantenido cifras elevadas** de forma constante —especialmente en lo referente a las amenazas persistentes y avanzadas—.

Esto quiere decir que, si bien la tendencia global ha mostrado cierta disminución de ciberactividad maliciosa, no ha sido así en Europa, donde el fenómeno sigue teniendo fuerte presencia y manteniendo una dinámica alcista. Esto implica una gran relevancia del contexto de Europa, lo cual enlazaría directamente con la actual situación geopolítica.

LA ADMINISTRACIÓN: EL SECTOR MÁS GOLPEADO

Se observa, una vez más, un gran número de incidentes dirigidos **contra la Administración Pública y contra los proveedores de servicios gubernamentales y digitales.** Esto último es de esperar dada la provisión horizontal de servicios para este sector y, por lo tanto, su impacto en muchos otros sectores.

Sin embargo, no deben perderse de vista otros sectores a los que también se está apuntando de forma notable. El sector financiero, por ejemplo, se enfrentó a un número constante de incidentes ocurridos durante los últimos meses, seguido de cerca por el sector de la salud. También se ha observado un número significativo de incidentes dirigidos a usuarios finales y no necesariamente a un sector en particular.

QUÉ NOS ESPERA EN EL 2023

Con un panorama como el detallado previamente, nos enfrentamos sin duda a un 2023 marcado por un aumento del número de intentos de ataque e intrusión, acompañando a todos los nuevos procesos de transformación digital y la adopción de nuevas tecnologías, pero que cuya base predominante de materialización será la facilidad y rapidez de éxito debido a la disposición de nuevas armas como la computación cuántica, las redes 5G, el malware como servicio, y los recursos de IA.

Todo ello favorecido también, por un crecimiento desigual y a un ritmo menor, de la concienciación de los usuarios y las organizaciones sobre materia de ciberseguridad, así como una recesión económica que limitará las inversiones en este sentido.

Se detallan a continuación los aspectos más destacables en este sentido.

AUMENTO DE LOS EFECTOS Y DE LAS INFLUENCIAS GEOPOLÍTICAS EN LA CIBERDELINCUENCIA

AUMENTO DE ATAQUES DISRUPTIVOS Y DESTRUCTIVOS

Según continúen —y aumenten— las tensiones entre Oriente y Occidente, se sucederán gran cantidad de ataques contra la disponibilidad, tanto disruptivos como destructivos, a todo tipo **de IC, redes OT, instituciones gubernamentales e industrias clave.** Los ataques de malware de tipo wiper irán en aumento.

Se espera que, en los próximos meses, algunos grupos de ransomware prorrusos se coordinen para llevar a cabo **operaciones destructivas contra organizaciones occidentales.** Especial mención a la seguridad de cables, terminales y conductos de distribución submarinos, particularmente difíciles de vigilar y proteger.

Si bien es cierto, la finalización del conflicto entre Rusia y Ucrania podría marcar un punto de inflexión, no pudiendo prever con certeza la evolución posterior del fenómeno.

CONFUSIÓN ENTRE FINES, TIPOLOGÍAS Y DIFERENCIACIÓN DE GRANDES GRUPOS Y ATAQUES: AMENAZAS APT, PATROCINADAS POR ESTADOS Y HACKTIVISTAS

Cada vez más, muchos de los ataques del contexto geopolítico serán **difícilmente identificables,** no pudiendo ser rastreados y pudiendo parecer accidentes aleatorios. Otros tomarán formas de pseudoataques de ransomware u operaciones hacktivistas para poder negar la autoría real de los mismos.

También aumentará la confusión, concretamente, con la tipología de muchos grupos, no estando siempre claro cuando se trata de un **grupo APT autónomo, si éste hace funciones de CaaS, si está patrocinado por algún Estado, o si se define como grupo con finalidades hacktivistas** que, realmente, pueda estar movilizado por algún Estado o ligado a grupos APT no hacktivistas, ya sea por sus miembros o por sus fines u objetivos.

Esta creciente interconexión entre grupos, ocultación de autorías o fines, y complejidad en las tensiones geopolíticas, dificultará enormemente el análisis y la comprensión de las amenazas y de sus autores.

AUMENTO DEL INTERÉS POR LA OBTENCIÓN DE INTELIGENCIA

Sin disminuir el recurso al tradicional agente infiltrado, y a software y metodologías de espionaje más silenciosas y tradicionales, la creciente tensión entre Oriente y Occidente traerá consigo un cada vez mayor número de **ataques cibernéticos dirigidos a la obtención de grandes cantidades de Inteligencia** de Gobiernos y multinacionales.

Debido a esto, aumentarán también los grupos y organizaciones que ofrezcan estos **servicios de Inteligencia privados** y de obtención de información.

ATAQUES A LA CADENA DE SUMINISTRO A GRAN ESCALA

SERVIDORES DE CORREO COMO OBJETIVO PRIORITARIO

Los servidores de correo representan un grandísimo **conjunto de softwares que involucran varios protocolos y que necesitan conexión** para funcionar correctamente, presentando la superficie de ataque más grande que se pueda imaginar y conteniendo Inteligencia clave de interés para los atacantes.

APUNTADO A TECNOLOGÍAS, PRODUCTORES Y OPERADORES SATELITALES

A medida que **se extiende el apoyo tecnológico en los satélites,** tanto por parte de los Estados como de empresas privadas, aumenta el riesgo de ataque por parte de los grupos APT más sofisticados.

Con las capacidades existentes, **crece la evidencia de que las APTs puedan atacar satélites** (como el incidente de Viasat, por ejemplo). Es probable que los agentes de amenazas de APTs presten cada vez más atención en el futuro a la manipulación, interferencia y filtración de las tecnologías satelitales.

AUMENTO DE ATAQUES A CADENA DE SUMINISTRO DIGITAL

Desde hace unos años, **las cadenas de suministro han ido conectándose paulatinamente a Internet,** pero no se han protegido, en muchos de los casos, de forma debida. La introducción de nuevas TIC en torno a dichas cadenas de suministro, y de las nuevas tecnologías introducidas mediante las cadenas de software en particular, hace muy probable que vayan apareciendo vulnerabilidades que aún no se hayan identificado.

PROVEEDORES DE API, INFRAESTRUCTURAS Y SERVIDORES ALOJADOS EN LA NUBE: DOBLE FACTOR DE RIESGO

Este tipo de servicios externos cada vez son más demandados por empresas de todos los tipos y tamaños para alojar, almacenar y procesar la información. Ya se han dejado ver, en los últimos meses, ataques a la cadena de suministro mediante **recurrentes intrusiones a proveedores de infraestructura en la nube** y, analizando las tendencias actuales, no se espera si no un continuo goteo de accesos no autorizados a este tipo de servidores, mediante los cuales acceder a grandes cantidades de información de empresas y negocios de todo tipo.

AUMENTO GENERALIZADO EN MALWARE: VOLUMEN Y SOFISTICACIÓN

LA NUEVA "PANDEMIA" CIBERNÉTICA DE 2023

Tal como muestran las estadísticas —y como bien han señalado los expertos de Kaspersky—, las mayores epidemias cibernéticas, en magnitud e impacto, **ocurren cada 6-7 años, habiendo sido el último el famoso *WannaCry,*** un gusano ransomware que infectó computadoras de todo el mundo en 2017, explotando la vulnerabilidad EternalBlue.

La creación de este tipo de malware debe ir secundada por una **vulnerabilidad que englobe una serie de características y condiciones muy concretas,** lo que hace muy difícil su materialización y su

predicción. No obstante, ante el gran incremento de vulnerabilidades halladas y las crecientes tensiones actuales, con la proliferación de ataques de robo y filtración de datos, no es difícil imaginar que la próxima gran epidemia está próxima a aparecer.

AMPLIACIÓN DE ALTERNATIVAS AL COBALTSTRIKE

CobaltStrike, una herramienta de red teaming, ha venido siendo ampliamente utilizada desde 2012 por gran parte de los ciberdelincuentes y de los grupos APT. No obstante, hay previsión de aumento de alternativas con fines similares, como **Brute Ratel C4, Sliver, Manjusaka o Ninja.**

Estas alternativas presentan **nuevas capacidades y técnicas de evasión** más avanzadas, lo cual será aprovechado por los atacantes, aprovechando el monopolio de atención que está recibiendo CobaltStrike por parte de los defensores.

USO DE SIGINT COMO VECTOR DE ENVÍO DE MALWARE

En este caso se colocarían, directamente, **servidores en posiciones clave de la red troncal de Internet,** permitiendo implementar ataques man-on-the-side que permitan la infección de innumerables víctimas sin interacción alguna.

Desplegar estas herramientas requieren de un poder político y tecnológico al alcance de muy pocos, por lo que, probablemente, por lo pronto **se implementará a nivel local,** dentro del propio país, involucrando proveedores de servicios de Internet (ISP).

MALWARE AVANZADO

Se prevé la difusión de **malware más maleable,** adaptable a gran cantidad de escenarios y que puede mutar y cambiar de apariencia para evadir la detección de firmas. Los atacantes podrían **cambiar repetidamente los archivos a nivel binario** para dificultar su reconocimiento por parte de los sistemas de seguridad de los dispositivos, del mismo modo que los virus biológicos mutan para pasar inadvertidos por un sistema inmunológico que estaba preparado para detectar y combatir anteriores cepas.

Énfasis aparte merece la nueva tendencia, que sin duda se mantendrá, del uso de **certificados de código comprometidos,** robados y comprados ilícitamente para firmar malware. Fabricantes como Microsoft están trabajando activamente para evitar esto, pero puede haber un crecimiento de casos a corto plazo antes de que las medidas sean efectivas —o incluso antes de que otros fabricantes comiencen a tomar medidas—.

EVOLUCIÓN EN EL PANORAMA DEL ROBO DE DATOS

NUEVAS MODALIDADES DE *RANSOMWARE*

Aparte de la tradicional figura del ransomware de *robo y extorsión,* cada vez está más de moda la modalidad de **robo y filtración de datos *(hack-and-leak).*** Esto implica el acceso no autorizado a un objetivo y la publicación de documentos, datos y archivos internos. Esto ha sido últimamente utilizado por los grupos de ransomware como método de extorsión presionando a las víctimas, pero este método está siendo utilizado, cada vez más, por **grupos APT con fines disruptivos** —en consonancia con la previsión del aumento de ataques de este tipo ya comentada—.

De cualquier forma, el **ransomware continuará siendo una amenaza grave** para organizaciones de todo tipo y tamaño, de todas partes del mundo, aunque expandiendo su tradicional enfoque puramente

económico a otros más variados: eliminación directa de datos, exigencias de tipo político... Tendremos así una nueva figura de ransomware más híbrida y combinada, dirigida a la destrucción, el robo de datos y el chantaje.

AUMENTO DE ATAQUES A LA INFORMACIÓN EN LA NUBE

Cada vez será más imprescindible el aumento de seguridad de los servicios alojados en la nube. Esta necesidad viene impulsad por el hecho de que, tras el escepticismo inicial, **las empresas depositan ahora una confianza excesiva** en la nube. Habiendo aumentado exponencialmente la superficie de ataque —debido a la creciente cantidad de información e infraestructura almacenada— y relegando la seguridad, en gran medida, a un segundo plano, es inevitable percibir aquí una tendencia mantenida al alza a corto y medio plazo.

Especial mención al caso ya comentado de **servidores, API e infraestructuras de almacenamiento en la nube, los cuales aúnan todos los factores de riesgo** del interés hacia las cadenas de suministro a gran escala con los factores de riesgo propios de los servicios de terceros alojados en la nube. Se espera igualmente un aumento de casos involucrando estos servicios.

LAS COOKIES DE INICIO DE SESIÓN AUMENTARÁN EL INTERÉS

La sofisticación de los atacantes para capturar cookies se está volviendo cada vez más avanzada, siendo éste un vector que **permite eludir la autenticación multifactor (MFA).** Con la adopción de SaaS, cada vez mayor, por parte de organizaciones y de particulares, y debido también a la generación de contraseñas más complejas y diferentes entre sí —gracias a las continuas recomendaciones de los expertos—, cada vez se recurre más a las cookies para controlar las credenciales de acceso de cada sitio.

Se espera que los ciberdelincuentes busquen formas de automatizar y escalar ataques a cookies de sesión y poder aumentar su rentabilidad.

EL CIBERCRIMEN COMO MODELO DE NEGOCIO (CaaS) AUMENTARÁ CONSTANTEMENTE

EL MERCADO DE LA CIBERDELINCUENCIA FACILITA EL ACCESO DE NUEVOS CIBERCRIMINALES

El CaaS no hará más que aumentar, habiendo demostrado ya en 2022 que algunas de sus modalidades, como **IAB, MaaS y RaaS,** han estado realmente presentes durante este periodo. **La mercantilización de vulnerabilidades y credenciales** han sido igualmente una tónica general, la cual se prevé se mantenga en alza.

El acceso a las nuevas tecnologías facilitará la proliferación de nuevos ciberdelincuentes que carezcan de habilidades o de tiempo necesario, pero que podrán navegar por diferentes **mercados ilícitos** para hacerse con todo tipo de listas de datos, cookies o credenciales robadas, rootkits, herramientas de ransomware, servicios de phishing personalizados, etc.

Todo ello traerá consigo un evidente **aumento de los llamados ataques de "conocimiento cero", así como una disminución de la edad promedio** de los actores de amenazas.

COMPRAVENTA DE MALWARE MODIFICADO Y REUTILIZADO

Con la llegada de nuevos ciberdelincuentes, los cuales muchas veces no tendrán opciones para crear software propio, **se optará cada vez más por servicios ya diseñados,** los cuales se irán implementando con modificaciones o mejoras para eludir su detección.

Debido a su menor tasa de detección, habrá una creciente demanda de **troyanos de tipo downloader y dropper,** convirtiéndose éstos en elementos básicos del Malware-as-a-Service (MaaS). En este tipo de malware se encuentran cada vez más variantes con elementos comunes provenientes de un mismo modelo.

EL PHISHING Y LA INGENIERÍA SOCIAL CONTINUARÁN SIENDO EL PRIMER VECTOR DE ENTRADA

SOFISTICACIÓN DE SEÑUELOS

Si bien continuamos viendo algunas campañas de phishing masivo de estilo tradicional, estamos viendo cada vez señuelos más elaborados, con **más atención y cuidado en la redacción de texto y en los detalles iconográficos.** Igualmente, las técnicas de spoofing cada vez son más depuradas, haciendo a veces verdaderamente difícil distinguir una comunicación legítima de una falsa.

Se espera que los ciberdelincuentes continúen aumentando esfuerzos en la creación de dichos señuelos, y no sólo en los casos más elaborados de spearphishing o de mayor personalización, sino también en las **campañas de phishing masivas.** Se espera, igualmente, gran aplicación de dicha sofisticación en las actividades de **BEC.**

Dicho esto, es probable que veamos un mayor **uso de cuentas conocidas — y "confiables"—, o infraestructura legítima,** para ejecutar campañas de phishing, por ejemplo, explotando vulnerabilidades en sistemas como Microsoft Exchange u Office 365. En este sentido, resaltar que estos eventos de abuso de infraestructura legítima podrán ocurrir, en gran medida, debido a malas configuraciones del DMARC.

INGENIERÍA SOCIAL PARA CONTRARRESTAR LA MFA

Cada vez son más las organizaciones, los programas y los dispositivos que han adoptado el modelo de la autenticación multifactorial como elemento de seguridad de acceso principal. Esta tendencia, que ya se sitúa en el 40 % según encuestas, se prevé que siga en aumento durante el 2023.

Para eludir estas soluciones de validación de seguridad, **la ingeniería social ya ha demostrado su efectividad.** Con la sofisticación de tácticas, técnicas y procedimientos que se están viendo en esta modalidad, será una vía recurrente para eludir la MFA.

EL ROBO DE CREDENCIALES SERÁ EL PRINCIPAL OBJETIVO

Las técnicas de fraude y engaño empleadas **pueden perseguir la obtención de cualquier tipo de información** que tenga valor para el delincuente, dependiendo de cuáles sean sus fines o procedimientos a implementar. Podemos encontrar falsos portales de pago para hacerse con los datos financieros que introduce la víctima, o perfiles falsos en redes sociales orientadas a realizar diferentes estafas.

No obstante, **los datos predilectos que buscarán los actores de ingeniería social será el de las credenciales de acceso** de las víctimas. Éstas serán, en la mayoría de caso, las llaves maestras perseguidas por los atacantes para conseguir acceso a todo tipo aplicativos con los que interactuar en nombre de la víctima.

VULNERABILIDADES

POTENCIAL AUMENTO DE VULNERABILIDADES PRODUCTO DE LA CODIFICACIÓN DE IA/ML

Las herramientas de IA/ML, entre otras funciones, pueden escribir código de forma autónoma, basándose en código informático existente para generar nuevas creaciones. Teniendo en cuenta esta base, **la calidad de sus resultados dependerá directamente de la calidad de los datos de aprendizaje** que se le han introducido previamente, así como de las instrucciones que se le dan.

Es importante señalar que, actualmente, ya contamos con métodos y procedimientos para evitar vulnerabilidades a la hora de producir código automático, por lo que un correcto empleo de la IA por parte de desarrolladores comprometidos mitigaría en gran medida esta tendencia. Todo dependerá, en este sentido, de la mejor o peor praxis del usuario.

A pesar de lo anterior, al igual que ocurría con los cibercriminales noveles acudiendo al CaaS, y teniendo en cuenta la creciente importancia que están adquiriendo los profesionales del sector TIC, con la aparición de nuevos desarrolladores inexpertos o sin tiempo cada vez serán más las personas no preparadas que acudan a IA para la creación autónoma de código, **aumentando exponencialmente las vulnerabilidades críticas** que puedan ser incluidas en futuras aplicaciones.

MAYOR CANTIDAD DE ATAQUES A PYMES DE TODA EUROPA

Las estadísticas nos avisan de que la actuación de los cibercriminales está, paulatinamente, **saliendo hacia fuera de EEUU y recalando en Europa,** siendo el nuevo escenario preferido del fenómeno de la ciberdelincuencia. En concreto se espera una mayor orientación a la **pequeña y mediana empresa, la cual es percibida como más vulnerable** que las grandes multinacionales. Se espera, incluso, el aumento de caso de ataques a usuarios particulares de forma generalizada.

Si bien se ha demostrado que hasta las grandes empresas —e incluso organizaciones "blindadas", como el FBI— son accesibles para los cibercriminales, con el aumento de vulnerabilidades y la creciente digitalización de los negocios se espera una **ampliación del abanico de víctimas,** concretamente a la parte más vulnerable del mismo.

ÁMBITO OT E ICS

EL SECTOR INDUSTRIAL AUMENTARÁ SU DIGITALIZACIÓN Y DISMINUIRÁ SU SEGURIDAD

El acercamiento cada vez mayor de redes OT a redes IT traerá consigo una mayor eficiencia de la industria, a la vez que un nuevo y gran torrente de **nuevas vulnerabilidades.** Debido a una digitalización abrupta, la escasez de personal y las regulaciones verticales, mantenerse actualizadas y seguras planteará grandes dificultades, las cuales no serán siempre debidamente afrontadas.

Es cierto que la modernización de los espacios de trabajo mediante la implementación de administración remota y automatización de redes ofrece un valor considerable para las organizaciones, pero, si no se protegen de forma adecuada, **aumentarán los riesgos de accesos no autorizados al ampliar la superficie de ataque, la cual expondrá los sistemas OT.** Es por ello por lo que se observarán patrones de ataque de OT con mayor frecuencia, más aún en relación con aquellos datos de OT distribuidos o manejados por redes IT y por servicios en la nube.

ATAQUES A INFRAESTRUCTURAS CRÍTICAS (IC) IMPACTARÁN EN LA SOCIEDAD CIVIL

En lo que a ataques disruptivos se refiere, muchos de los ataques dirigidos a ICS continuarán apuntando a IC relativas al **sector energético,** con impacto directo en la sociedad. Se estima, además de un aumento de focalización en empresas energéticas, un aumento de ataques en gran cantidad de sectores como logística y transporte, empresas tecnológicas y complejos industriales militares.

Las campañas de malware dirigidas a IC se mantendrán en 2023, y se continuará registrando nuevos tipos de malware con fines destructivos.

EL RIESGO DE LA OBSOLESCENCIA EN AMBIENTES OT

La falta de parches de seguridad y el software obsoleto presenta dos de las grandes amenazas que se ciernen sobre las redes OT y los sistemas ICS. Según estudios, se estima que el **75 % de los controladores industriales de redes OT tienen vulnerabilidades graves** por falta de parches de seguridad.

FOCALIZACIÓN EN DISPOSITIVOS MÓVILES E IoT

CRECEN LAS AMENAZAS ESPECÍFICAS PARA DISPOSITIVOS MÓVILES

Con el **aumento del uso de teléfonos y dispositivos inteligentes en los entornos de trabajo,** crece el interés en estos aparatos por hacerlos objetivo de ataques cibernéticos. Estos ataques han aumentado un 22 % en el último año y se espera que la tendencia continúe durante el 2023. Entre otras cosas, esto pone en riesgo la autenticación basada en SMS.

DISPOSITIVOS IoT: CONECTADOS, DESPROTEGIDOS Y DESACTUALIZADOS

Muchos dispositivos IoT, debido a una **carencia de seguridad,** a una **mala configuración** o a una desactualización de software, son propensos a sufrir ataques e intrusiones de todo tipo: toma de control, violación de datos, acceso a imágenes y registros, compromiso de credenciales, etc. Con el paso del tiempo, mayor será el número de estos dispositivos con configuraciones deficientes o software desactualizados, por lo que, muy probablemente, estaremos ante un aumento de ataques a estos dispositivos.

El problema se agrava si tenemos en cuento que esos mismos dispositivos **se ejecutan, probablemente, en la misma red que utilizan las personas para acceder a recursos corporativos** al trabajar desde casa, con la potencial exposición de direcciones IP.

DESINFORMACIÓN

ATAQUES DE DESINFORMACIÓN COMO DESESTABILIZADOR POLÍTICO Y EMPRESARIAL

Con el continuo **aumento en la cantidad de datos e información que se manejan** por Internet, por las redes sociales y por los medios de comunicación, **crecerá el número de focos de desinformación** orientado a desestabilizar ciertos ámbitos de la sociedad, como también a la mera ganancia de audiencia que conlleva el publicar noticias y titulares llamativos, independientemente de su veracidad.

En este contexto, crecerá la **instrumentalización de la desinformación como medio de manipulación de las masas,** para alejar a la sociedad de ciertas áreas y acercarla a otras alternativas, según los objetivos del autor.

Igualmente, se espera aumento de operaciones de desinformación por parte de **actores estatales expandiéndose fuera de Europa del Este,** con mayor riesgo durante operaciones físicas o geopolíticas de alto perfil.

DEEPFAKES MEJORADOS

El uso de deepfakes puede formar parte de un gran número de **ataques combinados,** como el engaño a entidades financieras o como apoyo en campañas de ingeniería social. La tecnología orientada a deepfakes ya se utiliza efectivamente para manipular y dirigir opiniones, o engañar a personas a que cedan credenciales o datos.

Con las **mejoras en la construcción de IA y con el incremento de recursos tecnológicos** a nuestro alcance, los deepfakes cada vez serán más sofisticados, numerosos, convincentes y efectivos.

EL SECTOR PÚBLICO Y LA ADMINISTRACIÓN SEGUIRÁN EN EL PUNTO DE MIRA

ATAQUES RECURRENTES A LA ADMINISTRACIÓN PÚBLICA

De modo coincidente con lo que hemos visto en los últimos meses, **se espera que la tendencia continúe al alza** en lo que a ataques a organismos públicos se refiere, de muchos de los sectores de la Administración y del Gobierno. Esta dinámica será consecuencia de gran parte de lo comentado anteriormente: aumento de cibercriminales con acceso a rootkits, mayor actividad de grupos APTs, hacktivistas y patrocinados por Estados, mayor sofisticación del malware y de las técnicas de phishing, etc.

Todo esto confluye, directamente, con la tendencia actual de apuntado a la Administración Pública, tanto por la **cantidad y calidad de información procesada,** como por la mayor vulnerabilidad percibida que presenta. Sin una clara renovación y fortificación de sus sistemas de defensa, todo ello parece indicar esta tónica en los próximos meses.

NUEVO INTERÉS EN LA ADMINISTRACIÓN LOCAL Y REGIONAL: AYUNTAMIENTOS Y MUNICIPIOS EN EL PUNTO DE MIRA

Sin disminuir lo comentado acerca de ataques dirigidos a la Administración Central del Estado, está aflorando una **nueva tendencia de ataques a pequeñas Administraciones de toda España,** así como de varios países de Europa. Estos ataques estarían mayormente dirigidos a la violación de datos, predominantemente a través de la figura del **ransomware.**

Esta tendencia al alza puede deberse a la **menor ciberseguridad percibida** de los municipios y de los ayuntamientos —en comparación con la Administración Central—, lo cual los haría blancos más fácilmente alcanzables. Igualmente, el **enorme daño potencial** que se le puede inferir a una Administración regional con este tipo de ataques puede ser percibido por el ciberdelincuente como una garantía extra de colaboración por parte de la víctima, con la consiguiente mayor probabilidad de que el rescate sea pagado.

¿CÓMO PODEMOS PROTEGERNOS?

Está en nuestra mano el aumentar nuestra seguridad en el entorno cibernético, y para ello no hay más que tener en cuenta ciertas recomendaciones muy sencillas:

- **Aumentar la salud de nuestras contraseñas.**
  Nuestras claves deben tener una longitud mínima de 16 caracteres, debiendo combinar, como mínimo, minúsculas, mayúsculas y números, añadiendo también símbolos y caracteres especiales cuando sea posible. Por supuesto, además de esto, debemos utilizar contraseñas únicas y diferentes para cada plataforma, no debiendo repetir la misma en varios accesos.

- **Actualizar el software y los dispositivos a las últimas versiones disponibles.**
  Para evitar que un atacante explote alguna vulnerabilidad que pueda afectarnos, siempre es recomendable estar al día en cuanto a actualizaciones y parches de seguridad se refiere. Los cibercriminales siempre están muy actualizados, y un sistema obsoleto es un factor de riesgo muy importante.

- **Establecer una configuración DMARC en el correo electrónico.**
  Para evitar que abusen de nuestra cuenta de correo y la utilicen para implementar ataques de phishing, mantener una configuración DMARC saludable es algo esencial. Este es un vector de entrada asiduo actualmente, por lo que es importante incidir en este punto.

- **Formación continua en ciberseguridad.**
  Cada día hay avances significativos tanto en técnicas de seguridad como de ataque, por lo que mantener una formación actualizada es siempre garantía de una mayor protección de nuestro entorno. Las nociones se olvidan y se oxidan, pero, por el contrario, los cibercriminales se mantienen entrenados y en forma. Refrescar nuestros conocimientos y adquirir nociones sobre nuevas tendencias es imprescindible.

- **Configurar bien nuestras opciones de seguridad en la nube.**
  No debemos dejarnos guiar por la falsa sensación de seguridad que nos genera el contar con servicios en la nube. Si bien este recurso facilita enormemente el trabajo, no hay que olvidar que se trata de un vector de entrada muy amplio y difícil de contener. Debemos establecer una configuración adecuada e implementar aquellos sistemas de seguridad, de control de accesos y de encriptado que tengamos a nuestro alcance.

- **Analizar concienzudamente comunicaciones, anuncios, adjuntos y enlaces.**
  Por norma general, debemos acceder a los sitios mediante su página web o aplicación oficial, en lugar de a través de anuncios o enlaces remitidos por email o SMS. Debemos extremar precauciones ante cualquier comunicación que no esperemos, más aún si se trata de remitente desconocido, pero no olvidando que una comunicación fraudulenta puede venir también de un remitente u organismo confiable.

- **Extremar precauciones en las redes IT.**
  En el caso de redes IT, los requisitos de seguridad aumentan en gran medida, dado que así lo hacen, también, los factores de riesgo y los vectores de entrada potenciales. Además de los consejos anteriores,

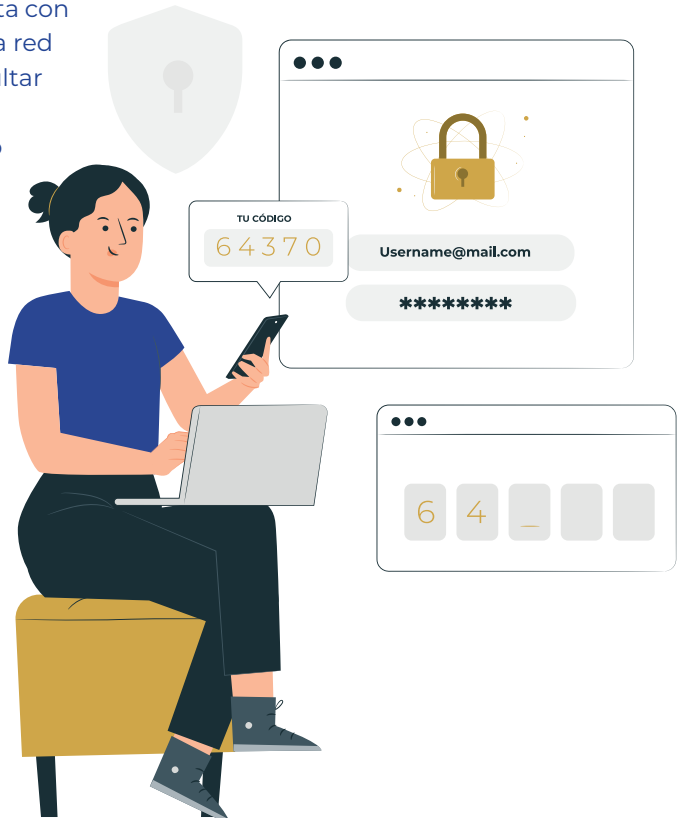
cualquier red IT debería tener en cuenta lo siguiente:

- **Ciberseguridad como anticipación, no como reacción.** Es esencial tomar las medidas adecuadas antes de que se produzcan los efectos adversos, lo cual ahorrará costes y pérdidas de notable magnitud. Las ciberamenazas crecen constantemente y la prevención es la barrera más efectiva para hacerles frente.
- **Hacer copias de seguridad —y guardarlas correctamente—.** Indudablemente, tener copias de seguridad siempre será un método de restablecimiento muy eficaz, reduciendo en gran medida los efectos de la pérdida de información. Estas copias deben configurarse acorde con las necesidades de negocio, tanto en periodicidad como en elementos abarcados. No obstante, tan importante es contar con copias de seguridad como guardar estas convenientemente. Se recomienda mantener dichas copias en dispositivos locales externos, desconectados de la red y de otros elementos.
- **Vigilancia y monitorización continua.** Los ataques y las intrusiones pueden materializarse en cuestión de segundos. Un actor de amenazas puede introducirse en un sistema y permanecer operando dentro durante semanas o meses. Es por ello esencial una correcta monitorización de procesos en nuestros sistemas, de cara a detectar aquellos indicios que nos alerten de cualquier tipo de actividad sospechosa.
- **Llevar a cabo auditorías periódicas.** Someter a examen el estado de nuestras barreras y sistemas, así como de nuestros elementos de seguridad, siempre nos brindará el feedback necesario para conocer la salud de nuestra ciberseguridad. Una auditoría periódica enriquecerá enormemente nuestra visión general acerca del punto de madurez que tenemos y de aquellos aspectos en los cuales debemos poner foco.

- **Máxima prevención en redes OT.**

Debido al ya comentado acercamiento de redes IT-OT, así como al aumento en el atractivo de estas últimas para los cibercriminales, es en estas redes uno de los entornos donde la ciberseguridad debe ser más concienzuda. Todas las recomendaciones anteriores son aplicables, pudiendo añadir las siguientes consideraciones específicas:

- **Establecer una seguridad en profundidad.** Es recomendable establecer un sistema de seguridad por capas, debiendo dedicar las capas más profundas a aquellos activos y recursos más críticos para la red. Del mismo modo que una ciudad medieval cuenta con muralla exterior y un sistema de murallas interiores, una red OT debería mostrar una protección análoga para dificultar las acciones maliciosas.
- **Favorecer la sectorización.** Tanto a nivel físico como cibernético, y en un plano más lateral que en el anterior, en un mismo nivel no debería ser todo igualmente accesible para todo el mundo. Siempre será positivo implementar ciertos controles de accesos a ciertas zonas y secciones, según la necesidad de saber y las labores de quienes hagan uso de ellas.
- **Valorar qué dispositivos necesitan conexión.** No todos los dispositivos y elementos deben estar necesariamente conectados a la red. Debe atenderse a qué sistemas y dispositivos tienen conexión a la red, a qué sitios y procesos están ligados, a dónde no necesitan acceder, y qué dispositivos no necesitan, en absoluto, una conexión. ◆



IR AL PRINCIPIO

REFERENCIAS

AT&T (2022) | *10 Cybersecurity predictions for 2023.* Obtenido de:
https://cybersecurity.att.com/blogs/security-essentials/10-cybersecurity-predictions-for-2023

Engineer Live (2022) | *Oil & gas cyber security considerations.* Obtenido de:
https://www.engineerlive.com/content/oil-gas-cyber-security-considerations

ENISA (2022) | *ENISA Threat Landscape 2022. European Union Agency for Cybersecurity.* Obtenido de:
https://www.enisa.europa.eu/publications/enisa-threat-landscape-2022

Fortinet (2022) | *Cyber Threat Predictions for 2023.* Obtenido de:
https://www.fortinet.com/content/dam/fortinet/assets/white-papers/wp-threat-prediction-2023.pdf

Gartner (2022) | *Gartner's 8 Cybersecurity Predictions for 2023-2025.* Obtenido de:
https://krontech.com/gartners-8-cybersecurity-predictions-for-2023-2025

IBM (X-Force) (2022) | *6 IBM cybersecurity predictions for 2023: Ransomware and CaaS will spike.* Obtenido de:
https://venturebeat.com/security/ibm-cybersecurity-predictions/

IBM (X-Force) (2022) | *Cybersecurity Trends: IBM's Predictions for 2023.* Obtenido de:
https://securityintelligence.com/articles/cybersecurity-trends-ibm-predictions-2023/

Kaspersky (2022) | *Advanced threat predictions for 2023.* Obtenido de:
https://securelist.com/advanced-threat-predictions-for-2023/107939/

Kaspersky (2022) | *Kaspersky predicts shifts in threat landscape to industrial control systems in 2023.* Obtenido de:
https://www.kaspersky.com/about/press-releases/2022_kaspersky-predicts-shifts-in-threat-landscape-to-industrial-control-systems-in-2023

Mandiant (2022) | *M-Trends 2022: Métricas de ciberseguridad, conocimientos y orientación desde la primera línea.* Obtenido de:
https://www.mandiant.es/resources/m-trends-2022

Nozomi Networks (2022) | *Cuatro perspectivas que marcarán la agenda de la ciberseguridad industrial en 2023.* Obtenido de:
https://technocio.com/cuatro-perspectivas-que-marcaran-la-agenda-de-la-ciberseguridad-industrial-en-2023/

Red Seguridad (2022) | *Cinco predicciones de ciberseguridad para 2023.* Obtenido de:
https://www.redseguridad.com/actualidad/cibercrimen/cinco-predicciones-de-ciberseguridad-para-2023_20221216.html

SANS (2022) | *The State of ICS/OT Cybersecurity in 2022 and Beyond. Cyolo.* Obtenido de:
https://www.sans.org/white-papers/state-ics-ot-cybersecurity-2022-beyond/

Trend Micro (2022) | *Future / Tense: Trend Microsecurity Predictions for 2023.* Obtenido de:
https://www.trendmicro.com/vinfo/us/security/research-and-analysis/predictions/2023

WatchGuard Technologies (2022) | *Watchguard's 2023 Cybersecurity Predictions.* Obtenido de:
https://www.watchguard.com/wgrd-resource-center/cyber-security-predictions

www.seresco.es