sedian

Seguridad Digital
de Andalucía

Informe

Predicciones de amenazas para el 2022

Tipo de documento: Informe

Autor del documento: AndalucíaCERT

Código del documento: CERT-IF-145238

Edición: 0

Categoría: Público

Fecha de elaboración: 17/01/2022

Junta de Andalucía

Tabla de contenidos

Objeto

El objeto de este documento es dar a conocer las predicciones de aquellos riesgos y amenazas que acontecerán en el año 2022 en base a las tendencias actuales de ciberdelincuencia.

Para ello, se resumirán las predicciones realizadas por algunas de las principales empresas referentes en el mundo de la ciberseguridad.

Alcance

Este documento va dirigido tanto al personal de la Junta de Andalucía como al publico en general.

Debe contemplarse como una visión general de aquellos aspectos que puedan afectar a lo largo de este año 2022 en cuanto a lo que en ciberseguridad se refiere.

Este informe no posee una certeza absoluta acerca de sus predicciones, pero puede servir como guía de estado y evolución de los distintos riesgos y amenazas, así como de las medidas a tomar ante ellas.

Introducción

Con la implantación generalizada del teletrabajo han aparecido nuevos retos a la hora de mantener la seguridad de la información, convirtiéndose en un desafío cada vez mayor.

En la actualidad se han consolidado ataques como ransomware coexistiendo con ataques tradicionales como SPAM, phishing o malware.

Ante este panorama, desde AndalucíaCERT se ha considerado oportuno elaborar el presente informe divulgativo, con el objetivo de que el lector pueda hacerse una idea de lo que deparará el año 2022 en cuanto a lo que en ciberseguridad se refiere.

Predicciones de las principales empresas del sector

En este epígrafe se resumirán las principales predicciones acerca de los riesgos y amenazas que tendrán lugar este año según los informes elaborados por algunas de las principales empresas del sector.

Fortinet

- Uso de IA por parte de los atacantes

  En la actualidad se utiliza la IA (Inteligencia Artificial) por parte de los equipos de defensa para detectar comportamientos inusuales que puedan indicar un ataque. Se prevé que los cibercriminales emplearán la IA para frustrar estos algoritmos e impedir que puedan utilizarse para detectar comportamientos anómalos.

  El deepfake es una de las preocupaciones crecientes, ya que aprovecha la IA para imitar actividades humanas que pueden ser utilizadas en ingeniería social. Un ejemplo de ello es GPT-3, que realiza un aprendizaje profundo de idiomas, lo que permite aprovechar correos electrónicos legítimos secuestrados para producir nuevos correos y respuestas más convincentes que permitan incluso mencionar conversaciones pasadas.

Por estos ejemplos y otras herramientas que se encuentran en desarrollo para permitir suplantar la voz o la imagen de otra persona en tiempo real, se considera que los ataques del futuro pueden tener como base la IA.

- Ransomware más destructivo

  El ransomware tradicionalmente se ha basado en su capacidad de cifrar y corromper datos para obligar a las organizaciones a pagar. Se están detectando ransomware con malware *Wiper*, que permite poder eliminar datos y paralizar sistemas críticos, a menos que se cumpla con las peticiones de los atacantes.

  Este es un paso más allá en la extorsión que se viene realizando por parte de los cibercriminales, que hasta ahora amenazaban con publicar datos robados o incluso contactaban con clientes de la víctima para presionar y que se realizase el pago demandado. Se han detectado casos en los que incluso los atacantes no cifran los datos, simplemente los roban y amenazan con publicarlos.

  Los atacantes de ransomware están combinando sus ataques con DDoS para saturar a los equipos de respuesta y limitar las posibles acciones de mitigación. Esto junto al malware *Wiper*, que amenaza con destruir sistemas y hardware, crea una urgencia adicional para que las víctimas cedan a los chantajes y paguen la cantidad solicitada

- Ataques a redes satelitales:

  El internet por satélite sigue creciendo gracias a los nuevos sistemas LEO (low earth orbit) que consiguen altas velocidades y reducen el precio. Por esto se esperan nuevas pruebas de concepto dirigidas a este tipo de redes como ICARUS, que es un ataque DDoS que aprovecha la accesibilidad global directa a los satélites para lanzar ataques desde numerosas ubicaciones.

  Los principales objetivos serán las organizaciones que dependen de este tipo de conexiones como juegos online, servicios críticos en ubicaciones remotas, oleoductos, cruceros, aerolíneas... Se prevé que aparecerán ataques como ransomware sobre esta infraestructura.

  Las redes satelitales supondrán una ampliación de la superficie de ataque a medida que las organizaciones conecten a este tipo de redes sistemas que antes se encontraban fuera de la red.

- Cripto Wallets:

  En los últimos años se ha detectado una disminución de los troyanos dirigidos a transacciones bancarias y transferencias electrónicas. Los bancos han mejorado en la detección y prevención frente a malware y fraude, lo que hace que cada vez más los delincuentes busquen otras alternativas.

Se ha detectado una nueva amenaza en la que se utiliza un generador de tarjetas regalo de Amazon falso para monitorear el portapapeles de la víctima en busca de direcciones de billeteras para remplazarlas por la del atacante, recibiendo así las posibles transacciones que tratase de realizar la víctima. Junto con este ataque se detectan cada vez más casos de phishing y malware diseñados exclusivamente para robar criptowallets.

Se espera que este tipo de malware aumente, no solo porque para los delincuentes es más fácil robar este tipo de billeteras, sino porque se espera que cada vez más empresas realicen este tipo de transacciones.

- Deportes electrónicos:

Los eSports o deportes electrónicos se han afianzado en la sociedad siendo un reclamo para cada vez más usuarios, competidores y profesionales, lo que ha generado una industria que se prevé que alcance un volumen de ingresos de 1.800 millones de dólares en 2022.

Este crecimiento hace que cada vez más salas de juego online y casinos los incluyan entre sus opciones de apuestas para aumentar sus ingresos.

Por este crecimiento se considera que los eSports pueden ser un objetivo atractivo para los atacantes, ya sea por ransomware, robos o ingeniería social. Y se espera que sean grandes objetivos en 2022.

McAfee

- Crecimiento de las redes sociales como vector de entrada

  Con el auge de las redes sociales en los últimos años se espera que se utilicen éstas como método de contacto por los actores maliciosos.

  Existen casos en los que supuestos perfiles con cargo directivo contactan con empleados de empresas objetivo directamente para eludir los sistemas de seguridad tradicionales, llegando en algunos casos a tomar el control de las cuentas de la víctima y expandiendo su mensaje desde la cuenta robada.

  Se ha demostrado que apuntar a los individuos es muy exitoso, por lo que se predice que este vector podría crecer no solo a través de grupos de espionaje, sino también de otros actores de amenazas que buscan infiltrarse en organizaciones para su propio beneficio criminal.

- Game of ransomware Thrones

Durante varios años, los ataques de ransomware han sido las amenazas cibernéticas con mayor impacto. El modelo de Ransomware-as-a-Service (RaaS) abrió las puertas de la ciberdelincuencia a actores menos cualificados, lo que finalmente condujo a más brechas de seguridad y mayores beneficios por parte de los delincuentes.

Durante mucho tiempo, los administradores y desarrolladores de RaaS han sido los más perseguidos por las autoridades, descuidando a quienes adquirían este tipo de malware, ya que se los consideraba menos cualificados. Esto creó una atmósfera en la que esos compradores menos cualificados podían prosperar y convertirse en ciberdelincuentes muy competentes.

En los últimos tiempos los populares foros de ciberdelincuencia han prohibido la publicidad de los actores de ransomware, por lo que los grupos RaaS no tienen una plataforma en la que reclutar clientes, desencadenando una falta de visibilidad, lo que dificulta que los desarrolladores de RaaS mantengan su posición actual en la clandestinidad.

Esto desembocará en que cada vez surjan más grupos de ciberdelincuencia autosuficientes y cambien el equilibrio de poder dentro del ecosistema RaaS, de aquellos que controlan el ransomware a aquellos que controlan las redes de la víctima.

- API

Los actores de amenazas prestan atención a las estadísticas y tendencias empresariales, identificando servicios y aplicaciones que ofrecen mayor riesgo potencial. Las aplicaciones en la nube han transformado la forma en que los desarrolladores de software diseñan, consumen y aprovechan las API. El alcance y la popularidad de algunas de estas aplicaciones en la nube, así como los datos y capacidades críticos para el negocio que se encuentran detrás de estas API, las convierten en un objetivo lucrativo para los actores de amenazas. Esto convierte las API en un vector de entrada para ataques más amplios.

Entre los riesgos clave que se espera que aumenten en el futuro está una posible configuración incorrecta de la API, que se puedan explotar los mecanismos de autenticación, evolución de los ataques de malware tradicionales para usar más las API, uso indebido de API para lanzar ataques a los datos empresariales, etc.

Por estos motivos se debería contar con mejores métodos de seguridad y mayor telemetría sobre esta tecnología para evitar un mal uso de la misma.

- Secuestro de contenedores

Los dockers o contenedores han adquirido un mayor protagonismo en los últimos años, convirtiéndose en la plataforma predilecta para las aplicaciones en la nube por su

portabilidad, eficiencia y velocidad. Esta nueva tecnología aumenta la superficie de ataque de la organización, para la cual se prevé que estos sean los riesgos clave:

- Riesgos en el orquestador: aumentarán los ataques en la capa de orquestación, como Kubernetes y la API asociada, impulsados principalmente por configuraciones incorrectas.

- Riesgo de imagen o registro: aumento en el uso de imágenes maliciosas o de puerta trasera aprovechando controles de vulnerabilidad insuficientes.

- Riesgos de contenedores: aumento de los ataques dirigidos a las aplicaciones vulnerables que estos albergan.

Explotar estos riesgos puede derivar en el secuestro de recursos para su utilización en malware de criptominería, robo de datos, mantener persistencia y escapar de contenedores al sistema anfitrión.

Kaspersky

- Amenazas financieras en 2022

Las criptomonedas son un activo digital, por lo que todas sus transacciones se producen online. Esta característica ofrece, entre otras cosas, cierto grado de anonimato a los usuarios que

las realizan. Esto atrae de manera significativa a los grupos de ciberdelincuentes e incluso a actores de amenaza patrocinados. Se han empezado a ver grupos de APT que se han dedicado a atacar el negocio de las criptomonedas y se prevé que esta actividad aumentará.

La forma en la que se realizan estos ataques evoluciona con el tiempo y cada vez aparecen nuevas formas de robar los activos financieros de los usuarios. En el caso concreto de las criptodivisas, los ciberdelincuentes se aprovechan de la fabricación y venta de dispositivos falsos incluyendo puertas traseras, realizando campañas de ingeniería social…

Además de las técnicas mencionadas se espera que se consoliden los ataques contra activos mediante infostealers (troyanos que roban información), ya que resultan sencillos y eficaces para los atacantes, por lo que se seguirán empleando en las primeras fases de los ataques.

Por ultimo, se prevé que se desarrollen cada vez más troyanos bancarios para móviles, especialmente para el sistema operativo Android, que permitan a los atacantes eludir los medios de seguridad de doble factor de autenticación implementados por las entidades bancarias.

- Peligros de la atención médica “conectada”

La telemedicina cuenta cada vez con más usuarios y se prevé que seguirá avanzando en los próximos años. Esto significa que habrá más aplicaciones para consultas médicas y el control de la salud de los pacientes, y los ciberdelincuentes tendrán la oportunidad de descubrir huecos en la seguridad en nuevas aplicaciones creadas por desarrolladores que nunca habían fabricado este tipo de productos. Además, es probable que aparezcan falsificaciones maliciosas de aplicaciones de telesalud en tiendas de aplicaciones: aplicaciones falsas que imiten a las verdaderas y prometan prestar la misma funcionalidad.

Por ende, la demanda de documentos médicos digitales falsos aumentará, al igual que la oferta. Cuantos más privilegios se les den a aquellos con un pasaporte COVID, más personas querrán comprar uno en lugar de vacunarse o hacerse pruebas.

La sensibilidad de los datos médicos que se encuentran en las filtraciones aumentará. Los datos contenidos en las historias clínicas son, en sí mismos, altamente sensibles. Sin embargo, las posibilidades de digitalización para los equipos médicos están en aumento, y los proveedores usan con más frecuencia dispositivos que pueden incorporarse a nuestro cuerpo o incluso sensores implantados en el cuerpo humano para recolectar información aún más sensible que no es necesariamente de naturaleza médica. Estos dispositivos pueden, por ejemplo, proporcionar detalles de los movimientos de una persona.

El tema médico será siempre un tema popular para utilizar en delitos cibernéticos. Desde el comienzo de la pandemia un número cada vez mayor de servicios médicos se trasladó a medios en línea, ya sea en parte o en su totalidad, por lo tanto, los pacientes ahora esperan notificaciones acerca de resultados de pruebas y mensajes de médicos. Por eso, un mensaje que falsamente se anuncie como una notificación “médica” importante puede tener tanto éxito para atrapar víctimas desprevenidas como los mensajes falsos de bancos.

El crecimiento en la cantidad de filtraciones de datos y ataques de ransomware en organizaciones médicas da cuenta, entre otras cosas, de una falta de consciencia con respecto a la seguridad de la información por parte de los empleados de atención médica. Si durante el año 2022 no se lleva a cabo de un proceso de capacitación a gran escala, lo cual no se espera por el momento, seremos testigos de un aumento continuado en este tipo de ataques.

Trend Micro

- Aumentarán los ataques en la nube

  El empleo de la nube y diferentes servicios en la misma por parte de las organizaciones ha aumentado notablemente y cada vez más compañías migran parte de su infraestructura a este modelo. Para aumentar sus ganancias los criminales deben

estar capacitados para cubrir todas las modalidades y poder atacar nuevas tecnologías.

Se prevé que continúen los ataques mediante phishing para robar credenciales de diferentes plataformas en la nube, pero también se accederá a aplicaciones o soluciones SaaS por otras vías, como contraseñas inseguras, claves no rotadas, contenedores inseguros obtenidos de fuentes no confiables...

Un efecto secundario del movimiento a plataformas en la nube es que los atacantes comenzarán a utilizar este enfoque en sus ataques, por lo que comenzarán a atacar en entornos de desarrollo en la nube o entornos DevOps. Desde TrendMicro se predice que los cibercriminales realizarán más campañas utilizando los principios de DevOps en las cadenas de suministros, Kubernetes e implementaciones de Infraestructure-as-code (IaC). Por este motivo se considera que los desarrolladores y los sistemas de compilación servirán como punto de entrada para que los atacantes puedan propagar malware a través de ataques a la cadena de suministro. Los tokens y las contraseñas de los desarrolladores contienen la claves para las operaciones de las empresas, y el uso de las credenciales de un desarrollador comprometido también aumenta la posibilidad del atacante de introducir malware sin ser detectado.

- Los servidores serán el principal campo de juego del ransomware

  Como cualquier amenaza, el ransomware sobrevive y prospera gracias a una evolución constante. Antes, los incidentes de ransomware se producían generalmente en los equipos finales de usuarios tras abrir correos electrónicos maliciosos o accediendo a URLs. Pero desde el comienzo de la pandemia se detectó un importante cambio en la tendencia en la forma de actuar de los operadores de ransomware.

  Los actores maliciosos ahora se enfocan en los servidores con servicios expuestos. Con el modelo híbrido de trabajo adoptado por muchas empresas, modelo en el que los empleados trabajan tanto remotamente como en las oficinas, se prevé que esta tendencia continúe los próximos años. Debido a la mayor superficie de ataque expuesta es más difícil para los equipos de ciberseguridad detener el ransomware en tiempo cero.

  Se prevé que los ataques de ransomware sean más específicos haciendo que las posibles medidas de defensa a nivel de red tomadas por las compañías no sean tan efectivas. Al ser relativamente nuevos los ataques de ransomware sobre servidores requieren realizar una inversión en protección al igual que se hacía en los equipos de usuarios.

El segundo punto en el que se espera que evolucionen los ataques de ransomware es que cada vez cobrará más importancia la extorsión y menos el cifrado. Se filtrarán y robarán datos confidenciales y con estos datos se extorsionará a la víctima pasando por alto incluso la fase de cifrado y bloqueo de acceso a los mismos. Los vectores de ataque, además de VPN, correos de phishing y puertos RDP expuestos, se trasladarán a la nube como objetivo más frecuente.

- Los equipos de seguridad deberán estar mejor equipados para contener posibles explotaciones de vulnerabilidades antiguas y nuevas.

  Se prevé que 2022 rivalice con 2021 como el año en que más vulnerabilidades *Zero-day* se detecten. En 2021 fueron 66 los exploit de este tipo descubiertos. El aumento del número de vulnerabilidades detectadas no sugiere que se esté reduciendo la calidad del código desarrollado, sino que cada vez hay más factores que animan a reportar el descubrimiento de vulnerabilidades por parte de los profesionales, como programas de recompensas.

  Cada vez se reducirá más la ventana de tiempo desde que se descubre una vulnerabilidad hasta que se escribe un exploit funcional, pasando de días a cuestión de horas, aprovechando el tiempo que pasa desde que se descubre la vulnerabilidad hasta que se implementa un parche para solucionarla. Los

tiempos de respuesta no son uniformes ya que no se emplea el mismo plan para parchear equipos finales que para parchear servidores.

En lugar de estudiar fragmentos de código para descubrir fallos y explotarlos, los actores maliciosos utilizarán los parches de seguridad para detectar qué funcionalidades contenían errores y adaptar su malware para aprovecharlo .

Más que nunca, las empresas deberán asegurarse de que sus equipos de seguridad de TI estén bien posicionados para adaptarse y abordar este aumento inminente de exploit. Esto implicará proporcionar a estos equipos el apoyo y los recursos que necesitarán para hacer un inventario de los dispositivos en un entorno de TI a través de la gestión de activos, supervisar las actualizaciones de seguridad de los proveedores para que puedan solventar lo antes posible las vulnerabilidades que se divulgan públicamente y aplicar parches virtuales o aislamiento de máquinas para proteger cualquier posible punto de entrada de amenazas.

- Las empresas se esforzarán por mejorar la monitorización y visibilidad de la red para proteger sus entornos IT contra las amenazas surgidas de la adopción de IoT.

  Los dispositivos inteligentes han sido objetivo de los atacantes ya que generalmente existe una menor capacidad de securizar

este tipo de dispositivos por parte de las empresas y es posible utilizarlos en diversos tipos de ataque como DDoS.

Para seguir siendo seguras las empresas recurrirán a sistemas como IDS o IPS, herramientas de análisis forense de red (NFTs), herramientas de detección de comportamiento anómalo (NBAD), herramientas NDR... En el caso de empresas que estén adoptando un modelo basado en la nube será necesario realizar un seguimiento del uso de recursos basados en la nube para detectar cualquier actividad anómala.

En 2022 los actores maliciosos tendrán aspiraciones más elevadas, que irán más allá del secuestro de dispositivos IoT como una base de ataque para su actividad delictiva o como un medio para moverse lateralmente dentro de una red. Los ciberdelincuentes tratarán de atacar estos dispositivos a medida que más fabricantes de automóviles, como General Motors, Honda y Toyota, utilicen los datos entregados por los automóviles conectados. Estos vehículos vienen equipados con una variedad de cámaras, láseres y otros sensores que registran las condiciones de conducción y el comportamiento del conductor, incluidas las velocidades y distancias de conducción de un automóvil, y los tipos de medios de entretenimiento consumidos por sus pasajeros. Estos conocimientos en tiempo real tienen una gran variedad de aplicaciones para clientes comerciales, como medir el éxito de la publicidad, evaluar la demanda del consumidor y determinar

descuentos en seguros de automóviles en función de los datos de conducción. Para los fabricantes de automóviles, estos datos también podrían usarse para monitorizar el funcionamiento de los diferentes componentes de vehículos, lo que mejoraría sus propias cadenas de suministro.

A medida que más de estos vehículos salgan a la carretera, los actores malintencionados se preparan para obtener ganancias de la mayor conectividad. La arquitectura de los automóviles inteligentes también se puede simplificar aún más si sus funciones y procesos de recopilación de datos más complejos se transfieren a la nube; de hecho, muchas aplicaciones y sistemas utilizados por los modelos de automóviles inteligentes más nuevos ya están alojados en servidores back-end en la nube, pero hacerlo podría exponer a los fabricantes de automóviles a otras amenazas, como DoS y man-in-the-middle (MitM).

Por estos motivos es importante que los diferentes fabricantes de coches inteligentes colaboren con proveedores de seguridad que permitan que este desarrollo se lleve a cabo de una forma segura.

- Amenazas en la cadena de suministro

La pandemia ha puesto de relieve la fragilidad de las cadenas de suministro. Se han producido grandes escaseces y retrasos debido a varios factores como aumento de la demanda, escasez

de contenedores de envío, problemas a la hora de encontrar trabajadores... Estos problemas han puesto en valor a las cadenas de suministros, lo que también ha llamado la atención de los delincuentes.

Aprovechando la gran interrupción en la cadena de suministro a nivel mundial, los actores malintencionados generarán un aumento en el modelo de extorsión cuádruple en 2022. Aprovecharán al máximo sus ataques cibernéticos obligando a las víctimas de renombre a pagar grandes sumas de dinero a través de una técnica de extorsión cuádruple: retener los datos críticos de la víctima a cambio de un rescate, amenazar con filtrar los datos y hacer pública la violación, amenazar con perseguir a los clientes de la víctima y atacar la cadena de suministro de la víctima o vendedores.

En 2021 el grupo de ciberdelincuentes DarkSide atacó el sistema de oleoductos más grande de EE.UU., Colonial Pipeline, impidiendo que la empresa accediera a sus sistemas informáticos y robando más de 100GB de datos corporativos. Siguiendo este ejemplo los actores malintencionados podrían denegar el acceso a datos críticos, como secretos de fabricación, retener el acceso a máquinas de producción, contactar con clientes y partes interesadas para presionar a las empresas para que paguen...

Las cadenas de suministro también serán el centro de atención de los intermediarios de acceso como servicio (AaaS). Una vez que los entornos vulnerables se ven comprometidos, los corredores de AaaS pueden vender el acceso a la red de la empresa, las cuentas administrativas y las credenciales de autenticación a los ciberdelincuentes a precios variables.

Check Point

- Fake news y desinformación.

El reclamo de '*fake news*' en torno a temas polémicos se ha convertido en un nuevo vector de ataque en años anteriores sin que la gente comprenda realmente su impacto total. A lo largo de 2021, se difundió información errónea sobre la pandemia de COVID-19 y la información de vacunación. El mercado negro de certificados de vacunas falsos se expandió a nivel mundial y ahora se venden falsificaciones de 29 países . Los pasaporte COVID falsos estaban a la venta por unos 100 dólares y el volumen de anuncios y vendedores se multiplicó durante todo el año. En 2022, los grupos cibernéticos continuarán aprovechando este tipo de campañas de noticias falsas para ejecutar varios ataques de phishing y estafas.

Además, antes de las elecciones presidenciales de EE. UU. de 2020, los investigadores de Check Point detectaron aumentos repentinos en dominios maliciosos relacionados con las

elecciones y el uso de "memes camuflados" destinado a cambiar la opinión pública. En el período previo a las elecciones de medio mandato de EE. UU. en noviembre de 2022, podemos esperar ver estas actividades en pleno efecto y el regreso de las campañas de desinformación en las redes sociales.

- Ataques a la cadena de suministro

  Los atacantes de la cadena de suministro se aprovechan de la falta de supervisión dentro del entorno de una organización permitiéndoles realizar cualquier tipo de ciberataque, como violaciones de datos e infecciones de malware. El conocido ataque a la cadena de suministro de SolarWinds se destaca en 2021 debido a su escala e influencia, pero se han producido otros ataques sofisticados a la cadena de suministro, como Codecov en abril y, más recientemente, Kaseya. Kaseya proporciona software para proveedores de servicios administrados (MSP) y el grupo de ransomware REvil explotó a la empresa para infectar a más de 1000 clientes con ransomware. El grupo exigió un rescate de 70 millones de dolares para proporcionar claves de descifrado para todos los clientes afectados.

  Los ataques a la cadena de suministro se volverán más comunes y los gobiernos comenzarán a establecer regulaciones para abordar estos ataques y proteger las redes. También buscarán colaborar con los sectores privados y otros países

para identificar y apuntar a más grupos de amenazas que operan a escala global y regional.

- La ‘guerra fría’ cibernética se intensifica

  La guerra fría cibernética se está intensificando y tiene lugar online a medida que más actores de los estados nacionales presionan a los gobiernos occidentales para seguir desestabilizando la sociedad. La infraestructura mejorada y las capacidades tecnológicas permitirán que los grupos terroristas y los activistas políticos avancen en sus agendas y lleven a cabo ataques generalizados más sofisticados. Los ataques cibernéticos se utilizarán cada vez más como conflictos indirectos para desestabilizar las actividades a nivel mundial.

- Filtraciones de datos a mayor escala

  En 2022 veremos un aumento en las filtraciones de datos que serán de mayor escala. Estas infracciones también tendrán el potencial de costar más a las organizaciones y los gobiernos para recuperarse. En mayo de 2021, una gran compañía de seguros de EE. UU. pagó un rescate de 40 millones de dólares a atacantes informáticos. Este fue un récord, y podemos esperar que el rescate exigido por los atacantes aumente en 2022.

- Aumento de malware móvil

En 2021, el 46 % de las organizaciones tenían al menos un empleado que descargaba una aplicación móvil maliciosa. El paso al trabajo remoto para casi poblaciones enteras en todo el mundo durante la pandemia de COVID-19 vio cómo la superficie de ataque móvil se expandía drásticamente, lo que resultó en que el 97 % de las organizaciones se enfrentarán a amenazas móviles de varios vectores de ataque. A medida que las billeteras móviles y las plataformas de pago móvil se utilicen con mayor frecuencia, los ciberdelincuentes evolucionarán y adaptarán sus técnicas para explotar la creciente dependencia de los dispositivos móviles.

- Criptomonedas en el punto de mira de los atacantes

  Cuando el dinero se convierte en puro software, la seguridad cibernética necesaria para protegerse contra los atacantes informáticos que roban y manipulan bitcoins y altcoins seguramente cambiará de manera inesperada. A medida que los informes de Cryptohacking desencadenados por NFT gratuitos se vuelven más frecuentes, Check Point Research (CPR) investigó OpenSea y demostró que era posible robar las billeteras criptográficas de los usuarios. En 2022, podemos esperar ver un aumento en los ataques relacionados con criptomonedas.

- Los atacantes aprovechan las vulnerabilidades de los microservicios para lanzar ataques a gran escala

El cambio a la nube y DevOps dará como resultado una nueva forma de botnet. Con los microservicios convirtiéndose en el método líder para el desarrollo de aplicaciones y la arquitectura de microservicios adoptada por los proveedores de servicios en la nube (CSP), los atacantes están utilizando las vulnerabilidades que se encuentran en los microservicios para lanzar sus ataques. También podemos esperar ver ataques a gran escala dirigidos a los CSP.

- Los atacantes usan la tecnología deepfake como arma

  Las técnicas para videos o audios falsos ahora son lo suficientemente avanzadas como para usarlas como armas y crear contenido específico para manipular opiniones, precios de acciones u otras acciones. Como en el caso de otros ataques móviles que se basan en la ingeniería social, los resultados de un ataque de phishing pueden variar desde el fraude hasta el espionaje más avanzado. Por ejemplo, en uno de los ataques de phishing deepfake más importantes, un gerente de banco en los Emiratos Árabes Unidos fue víctima de la estafa de un atacante que utilizó la clonación de voz de IA para engañar al gerente del banco para que transfiriera 35 millones de dólares. Los actores de amenazas utilizarán ataques de ingeniería social deepfake para obtener permisos y acceder a datos confidenciales.

- Las herramientas de penetración continúan creciendo

A nivel mundial en 2021, 1 de cada 61 organizaciones se vio afectada por ransomware cada semana. El ransomware seguirá creciendo, a pesar de los esfuerzos de las fuerzas del orden para limitar este crecimiento a nivel mundial. Los actores de amenazas apuntarán a las empresas que pueden pagar el rescate, y los ataques de ransomware se volverán más sofisticados en 2022. Los delincuentes informáticos utilizarán cada vez más herramientas de penetración para personalizar los ataques en tiempo real y trabajar dentro de las redes de las víctimas. Las herramientas de penetración son el motor detrás de los ataques de ransomware más sofisticados que tuvieron lugar en 2021. A medida que crece la popularidad de este método de ataque, los atacantes lo utilizarán para llevar a cabo ataques de extorsión y exfiltración de datos.

SOPHOS

- El futuro del ransomware

El ransomware ha reivindicado su posición como protagonista del ecosistema de la ciberdelincuencia. Como uno de los tipos de ataques de malware más dañinos y costosos, el ransomware sigue siendo la clase de amenaza cibernética que mantiene en vela a la mayoría de administradores. En 2022, el ransomware no da señales de remitir, aunque su modelo de negocio ha

experimentado algunos cambios que parece que persistirán e incluso crecerán durante el próximo año.

El ransomware no es nuevo, pero ha habido cambios significativos en el panorama de esta amenaza durante este periodo: el blanco son ahora organizaciones cada vez más grandes y el modelo de negocio que dicta la mecánica de los ataques ha cambiado.

El cambio más importante es el paso de delincuentes "orientados verticalmente", que crean ransomware y luego atacan a organizaciones utilizando su propio código a medida, a un modelo en que un grupo genera el ransomware y luego alquila su uso a especialistas en el tipo de allanamiento virtual que requiere un conjunto de habilidades distinto al de los creadores del ransomware. Este modelo de ransomware como servicio (o RaaS) ha cambiado el panorama de formas que no podíamos predecir.

Sophos cree que, en 2022 y en años posteriores, el modelo de negocio RaaS seguirá dominando el panorama de amenazas para los ataques de ransomware, ya que es un modelo que permite a los expertos en la creación de ransomware seguir desarrollando y mejorando su producto, a la vez que da a los expertos en irrupciones de "acceso inicial" la posibilidad de centrarse en esa tarea con mayor intensidad. Se ha visto a estos ejecutores de RaaS innovar en nuevas formas de penetrar

en redes cada vez mejor protegidas, y se prevé que seguirán avanzando en esta dirección en el próximo año.

Los atacantes aprovecharon el hecho de que el "tiempo de permanencia" medio (durante el que tienen acceso a la red de una organización objetivo) puede ser de días a semanas, y empezaron a utilizar ese tiempo para descubrir los secretos de una organización y trasladar todo lo que les pareciera de valor a un servicio de copia de seguridad en la nube. Después, al lanzar el ataque de ransomware, añadían una segunda amenaza: pague o haremos públicos sus documentos internos más sensibles, los datos de sus clientes, su código fuente, los historiales de sus pacientes o cualquier otra cosa.

Es una estrategia que ha devuelto el poder a los atacantes del ransomware. Las grandes organizaciones no solo se enfrentan a una reacción negativa de los clientes, sino que también podrían sucumbir ante las leyes de privacidad, como el RGPD europeo, si no evitan la divulgación de información de identificación personal perteneciente a clientes o consumidores, por no hablar de la pérdida de secretos comerciales a manos de la competencia. En lugar de arriesgarse a las consecuencias normativas (o bursátiles) de una revelación de tal calibre, muchas de las organizaciones afectadas optan por pagar el rescate (o hacer que su compañía de seguros lo haga). Naturalmente, los atacantes pueden entonces hacer lo que

quieran, incluso vender esos datos competitivos sensibles a otros, pero las víctimas no pueden resistirse.

- El malware engendra malware

  Cobalt Strike es una suite de herramientas de explotación producida comercialmente destinada a la "emulación de amenazas", es decir, a reproducir los tipos de técnicas utilizadas por los ciberdelincuentes. Lanzada por primera vez en 2012, suele ser utilizada por los técnicos de pruebas de penetración y los red team corporativos como parte del conjunto de herramientas de "seguridad ofensiva".

  El aspecto comercial de Cobalt Strike es su puerta trasera Beacon, que puede configurarse de varias maneras para ejecutar comandos, descargar y ejecutar software adicional, y retransmitir comandos a otras cargas Beacon instaladas en una red objetivo. Las cargas Beacon pueden personalizarse para emular una gran variedad de amenazas. Por desgracia, también pueden utilizarse con malas intenciones. De hecho, las cargas Beacon son tan buenas que los delincuentes solo tienen que hacer pequeñas modificaciones en el código fuente para utilizar la carga con el objetivo de afianzarse en un equipo infectado.

  Esto se ha convertido en un importante motivo de preocupación en los últimos años, ya que copias filtradas del código fuente de la suite, brechas en su estructura de licencias y versiones

completas pirateadas de Cobalt Strike han llegado a manos de un tipo de usuario muy diferente de la base de clientes prevista del producto.

Como resultado, la mayoría de los casos de ransomware que hemos visto en el último año han implicado el uso de cargas Beacon de Cobalt Strike. Mientras que muchos operadores de malware utilizan puertas traseras asociadas a la plataforma de código abierto Metasploit, Beacon de Cobalt Strike se ha convertido en la herramienta favorita de los afiliados del ransomware y de los brókeres de acceso que venden vulnerabilidades a las bandas de ransomware y a menudo se la relaciona con la ejecución del ransomware. También hemos observado que otros operadores de malware, incluido el extractor de criptomonedas LemonDuck, utilizan Cobalt Strike para el acceso y la propagación lateral.

En algunos casos, las cargas Beacon son distribuidas por documentos maliciosos mediante SPAM u otros instaladores, o a través de exploit de servidor que permiten que las cargas se instalen e inicien de forma remota. En otros, Beacon se utiliza para realizar gran parte de la penetración en la red y para ejecutar el propio ransomware.

Prevemos que esta tendencia continúe. Herramientas como Cobalt Strike facilitan que las bandas de ransomware amplíen sus operaciones, utilizando manuales de estrategias y

herramientas para guiar a los afiliados en la consecución de sus objetivos, y es probable que más intrusiones sean impulsadas por cargas Beacon por este motivo.

Dado que muchas de las familias de malware más distribuidas también convierten a un equipo infectado en un posible receptor de Cobalt Strike o de cargas de malware, es poco probable que la faceta de plataforma de distribución de malware de estas familias de malware llegue a desaparecer. Por desgracia, esto significa que los administradores y los equipos de seguridad deben tratar con prontitud incluso las alertas de malware leves, ya que cualquier infección, por insignificante que parezca, puede ser simplemente el comienzo de un ciberataque mucho más devastador.

- Seguridad e IA

Aunque todavía no hemos visto una adopción generalizada de estas nuevas tecnologías por parte de los adversarios, es de esperar que se produzca en los próximos años, por ejemplo, en la generación de contenidos web de Watering hole y correos electrónicos de phishing. No muy por detrás de ellas en el "proceso de industrialización" de la IA estarán las tecnologías de síntesis de voz de redes neuronales y la tecnología del deepfake de vídeo, menos avanzadas que las tecnologías de IA en el ámbito de la imagen y el texto.

Este año se han visto más pruebas de que la tecnología de redes neuronales seguirá alterando viejas y nuevas áreas de la ciberdefensa. Destacan dos innovaciones en este sentido. En primer lugar, un equipo de Google, DeepMind, ha desarrollado una solución innovadora, AlphaFold, para predecir la estructura tridimensional de las proteínas a partir de registros de sus secuencias de aminoácidos, un logro reconocido como positivamente transformador para la biología y la medicina. Aunque el traspaso de este tipo de tecnología a la seguridad no se ha explorado a fondo, el avance de AlphaFold sugiere que, al igual que en la biología, las redes neuronales pueden ser la clave para resolver problemas que antes se consideraban inabordables en la seguridad. En segundo lugar, y también dignos de mención, están los avances demostrados que han conseguido los investigadores en la aplicación de redes neuronales a la generación de código fuente. Expertos tanto de Google como de OpenAI han demostrado de forma independiente que los investigadores pueden servirse de las redes neuronales para producir código fuente basado en instrucciones de lenguaje natural no estructurado. Estas demostraciones sugieren que solo es cuestión de tiempo hasta que los adversarios adopten las redes neuronales para reducir el coste de generar malware inédito o muy variable. También es imperativo que los encargados de la seguridad investiguen la utilización de las redes neuronales conscientes del código fuente para detectar mejor el código malicioso. Estos avances

conducen a una conclusión principal: la revolución de la IA dista mucho de haber terminado, y los profesionales de la seguridad harían bien en seguir su ritmo y encontrar aplicaciones defensivas de los nuevos planteamientos y tecnologías de la IA.

En 2022 y posteriormente, las empresas innovadoras de ciberseguridad se distinguirán por demostrar nuevas aplicaciones del *machine learning*. Aún se considera que hay campos en los que se necesita seguir avanzando.

El primero es el ámbito poco explorado del *machine learning* aplicado a la seguridad y orientado al usuario. Creemos que, en los próximos años, el ML orientado al usuario hará que los productos de seguridad TI sean tan intuitivos a la hora de hacer recomendaciones de seguridad como lo es Google para encontrar páginas web y Netflix para sugerir contenidos. El centro de operaciones de seguridad (SOC) basado en IA resultante será mucho más fácil de usar y más eficiente que los SOC actuales.

Los dispositivos del Internet de las cosas (IoT) que ejecutan un shell Linux de BusyBox de funciones limitadas también siguen siendo un objetivo para los gusanos que distribuyen criptomineros y otro malware molesto en dispositivos de uso común como router o almacenamiento conectado a la red. Las redes de bot como Mirai se aprovechan de las contraseñas predeterminadas no modificadas o de las vulnerabilidades de

software en productos como los descodificadores de bajo coste para instalar código malicioso en esos dispositivos. Por desgracia, si una red de bot como Mirai o un criptominero pueden imponerse en un dispositivo, podemos verlo como un claro aviso de que algo mucho peor está por llegar.

El segundo ámbito que se considera que tiene un potencial transformador para los responsables de la defensa es el uso de redes neuronales de supererogación para resolver problemas de seguridad que actualmente se consideran intratables.

En los próximos años tendremos que volver a examinar problemas (como la identificación de vulnerabilidades y la aplicación de parches automáticos) que antes considerábamos intratables para los sistemas automatizados e intentar resolverlos mediante la aplicación inteligente del Deep Learning, a escala.

En resumen, la inteligencia artificial está cambiando a un ritmo vertiginoso. Los nuevos trucos se convierten en viejos, y los viejos trucos se refinan, se pulen y se convierten en productos de consumo generalizado para las masas de desarrolladores en plazos de meses o unos pocos años. Y aunque lo que parecía imposible a menudo se hace posible gracias al Deep Learning, algunas capacidades ensalzadas de forma exagerada, como la autonomía de los vehículos, siguen siendo obstinadamente difíciles.

- El imparable malware para móviles

  Los equipos Windows no son el único objetivo de los ciberdelincuentes. El malware también afecta a la plataforma Android y, en menor medida, a la plataforma iOS para dispositivos móviles. A medida que nuestros dispositivos informáticos portátiles han evolucionado hasta convertirse en las herramientas dominantes que utilizamos para todo, desde las compras online hasta la autenticación multifactor, pasando por los mensajes a nuestra familia y amigos, la protección de esos dispositivos frente a una amplia gama de amenazas difíciles de erradicar constituye una tarea esencial.

  Un ejemplo de ellos es el malware Joker, que adopta la forma de una gran variedad de aplicaciones, entre las que se incluyen apps utilitarias (como lectores de códigos QR), apps que pretenden instalar bonitos fondos de pantalla, apps de linterna y protectores de pantalla. Una vez instalada, la app suscribe al usuario desprevenido a servicios de SMS de tarifas especiales que pueden llegar a cobrar cuotas exorbitantes al mes y que se facturan a través del operador de telefonía móvil del abonado. Esto puede provocar retrasos en la detección de la facturación fraudulenta y hacer que las víctimas tengan que cubrir a menudo el coste de un mes o más de cargos.

  A pesar de los análisis automatizados de Google que rastrean las apps en Play Store en busca de código malicioso, Joker

evade las restricciones de Play Protect utilizando algunos trucos inteligentes para ocultar sus verdaderas intenciones a Google Play. Además de sepultar el código en lo más profundo de la app, utilizar técnicas para ocultar la información maliciosa y entorpecer a los investigadores mediante la ofuscación, Joker también ha estado moviendo el código malicioso más adelante en la cadena, después de que aparezca en Play Store. La app que aparece en Play Store es una aplicación limpia que contiene una dirección URL que descarga otro fragmento de código. Ese código tiene otra URL de descarga, que a su vez extrae un fragmento de código posterior, con otra URL oculta en su interior.

Este bucle se produce varias veces antes de que el código malicioso Joker sea descargado por un fragmento de código más adelante en la cadena. Creemos que esta larga cadena permite al malware engañar repetidamente a las defensas de Play Store. Según SophosLabs, no hay ninguna razón para pensar que esta práctica vaya a cesar y prevé que los desarrolladores de Joker continúen su juego del gato y el ratón con Google para evadir la detección de Play Protect y otros mecanismos de escaneado de código malicioso.

- La infraestructura bajo ataque

Desde el ataque a SolarWinds al ataque de ransomware que obligó a cerrar Colonial Pipeline, pasando por el ataque masivo

del ransomware REvil durante el fin de semana festivo del 4 de julio en Estados Unidos, la infraestructura que sustenta los negocios en Internet parece hallarse constantemente amenazada.

A medida que el ecosistema de la ciberdelincuencia se ha ido ampliando, los delincuentes que forman parte de él han ido limitando sus objetivos, centrándose en hacer bien un único trabajo pequeño en lugar de tratar de abarcarlo todo. La aparición de una clase de delincuentes conocidos como "brókeres de acceso inicial" (IAB) es una de las formas en que este enfoque en la especialización ha cambiado el panorama de las amenazas. Como es de esperar, el "acceso inicial" que venden estos delincuentes sirve como puerta de enlace a grandes organizaciones o redes empresariales.

Se cree que el mercado de los IAB no hará más que crecer en 2022, y que estos servicios seguirán alimentando la epidemia de ransomware que hemos estado padeciendo.

El panorama de las amenazas es un terreno en constante cambio, en que los atacantes están siempre al acecho de nuevos exploit o de oportunidades inmediatas. Aunque la mayoría de las amenazas actuales se presentan para sistemas operativos Windows, cada vez más se detecta malware que afecta a dispositivos Linux. En estos sistemas operativos los scripts de Bash desempeñan un papel similar al de los scripts

de PowerShell o los archivos por lotes en el entorno de Windows. El ransomware llamado DarkRadiation era más bien una colección de scripts de Bash que un único ejecutable convencional. Siguiendo los patrones de otros ejecutores de ransomware en redes Windows, los scripts de DarkRadiation se dirigen específicamente a las distribuciones de Debian o Red Hat (CentOS). Los scripts realizan operaciones de reconocimiento, propagación lateral y cifrado de archivos importantes.

Además de los servidores convencionales, los hipervisores representan objetivos atractivos para los ataques de ransomware, ya que un solo hipervisor podría albergar muchos equipos virtuales que actúan como servidores para una gran organización o red empresarial

Debido a la amplia disponibilidad y al escaso soporte que ofrecen algunas marcas de dispositivos de red de bajo coste a nivel del consumidor, los atacantes automatizados como Mirai no se enfrentan a ningún tipo de presión. Se espera que los ataques dirigidos tanto a los valiosos servidores de Linux como a los productos electrónicos de consumo básicos sigan avanzando sin tregua en 2022.

Conclusiones

Como el lector habrá podido comprobar, la mayoría de las empresas del sector coinciden en los siguientes puntos:

- El teletrabajo y la mezcla del ámbito del hogar con el empresarial ha tenido una impacto muy alto en la forma de actuar de los criminales, y seguirá teniéndolo.

- Los ataques de ransomware continuarán teniendo un notable peso en el total de los ataques cibernéticos, volviéndose incluso más dañinos.

- El hecho de que cada vez más dispositivos se conecten a las redes de las infraestructuras provoca la aparición de nuevos vectores de entrada.

- La aparición de nuevas formas de transacciones económicas, muchas de ellas mediante criptodivisas, hace que se convierta en un atractivo para los cibercriminales.

- La infraestructura en la nube y el despliegue de servicios en dockers abrirá nuevas puertas de entrada que deben ser correctamente securizadas.

- La fragilidad de la cadena de suministros en un mundo completamente globalizado ha puesto un nuevo objetivo en el punto de mira de los actores maliciosos.

- En los próximos años la aparición de infecciones en dispositivos móviles será cada vez mayor y se deberá tener más en cuenta por parte de los equipos de seguridad corporativa.

Glosario

API:	Siglas de la expresión inglesa *Application Programming Interface* (Interfaz de Programación de Aplicaciones). Conjunto de funciones y procedimientos que cumplen una o muchas funciones con el fin de ser utilizadas por otro software.
APT:	Siglas de la expresión inglesa *Advanced Persistent Threat* (Amenaza Persistente Avanzada). Conjunto de procesos informáticos, sigilosos y continuos, dirigidos a penetrar la seguridad de una entidad específica.
bot:	Contracción de robot. Tipo de programa informático autónomo que es capaz de llevar a

	cabo tareas concretas e imitar el comportamiento humano diseñados en cualquier lenguaje de programación.
DDoS:	Siglas de la expresión inglesa Distributed Denial of Service (Ataque de denegación de servicio distribuido). Se produce generando un gran flujo de información desde varios puntos de conexión hacia un mismo destino con la intención de alterar el correcto funcionamiento de dicho destino.
deepfake:	Aprendizaje basado en inteligencia artificial que se utiliza con la intención de crear contenido falso.
exploit:	Fragmento de software, de datos o secuencia de comandos o acciones, utilizada con el fin de aprovechar una vulnerabilidad de seguridad de un sistema de información para conseguir un comportamiento no deseado.
IA:	Siglas de la expresión inglesa *Artificial Intelligence* (Inteligencia Artificial). Concepto que se refiere a la inteligencia llevada a cabo por máquinas, basada en el análisis formal y

	estadístico del comportamiento humano ante diferentes problemas.
IoT:	Siglas de la expresión inglesa *Internet of Things* (Internet de las cosas). Concepto que se refiere a la interconexión digital de objetos cotidianos con Internet.
IT:	Siglas de la expresión inglesa *Information Technology* (Tecnologías de la Información. Agrupan los elementos y las técnicas utilizadas en el tratamiento y la transmisión de las informaciones, principalmente de informática, Internet y telecomunicaciones.
machine learning:	Disciplina científica del ámbito de la Inteligencia Artificial que crea sistemas que aprenden automáticamente, pudiendo identificar tipos de patrones complejos en millones de datos de forma más concretapor ellos mismos.
malware:	Contracción de *Malicious Software* (Software Malicioso). Tipo de programa o código informático malicioso cuya función es dañar un sistema o causar un mal funcionamiento.

phishing:	Técnica de ingeniería social utilizada por los delincuentes para obtener información confidencial como nombres de usuario, contraseñas y detalles de tarjetas de crédito haciéndose pasar por una comunicación confiable y legítima principalmente utilizada vía correo electrónico.
QR:	Siglas de la expresión inglesa *Quick Response* (Código de Respuesta Rápida). Es un módulo para almacenar información en una matriz de puntos o en un código de barras bidimensional. La matriz se lee en el dispositivo móvil por un lector específico y de forma inmediata nos lleva a una aplicación en internet y puede ser un mapa de localización, un correo electrónico, una página web o un perfil en una red social.
ransomware:	Malware que restringe el acceso a determinadas partes o archivos del sistema infectado para pedir un rescate a cambio de remover esa restricción.
router:	Dispositivo que ofrece una conexión WiFi, que normalmente está conectado a un módem y que envía información de Internet a tus

	dispositivos personales, como ordenadores, teléfonos o tablets.
software:	Sistema formal de un sistema informático, que comprende el conjunto de los componentes lógicos necesarios que hacen posible la realización de tareas específicas.
SPAM:	Correo electrónico no solicitado que se envía a un gran número de destinatarios con fines publicitarios o comerciales.
URL:	Siglas de la expresión inglesa *Uniform Resource Locators* (Localizador de Recursos Uniforme). Dirección que es dada a un recurso único en Internet.
VPN:	Siglas de la expresión inglesa *Virtual Private Network* (Red Privada Virtual). Tecnología que permite que dispositivos en la red envíe y reciba datos sobre redes compartidas o públicas como si fuera una red privada, con toda la funcionalidad, seguridad y políticas de gestión de una red privada. Esto se realiza estableciendo una conexión virtual punto a punto mediante el uso de conexiones

	dedicadas, cifrado o la combinación de ambos métodos.
Watering hole:	Un ataque ‘Watering hole’ o ataque de abrevadero consiste en infectar con malware sitios web de terceros muy utilizados por los usuarios de la organización objetivo. Cuando los usuarios de la organización accedan al sitio web comprometido quedarán infectados.
Wiper:	El malware wiper supone un riesgo a nuestra información personal, documentos y cualquier tipo de archivos que tengamos almacenados ya que tiene como objetivo el borrado del contenido que haya en una memoria o disco.

Documentación de referencia

[1] Personal de Fortinet. <<Cyber Threat Predictions for 2022: An Annual Perspective by FortiGuard Labs>>. Paper de Fortinet, noviembre de 2021. Disponible en línea. https://www.fortinet.com/content/dam/maindam/PUBLIC/02_MARKETIN

G/02_Collateral/WhitePaper/wp-threat-prediction-2022.pdf (Fecha de consulta, 24/01/2022).

[2] Personal de McAfee y FireEye. <<2022 Threat Predictions >>. Blog de McAfee, octubre de 2021. Disponible en línea. https://www.mcafee.com/blogs/enterprise/mcafee-enterprise-atr/mcafee-enterprise-fireeye-2022-threat-predictions/?eid=QKBAR7TC (Fecha de consulta, 27/01/2022).

[3] Personal de Kaspersky. <<Predicciones 2022 sobre Amenazas Persistentes Avanzadas (APT)>>. Blog de Kaspersky, diciembre de 2021. Disponible en línea. https://www.kaspersky.es/about/press-releases/2021_predicciones-2022-sobre-amenazas-persistentes-avanzadas-apt (Fecha de consulta, 31/01/2022).

[4] Personal de Kaspersky. <<Amenazas financieras en 2022: aumentan los troyanos que roban información y los ataques a criptomonedas >>. Blog de Kaspersky, enero de 2022. Disponible en línea. https://www.kaspersky.es/about/press-releases/2022_amenazas-financieras-en-2022-aumentan-los-troyanos-que-roban-informacion-y-los-ataques-a-criptomonedas (Fecha de consulta, 31/01/2022).

[6] Personal de Trend Micro Research. <<Turning the Tide: Trend Micro Security Predictions for 2022>>. Report de Trend Micro, diciembre de 2021. Disponible en línea. https://documents.trendmicro.com/assets/rpt/rpt-toward-a-new-

momentum-trend-micro-security-predictions-for-2022.pdf Fecha de consulta, 03/02/2022).

[7] Personal de Check Point. <<CCheck Point Software 2022 Cyber-security Predictions also anticipates an increase in supply chain attacks in the new year>>. Press de Check Point, diciembre de 2021. Disponible en línea. https://blog.checkpoint.com/2021/10/26/deepfakes-cryptocurrency-and-mobile-wallets-cybercriminals-find-new-opportunities-in-2022/ (Fecha de consulta, 07/02/2022).

[8] Personal de Sophos. <<Sophos 2022 Threat Report>>. Paper de Sophis, diciembre de 2021. Disponible en línea. https://www.sophos.com/en-us/medialibrary/pdfs/technical-papers/sophos-2022-threat-report.pdf Fecha de consulta, 10/02/2022).