sedian

Seguridad Digital
de Andalucía

Informe

Predicciones de amenazas para el 2021

Tipo de documento: Informe

Autor del documento: AndalucíaCERT

Código del documento: CERT-IF-122834-00

Edición: 0

Categoría: Público

Fecha de elaboración: 04/02/2021

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 2021 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 2021 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

Cada vez existen más dispositivos conectados y se diversifican más las tecnologías en uso, por lo que mantener la seguridad de la información constituye un desafío cada vez mayor.

En el ecosistema actual coexisten tanto las amenazas más tradicionales (SPAM / phishing, fugas de información, infecciones por malware, hacktivismo, etcétera) como los nuevos modelos de cibercrimen (ransomware, APTs, ataques contra infraestructuras críticas, ciberespionaje o similares).

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 2021 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

- Los troyanos evolucionan para apuntar hacia el perímetro de la red

  Si bien los usuarios finales y sus recursos domésticos ya son objetivo de los ciberdelincuentes, los atacantes más sofisticados los utilizarán como un trampolín hacia otros objetivos gracias al auge del teletrabajo. Los ataques a la red corporativa lanzados desde la red doméstica de un trabajador remoto, especialmente cuando se comprendan los patrones de uso del usuario, se podrán simular cuidadosamente para que no levanten sospechas.

  Con el tiempo, las familias de malware más avanzadas también podrían descubrir datos y patrones aún más valiosos utilizando nuevos troyanos y así poder realizar actividades invasivas como interceptar solicitudes fuera de la red local, comprometer sistemas adicionales o inyectar comandos de ataque añadidos.

- La tecnología 5G podrá habilitar ataques avanzados de enjambre

  Comprometer los nuevos dispositivos con tecnología 5G abrirá oportunidades para amenazas más avanzadas. Los ciberdelincuentes están progresando en el desarrollo y despliegue de ataques basados en enjambres. Estos ataques aprovechan los dispositivos secuestrados y los dividen en subgrupos, cada uno con habilidades especializadas. Las tecnologías de enjambre requieren una gran cantidad de potencia de procesamiento para permitir que enjambres de bots individuales compartan información de manera eficiente entre ellos. Esto les permitirá descubrir, compartir y correlacionar vulnerabilidades rápidamente, para luego perfeccionar sus métodos de ataque.

- Avances en los ataques de ingeniería social

  Los dispositivos inteligentes y otros sistemas domésticos que interactúan con los usuarios ya no serán simplemente el objetivo final de los ataques, sino que también servirán como propósito para ataques más profundos y elaborados. Aprovechar la información contextual sobre los usuarios, incluidas rutinas diarias, hábitos o información financiera, podría hacer que los ataques basados en ingeniería social sean más exitosos. Los ataques más inteligentes podrían llevar a mucho más que apagar los sistemas de seguridad, deshabilitar cámaras o secuestrar dispositivos inteligentes, podrían permitir el secuestro y la extorsión de datos de carácter personal o sensible.

- Nuevas formas de aprovechar el ransomware en infraestructuras críticas

  El ransomware continúa evolucionando y a medida que los sistemas IT convergen cada vez más con los sistemas OT en las infraestructuras críticas, aumentará el riesgo de acceso a los datos y de compromiso de los dispositivos. En el futuro, es posible que la población se pueda encontrar en riesgo cuando los dispositivos de campo y los sensores situados en el borde de los sistemas OT, que incluyen infraestructuras críticas, se conviertan cada vez más en objetivos de los ciberdelincuentes.

- Avances en el criptominado a través del compromiso de dispositivos secundarios

  El poder de procesamiento es importante, sobre todo si los ciberdelincuentes quieren escalar ataques futuros a través de técnicas de machine learning o IA . Eventualmente, al comprometer los dispositivos periféricos por su capacidad de procesamiento, los ciberdelincuentes podrían procesar cantidades masivas de datos y aprender más sobre cómo y cuándo se utilizan ciertos dispositivos periféricos, así como aprovechar sus capacidades técnicas orientadas a la criptominería. Los equipos infectados, que son secuestrados para el aprovechamiento de sus recursos, a menudo se identifican porque el uso de la CPU afecta directamente la experiencia de trabajo del usuario final, pero poner en peligro los dispositivos secundarios podría ser mucho menos perceptible.

- La amenaza de la computación cuántica

  El enorme poder de la computación cuántica podría hacer trivial la resolución de algunos algortimos de cifrado asimétrico. Como resultado, las organizaciones deberán prepararse para cambiar a algoritmos criptográficos resistentes a los cuánticos, utilizando el principio de agilidad criptográfica para garantizar la protección de la información actual y futura. Aunque no se considera que el ciberdelincuente promedio pudiera tener acceso a computadoras cuánticas, algunos estados/naciones sí que lo tendrán, por lo que la amenaza eventual se hará realidad si no se realizan preparativos de cara a prevenir y contrarrestar, adoptando una posición ágil en este punto.

McAfee

- Las técnicas de puerta trasera en la cadena de suministro aumentarán

  El mundo de la ciberseguridad ha sido sacudido en los últimos meses, tal y como ocurrió con hechos ya históricos dentro de este sector como fueron WannaCry o Emotet, a través del compromiso del software de gestión y monitorización de la plataforma SolarWinds Orion. Este ataque habría servido para distribuir puertas traseras, a través del malware denominado Sunburst, a docenas de clientes de dicha misma compañía, incluidas varias agencias gubernamentales estadounidenses de alto perfil.

Lo que hace que este tipo de ataque sea tan peligroso es que utiliza software confiable para eludir las medidas de detección, infiltrarse en las organizaciones de sus víctimas a través de una puerta trasera y permitir que el atacante realice acciones sin llamar la atención. Esto podría conllevar al robo o la destrucción de datos, al secuestro de sistemas críticos para solicitar un rescate, a la orquestación de fallas del sistema o simplemente a la descarga de contenido malicioso adicional en toda la organización para mantener el control incluso después de que la amenaza inicial pareciese haber sido erradicada. Cada organismo o empresa violada podría tener diferentes puertas traseras secundarias, lo que significa que no existe una receta única para desalojar la intrusión. Es difícil, por tanto, determinar exactamente qué propiedad intelectual o qué datos privados de los empleados han podido ser afectados y, de igual forma, es posible que nunca se llegue a saber el alcance total del compromiso.

El descubrimiento del ataque a la cadena de suministro de la empresa SolarWinds expondrá técnicas de ataque que otros ciberdelincuentes de todo el mundo intentarán imitar en el futuro.

- Atacar la casa para atacar la oficina

La pandemia mundial hizo trasladar a los empleados de la oficina al hogar, convirtiendo el entorno doméstico en un entorno laboral. Los cibercriminales han aumentado así sus objetivos, añadiendo a su lista la superficie de ataque doméstica, la cual ha sido ampliamente atacada en los últimos meses a través de campañas de phishing con

enlaces maliciosos introducidos a través de dispositivos con medidas más débiles de seguridad.

Muchos de estos dispositivos domésticos se encuentran “huérfanos” debido a que sus fabricantes no ofrecen soporte ni actualizaciones de seguridad para parchear nuevas amenazas y vulnerabilidades. Actualmente la situación en numerosas empresas viene dada por el teletrabajo con equipos configurados por el propio usuario y que, por lo tanto, carecen de una administración centralizada. Los cibercriminales intentarán aprovechar la falta de actualizaciones periódicas de software y firmware, la falta de funciones de mitigación de seguridad, las políticas de privacidad débiles, las vulnerabilidades y la propensión del usuario a ser víctima de ataques de ingeniería social. Una vez lleguen a comprometer el entorno doméstico, se lanzarán una variedad de ataques al resto de dispositivos corporativos y de consumo.

- Los ataques a plataformas en la nube se volverán altamente personalizados

  La pandemia también ha acelerado el ritmo de la transición de la IT corporativa a la nube, aumentando el potencial de nuevos tipos de ataques corporativos relacionados con el entorno cloud. Gracias a la adaptación de los entornos remotos y con la gran cantidad de empresas que han implementado el teletrabajo, no solo hay un número creciente de usuarios de la nube, sino también muchas más transacciones y datos en movimiento.

Los ciberdelincuentes desarrollarán nuevos ataques altamente mecanizados contra miles de redes domésticas heterogéneas. Además, también podrían usar IA y machine learning para eludir las tecnologías de filtrado de red tradicionales implementadas para proteger las instancias en la nube. Se aprovecharán algoritmos distribuidos y de aprendizaje por refuerzo para identificar planes de ataque enfocados principalmente en evitar bloqueos de cuentas. Al mismo ritmo que maduran las posturas de seguridad empresarial en la nube, los atacantes se verán obligados a crear exploits altamente específicos para empresas, usuarios y aplicaciones concretas.

- Nuevas estafas de pago móvil

  A medida que los usuarios se vuelven cada vez más dependientes de los pagos móviles, los cibercriminales buscarán cada vez más explotar y engañar a los usuarios con mensajes fraudulentos de phishing o smishing que contendrán URLs de pago maliciosas. Se espera un aumento en esta tendencia, en las que un usuario podría recibir un correo electrónico de phishing, un mensaje directo a través de alguna red social o un mensaje de smishing que le indicase que podría recibir un pago, un reembolso o un premio en efectivo haciendo clic en un enlace malicioso.

- Qshing: abuso de códigos QR en la era COVID

  La pandemia ha creado la necesidad de que se opere y se realicen transacciones en todas las áreas de una manera "sin contacto". El

uso de códigos QR ha proliferado en muchas áreas, incluidos pagos, paquetería, restaurantes, comercio minorista u ocio. Los códigos QR ayudan a limitar el contacto directo entre empresas y consumidores en todos los entornos y permite a los usuarios escanearlos fácilmente e interactuar con el resultado de los mismos.

Sin embargo, los tecnicismos de los códigos QR son un misterio para la mayoría de los usuarios y eso los hace potencialmente peligrosos, especialmente si los ciberdelincuentes buscan explotarlos para atacar a sus víctimas. Dado que los códigos QR están diseñados precisamente para ocultar el texto de la URL, los usuarios tienen dificultades para identificar códigos QR maliciosos. Por lo tanto, no sorprende que se hayan utilizado códigos QR en esquemas de phishing para evitar los intentos de las soluciones anti-phishing de identificar las URLs maliciosas en los mensajes de correo electrónico. En tales esquemas, las víctimas escanearían códigos QR fraudulentos y serían redirigidas a sitios web maliciosos donde se les pedirían credenciales de inicio de sesión, información personal o información de pago. De igual forma, también podrían usarse para descargar programas maliciosos en el dispositivo de un usuario. Los piratas informáticos utilizarán cada vez más estos esquemas de códigos QR y los ampliarán mediante técnicas de ingeniería social.

- Redes sociales como vectores de ataque en el lugar de trabajo

  Tradicionalmente, los ciberdelincuentes han dependido en gran medida de los correos electrónicos como vector de ataque para

comprometer a las organizaciones a través de empleados individuales. Sin embargo, como las organizaciones tienden a implementar medidas para la detección de SPAM, prevención de pérdida de datos y otras soluciones para evitar los intentos de phishing en cuentas de correo electrónico corporativo, se prevé que surjan ataques más sofisticados contra los empleados objetivo a través de las plataformas de redes sociales a las que estas defensas no pueden aplicarse.

De esta forma, los ciberdelincuentes utilizarán cada vez más las funciones de mensajería de plataformas como LinkedIn, WhatsApp, Facebook o Twitter para hacer partícipes, desarrollar relaciones y posteriormente comprometer a los empleados corporativos, especialmente ahora que las organizaciones están tendiendo a involucrar a los consumidores potenciales en las plataformas sociales mediante la recopilación de información, el desarrollo de contenido especializado y las interacciones específicas con los clientes. Si bien es poco probable que el correo electrónico sea reemplazado alguna vez como vector de ataque, se estima que este nuevo vector de plataforma de redes sociales se volverá más común.

Kaspersky

- Los actores de amenazas APT comprarán a los cibercriminales el acceso inicial a las redes

A lo largo de los últimos meses se ha observado un aumento de ataques selectivos de ransomware que usaban malware genérico para penetrar en las redes atacadas. También se han observado conexiones entre los ataques selectivos de ransomware y redes clandestinas que se dedican a comercializar con credenciales robadas. Se cree que los actores de APT comenzarán a usar el mismo método para infectar a sus víctimas. Las organizaciones deberían prestar mayor atención a este tipo de malware y llevar a cabo actividades básicas de respuesta a incidentes en cada equipo infectado a fin de asegurarse de que no se haya usado malware genérico para lanzar amenazas más sofisticadas.

- Más países se sumarán a las acusaciones de ciberespionaje como parte de sus ciberestrategias

  Hace unos años se predijo que los gobiernos recurrirían a acusar de acciones de ciberespionaje a otros países, para hacer llamar la atención sobre las actividades de grupos de APTs. Se cree que esta tendencia se verá en estados/naciones que la replicarán, sobre todo como represalia a acusaciones previas realizadas por países como Estados Unidos. Esta estrategia implicará la publicación de informes sobre las herramientas y actividades de países adversarios.

  Exponer las herramientas de los grupos de APT no es algo nuevo, sin embargo, es la primera vez que se hará de manera oficial a través de agencias gubernamentales. Se cree que en el futuro más países se sumarán a esta estrategia. En primer lugar, se prevé que sean los

países aliados tradicionales de EE.UU quienes puedan empezar a replicar este proceso y, posteriormente, los blancos de tales descubrimientos podrían seguir el ejemplo como una forma de represalia.

- Más empresas de Silicon Valley tomarán medidas contra los intermediarios de día cero

  Hasta hace poco los intermediarios en la venta de zero days comercializaban sus exploits sin que las grandes compañías como Microsoft, Google o Facebook les prestasen atención. Sin embargo, esto habría cambiado después de que en los últimos meses se hayan atacado cuentas mediante vulnerabilidades en WhatsApp, entre las que estarían perfiles de alto nivel como el de Jeff Bezos. Tras estos incidentes WhatsApp inició acciones legales contra los grupos que se encontraban detrás de los ataques por haber explotado una vulnerabilidad en su software y porque la tecnología que este grupo vendió, fue utilizada para atacar a más de 1400 de sus clientes en 20 países distintos entre ellos activistas de derechos humanos, periodistas y otros perfiles con gran repercusión. Posteriormente, un juez estadounidense falló en favor de cursar el juicio. El resultado del caso podría tener amplias consecuencias, una de las cuales podría ser que otras empresas también inicien acciones legales contra los modelos de negocio que venden exploits de día cero.

  Se prevé que debido a la creciente presión de la opinión pública y los riesgos de daños a la reputación, otras empresas podrían seguir los

pasos de WhatsApp e iniciar acciones legales contra los intermediarios de día cero, demostrando así a sus clientes que se preocupan por la protección de su datos e información.

- Más ataques contra dispositivos de red

  Dada la tendencia hacia la mejora general de la seguridad corporativa, se cree que los ciberdelincuentes desviarán sus esfuerzos a explotar vulnerabilidades en los dispositivos puente de red, como las pasarelas VPN. Esta idea irá a la par con el giro hacia el teletrabajo, que requiere que más empresas usen e implementen configuraciones VPN para sus operaciones.

  La atención cada vez mayor en el trabajo a distancia y la dependencia de las VPNs abre otro potencial vector de ataques: la recopilación de las credenciales de los usuarios a través de estrategias de ingeniería social con el objetivo de comprometer las VPNs corporativas. En algunos casos, esto permitiría al atacante cumplir con sus objetivos de espionaje sin instalar malware en el equipo de la víctima.

- La aparición de vulnerabilidades 5G

  El 5G ha concentrado la atención este año, en parte suscitada por EE.UU, que habría presionado en cierta forma a países “amigos” para desalentarlos a adquirir los productos de la marca Huawei, una de las empresas líderes en el despliegue de esta tecnología. Como resultado de estas acciones, se han viralizado numerosos rumores e

historias sobre posibles riesgos asociados a esta tecnología. Esta atención dirigida a la seguridad del 5G significaría que tanto investigadores públicos como privados estarían analizando productos Huawei y de otras empresas del sector en busca de problemas de implementación, fallas en el cifrado e incluso puertas traseras. Tales fallas, sin duda, captarán el interés masivo de los cibercriminales, ya que a medida que aumente el uso del 5G y que más dispositivos dependan cada vez más de la conectividad que ofrece, los atacantes tendrán un gran incentivo para buscar vulnerabilidades que puedan explotar.

- Se “amenazará” para obtener dinero

  Se han visto varios cambios y refinamientos en las tácticas que han usado los cibercriminales en torno al ransomware en los últimos años. El más notable es que los ataques han evolucionado de ser especulativos, aleatorios y distribuidos a grandes cantidades de víctimas potenciales, a ser altamente selectivos y exigir considerables rescates a una sola víctima. Estas víctimas se seleccionan con mucho cuidado, en base a su capacidad de pago, dependencia de los datos cifrados y amplitud del impacto que el ataque pueda tener. Ningún sector se libra de ellos a pesar de las promesas de los cibercriminales de no atacar hospitales. También se ha visto que buscan sacar ventaja amenazando con publicar los datos robados si la empresa rehusa pagar el rescate exigido.

Es posible que esta tendencia siga evolucionando a medida que los ciberdelincuentes que usan ransomware busquen maximizar sus ganancias. Es probable que en el futuro se vea una concentración de los principales grupos de ransomware, que comiencen a focalizar sus actividades y obtengan capacidades similares a las de los grupos de APTs. Mientras tanto, grupos más pequeños seguirán con el modelo establecido que depende de mantener redes de bots y de subcontratar el ransomware.

- Ataques más perjudiciales

  Cada vez más aspectos de la vida dependen de la tecnología y la conectividad a Internet. Como resultado de esto, se tiene una superficie de exposición mucho mayor que antes. Por lo tanto, es probable que en el futuro los ataques perjudiciales sean más frecuentes. Por una parte, los daños podrían resultar de ataques selectivos, orquestados y diseñados para afectar infraestructuras críticas y, por otra, podría tratarse de daños colaterales como consecuencia de ataques masivos contra organizaciones con las que es fácil relacionarse en el día a día, como escuelas, bancos, comercios, servicios de correo o transporte.

- Los atacantes seguirán explotando la pandemia del COVID-19

  La pandemia del COVID-19 ha puesto al mundo del revés, afectando a casi todos los aspectos de nuestras vidas. Atacantes de toda laya, incluyendo actores de amenazas APT, reaccionaron rápidamente

ante la oportunidad de explotar el interés en este tema. Esto no cambió las tácticas, técnicas y procedimientos que ya se seguían, sino que ha sido aprovechado y es un tema persistente de interés que pueden explotar con técnicas de ingeniería social.

La pandemia seguirá afectando nuestras vidas por un tiempo indeterminado y los actores de amenazas también seguirán explotándola para penetrar los sistemas que tienen como objetivo. Existen reportes en los últimos meses sobre grupos APT que habrían atacado centros de investigación de COVID-19 y del desarrollo de vacunas. Mientras dure, todos los aspectos relacionados con el COVID-19 que puedan ser explotados, seguirán siendo de interés estratégico para los ciberdelincuentes.

Trend Micro

- Los agentes de amenazas convertirán las oficinas domésticas en sus nuevos centros criminales

  La pandemia en curso y los confinamientos resultantes en muchas partes del mundo han obligado a una cantidad ingente de empleados al trabajo remoto. Como resultado, muchos empleados y empresas están empezando a darse cuenta de la viabilidad de trabajar desde casa tanto en el presente como en el futuro. En estas circunstancias, los usuarios y las empresas tendrán que protegerse de las amenazas, las instalaciones y configuraciones de los equipos de trabajo.Esto no solo será de aplicación para los equipos de IT, que de repente

necesitan desplegar mecanismos para asegurar a toda la fuerza laboral remota de la organización, sino también para usuarios individuales, que necesitan tomar más precauciones.

Los límites entre el trabajo y la vida privada se han roto a medida que se trabaja con proveedores de servicios de Internet en el hogar, con routers y máquinas que posiblemente no tengan parches, con otros dispositivos conectados en segundo plano y con miembros de la familia que comparten ordenadores mientras trabajan para diferentes organizaciones. Las redes domésticas se convertirán en puntos de lanzamiento de ataques para los agentes de amenazas que buscan secuestrar máquinas y saltar a otros dispositivos en la misma red, con el objetivo de ganar un punto de apoyo corporativo. Los actores maliciosos aprovecharán el software instalado o las vulnerabilidades troyanizadas no parcheadas, saltando de una máquina de un trabajador remoto a otra hasta encontrar un objetivo adecuado.

- La pandemia del COVID-19 dará un vuelco a las prioridades en ciberseguridad, ya que resulta ser un terreno fértil para las campañas maliciosas

  Los agentes de amenaza ven cualquier evento importante como una oportunidad para la manipulación o el sabotaje y no es diferente con la pandemia actual del coronavirus; ya que actualmente se encuentran explotando los temores colectivos relacionados con el COVID-19. Los ciberdelincuentes seguirán apostando por las

oportunidades que ofrece la ingeniería social y permanecerán activos con campañas que utilicen señuelos temáticos del coronavirus. El sector de la salud, en particular, será el centro de atención. Como muchos médicos se han pasado a la telemedicina y la prestación de servicios médicos se ha vuelto aún más crítica, la seguridad informática de los sistemas sanitarios será puesta a prueba. Los equipos de seguridad no solo tendrán que hacer frente a los riesgos de seguridad asociados a los datos de los pacientes y a los ataques de malware sino también a la posibilidad del espionaje médico.

Las campañas de desinformación también dificultarán a los usuarios la tarea de desentrañar muchas incertidumbres de la pandemia. Los ciberdelincuentes se inclinarán por utilizar la información errónea para atraer a los usuarios a hacer clic en archivos adjuntos y enlaces maliciosos. Estas estafas se enviarán a través de correos electrónicos, aplicaciones falsas, dominios maliciosos y redes sociales, con el fin de proporcionar información sobre la salud, supuestas vacunas y las correspondientes listas de espera.

- Las configuraciones de teletrabajo obligarán a las organizaciones a enfrentarse a entornos híbridos y arquitecturas de seguridad insostenibles

  A medida que el teletrabajo se afiance todavía más en el futuro, los entornos híbridos, en los que el trabajo y los datos personales se mezclan en una sola máquina, supondrán un importante reto para las organizaciones que tengan menos control sobre el uso de los

datos por parte de los empleados. La mezcla de tareas personales y laborales difumina las líneas relativas al lugar donde se almacenan y procesan los datos.

A medida que las diversas tecnologías utilizadas en el trabajo remoto ocupen los titulares de las noticias sobre cuestiones de seguridad, los modelos zero trust cobrarán impulso como un enfoque eficaz para potenciar las fuerzas de trabajo distribuidas. Al eliminar la confianza implícita en cualquier equipo dentro o fuera de la red, todo se deberá verificar antes. Los equipos IT tendrán que revisar los enfoques de seguridad para acomodar las configuraciones de trabajo remoto a largo plazo. Las organizaciones harían bien en esbozar políticas de trabajo desde el hogar (incluida la coordinación con los proveedores de servicios gestionados), manejo de datos y, en la medida de lo posible, hacer cumplir la línea que separa el uso personal y empresarial de los dispositivos.

- La necesidad sin precedentes de rastrear contactos hará que los agentes maliciosos dirijan su atención a los datos recopilados por los usuarios

  Los niveles sin precedentes de recopilación de datos en los esfuerzos por monitorizar y vigilar el estado de salud de las personas atraerán a los delincuentes y activistas políticos a intentar obtener estos datos. La prisa por aplicar estas medidas aumentará el riesgo de exponer o filtrar los datos de los usuarios. El acceso rápido a los datos podría ser crucial para luchar contra la pandemia, pero la flexibilización de

las medidas de privacidad de los datos también conlleva sus propios problemas. Las grandes bases de datos, junto con las implementaciones apresuradas, son y serán objetivos de gran valor para los agentes maliciosos que buscan comprometer los datos recopilados. Los grupos de ciberdelincuentes pueden abusar de ello de diferentes maneras, incluida la extracción de información de identidad y su venta en el mercado negro. La falta de protocolos y protecciones estrictas deja a los servidores o bases de datos vulnerables a la explotación. Los gobiernos tendrán que prepararse y tomar las medidas adecuadas para proteger los datos del acecho de los ciberdelincuentes.

- Los atacantes rápidamente convertirán en armas las vulnerabilidades recién desveladas, dejando a los usuarios un estrecho margen para parchear

  Mientras que las vulnerabilidades de día cero se refieren a fallos o errores que acaban de ser revelados pero que permanecen sin parchear, las vulnerabilidades de día N son las que han sido conocidas públicamente y que pueden tener parches desplegados. Hay innumerables vulnerabilidades conocidas hoy en día y muchas organizaciones descubrirán que tienen una exposición considerable en sus respectivas huellas digitales. Se prevé una rápida adopción de vulnerabilidades y exploits del tipo día N liberadas por la comunidad de investigación que los atacantes utilizarán activamente. También surgirán mercados de vulnerabilidades día N para comerciar o vender errores conocidos explotables, en los que no es descabellado

especular que los vendedores también ofrecerán personalización de exploits en función del tipo de ataque, permitiendo a los agentes relativamente inexpertos elaborar ataques altamente personalizados.

- Las APIs expuestas serán el próximo vector de ataque favorito para las brechas empresariales

  Muchos negocios dependen de APIs para proporcionar acceso a los sistemas internos e interactuar con los clientes. A medida que las APIs se hagan más prominentes en el espacio empresarial, también lo será su superficie de ataque. Estas se convertirán en un objetivo, ya que también actúan como conductos para la integración de terceros y se prevé que la seguridad de estas será una nueva área de interés para los cibercriminales. Las APIs, aunque ya son comunes, tienen una seguridad aún incipiente ya que introducen varios puntos débiles que podrían ser vectores de ataque en brechas de datos de aplicaciones empresariales, tal y como ya ha ocurrido en numerosas ocasiones en la que se ha obtenido acceso a la información personal de usuarios y se ha encontrado código fuente expuesto. Los mecanismos de defensa tradicionales que implican resolución de problemas a través de imágenes, código ejecutado en el navegador o instrumentación móvil no pueden ser utilizados eficazmente para prevenir un ataque automatizado, lo que significa que las APIs están solo parcialmente protegidas, si es que lo están.

- El software empresarial y las aplicaciones cloud utilizadas para el trabajo remoto serán acosados por errores críticos

  Se espera que se encuentren y se divulguen públicamente cada vez más vulnerabilidades en el software y los servicios más importantes utilizados en entornos de trabajo distribuidos. Tanto los ciberdelincuentes como los grupos de agentes de amenazas aprovecharán las debilidades en el software más popular como parte de sus campañas. El procesamiento de información potencialmente sensible en estas plataformas de software de colaboración será una preocupación importante para las organizaciones con una fuerza laboral remota cada vez mayor y en particular en las industrias reguladas, como pueden ser los servicios financieros o la asistencia sanitaria. La adopción del uso de la tecnología cloud continuará para hacer frente al efecto de la pandemia en las operaciones y se espera que esta tendencia continúe creciendo incluso cuando la pandemia retroceda. Las organizaciones que migraron de forma rápida y al azar se enfrentarán a las implicaciones de seguridad. Se prevé que las brechas de datos y el compromiso exponencial en las infraestructuras cloud sean causados no por los proveedores de la nube, sino por las configuraciones incorrectas y los errores involuntarios de los usuarios o del despliegue precipitado tanto de aplicaciones como de contenedores de aplicaciones.

Check Point

- Asegurar la 'nueva normalidad'

  La pandemia del COVID-19, aún sin una fecha de fin determinada, afianzará cada vez más la “nueva normalidad”. Tras las prisas por implantar el trabajo remoto y flexible, las organizaciones necesitarán proteger mejor sus nuevas redes distribuidas y las implementaciones en la nube para mantener sus aplicaciones y datos protegidos. Esto implicará automatizar la prevención de amenazas en todos los puntos de la red, desde los dispositivos móviles y terminales de los empleados hasta los dispositivos IoT y el entorno cloud, para detener la propagación rápida de ataques avanzados que ya han sido vistos en todo tipo de organizaciones y evitar el aprovechamiento de las debilidades para violar datos confidenciales.

- No hay cura para las vulnerabilidades relacionadas con el COVID-19

  La pandemia continuará dominando los titulares en los medios de comunicación a corto y medio plazo: las noticias sobre desarrollos de vacunas o nuevas restricciones nacionales continuarán utilizándose en campañas de phishing, tal y como viene siendo habitual hasta ahora. Las compañías farmacéuticas y entidades sanitarias relacionadas también continuarán siendo blanco de ataques maliciosos de criminales o estados/naciones que buscan explotar esta situación.

- La doble extorsión aumenta la apuesta por el ransomware

Se ha observado un cambio de tendencia en lo que a ataques de ransomware se refiere, produciéndose un incremento en la denominada doble extorsión: los piratas informáticos primero extraen grandes cantidades de datos confidenciales antes de cifrar las bases de datos de una víctima y, posteriormente, amenazan con publicar esos datos a menos que se paguen las demandas de rescate. Esta tipología de ataque se ha vuelto tan perturbadora que se han establecido normas y procedimientos que han suavizado la postura acerca de los rescates: si antes no se recomendaba realizar el pago, ya que esto incentivaba este tipo de prácticas y, al fin y al cabo, se pretendía recuperar los datos a partir de las copias de seguridad almacenadas, ahora las empresas pueden valorar estos pagos para proteger a sus accionistas, empleados y clientes.

- Armando deepfakes

  Las técnicas para alterar videos o audios falsos ahora son lo suficientemente avanzadas como para ser desarrolladas y utilizadas para crear contenido específico con el objetivo de manipular opiniones. A un nivel más simple, un video o un audio podrían falsificarse para suplantación de identidad , de modo que los perfiles de alto nivel podrían suplantarse dando instrucciones al resto de personal cercano para realizar acciones fraudulentas.

- ¿Intimidad? ¿Privacidad ?

Para muchas personas, sus dispositivos móviles ya están dando mucha más información personal de la que creen gracias a las aplicaciones que exigen un acceso amplio a contactos, mensajes y demás información personal. Este problema se habría magnificado con las aplicaciones de rastreo de contactos del COVID-19, que con errores, se lanzaron sobre la marcha, rápidamente y con problemas de privacidad, poniendo en riesgo de esta forma, datos estrictamente personales.

- Beneficios y desafíos de 5G

  El mundo de alta velocidad totalmente conectado prometido por la tecnología 5G también brindará a los delincuentes y piratas informáticos oportunidades para lanzar ataques aprovechando esta conectividad. Los dispositivos de salud digitales, los servicios de automóviles, las aplicaciones de ciudades inteligentes y el resto de la nueva tecnología implementada recopilarán enormes cantidades de datos e información sobre los usuarios. Este enorme volumen de datos a través de dispositivos 5G siempre interconectados deberá protegerse contra infracciones, robos y alteraciones para garantizar la privacidad y la seguridad contra ataques por parte de los ciberdelincuentes.

- Internet de las amenazas

  A medida que termine la implementación y se comience con la utilización masiva de las redes 5G la cantidad de dispositivos IoT

conectados se expandirá enormemente, lo que aumentará drásticamente la vulnerabilidad de las redes a los ataques por parte de los ciberdelincuentes. Los dispositivos IoT y sus conexiones a redes y hacia la nube seguirán siendo un eslabón débil de la seguridad, ya que es difícil obtener una visibilidad completa de los dispositivos, que a su vez tendrán requisitos de seguridad complejos. Será necesario un enfoque más holístico en lo que a la seguridad IoT se refiere, con una combinación de controles nuevos y tradicionales para proteger estas redes de dispositivos en constante crecimiento para todos los sectores, tanto industriales como comerciales.

ESET

- El futuro del trabajo: adoptar una nueva realidad

  El advenimiento de la pandemia de COVID-19 ha marcado el comienzo de la implementación masiva del trabajo remoto, que ha visto una mayor dependencia de la tecnología que nunca. Este alejamiento de la oficina ha traído beneficios para los empleados, pero también ha dejado las redes de las empresas vulnerables a los ataques.

  A medida que se digitalice cada vez más la vida laboral y familiar, la ciberseguridad tomará más importancia y se convertirá, si no lo es ya, en el eje empresarial. Los ciberataques son una amenaza persistente para las organizaciones y las empresas deben crear

equipos y sistemas IT resistentes para evitar las consecuencias financieras y de reputación de dicho ataque.

- Ransomware con doble extorsión: paga o se filtran tus datos

  Es posible que los ataques frustrados o los procesos de copia de seguridad y restauración diligentes ya no sean suficientes para defenderse de un ciberdelincuente que ha logrado comprometer exitosamente un entorno y que exige el pago de un rescate por el mismo. El éxito en la monetización dependerá de la afectación tras el chantaje de la divulgación pública de los datos comprometidos, que ofrecerá a los ciberdelincuentes una mayor posibilidad de obtener un retorno de la inversión y que se verá cada vez más llevada a cabo.

- Más allá de la prevención: mantenerse al día con las arenas movedizas de las ciberamenazas

  En los últimos años los grupos de ciberdelincuentes han recurrido al uso de técnicas cada vez más complejas para implementar ataques altamente dirigidos. Hace tiempo que se comenzó a hablar de ataques de “malware sin archivos” que se aprovechan de las propias herramientas y procesos del sistema operativo con fines maliciosos. Estas técnicas han ganado más peso recientemente, habiendo sido empleadas en varias campañas de ciberespionaje y por varios actores maliciosos, principalmente para atacar objetivos de alto perfil, como entidades gubernamentales.

Las amenazas sin archivos han evolucionado rápidamente y se espera que en el futuro, estos métodos se utilicen en ataques cada vez más complejos y de mayor escala. Esta situación destaca la necesidad de que los equipos de seguridad desarrollen procesos que aprovechen herramientas y tecnologías que no solo eviten que el código malicioso comprometa los sistemas informáticos, sino que también tengan capacidades de detección y respuesta, incluso antes de que estos ataques cumplan su misión.

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 tendrá una importancia muy alta, tanto en el presente como en el futuro.

- La pandemia estará presente durante todavía un tiempo indeterminado, con lo que ello conlleva; seguirán potenciándose ataques basados en ingeniería social, phishing o deepfakes.

- Aumentarán cada vez más los ataques dirigidos y cambiará la forma en la que se llevan a cabo, aprovechándose en todo momento del impacto o posible repercusión para extorsionar a sus objetivos.

- El despliegue y utilización de la tecnología 5G de forma masiva creará posiblemente un nuevo ámbito y vectores de ataques orientados a esta nueva superficie de exposición.

- Como viene siendo habitual, la tendencia de crecimiento del malware dedicado y con objetivos específicos seguirá desarrollándose y creciendo, viendo cómo año tras año siguen siendo cada vez más efectivos y cómo tienen cada vez más repercusión.

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.
cloud:	Computación en la nube. Consiste en la posibilidad de ofrecer servicios a través de Internet. es una tecnología nueva que busca tener todos nuestros archivos e información en Internet, sin preocuparse por poseer la capacidad

	suficiente para almacenar información en equipos locales.
CPU:	Siglas de la expresión inglesa *Central Processing Unit* (Unidad Central de Procesamiento). Placa o chip que se encuentra integrada a la tarjeta madre, y contiene todos los circuitos esenciales para el funcionamiento del aparato electrónico que lo contenga.
deepfake:	Aprendizaje basado en inteligencia artificial que se utiliza con la intención de crear contenido falso.
Emotet:	Malware troyano de tipo polimórfico que cambia automáticamente su código cada cierto tiempo o con acciones determinadas del dispositivo, haciendo que sea más difícil para los antivirus detectar su firma.
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.
firmware:	Programa informático que establece la lógica de más bajo nivel que controla los circuitos

	electrónicos de un dispositivo de cualquier tipo. Está fuertemente integrado con la electrónica del dispositivo, siendo el encargado de controlar y ejecutar correctamente las instrucciones externas.
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.
OT:	Siglas de la expresión inglesa *Operation Technology* (Tecnología de la Operación). Se encuentra dedicada a detectar o cambiar los procesos físicos a través de la monitorización y el control de dispositivos también físicos, como tuberías o válvulas, principalmente en el ámbito industrial.
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.
Qshing:	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 códigos QR.
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.
smishing:	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 SMS.
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.
Sunburst:	Malware troyano de tipo ransomware que una vez accede a las redes de las organizaciones permanece latente acumulando datos y registros de las mismas. Transcurridos entre 10 y 14 días, envía datos a un servidor de control y comando remoto; en este punto, los ciberatacantes analizan dicha información y escalan el ataque únicamente sobre los objetivos que consideren.
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.
WannaCry:	Malware troyano de tipo ransomware que cifra los archivos e información almacenada en los equipos afectados y que posteriormente, exige un pago o rescate) para poder descifrarlos.
zero trust:	Es un concepto de modelo de seguridad que se apoya en la idea de que las organizaciones no deberían confiar de manera predeterminada en nada que esté dentro o fuera de su red o perímetro.

Documentación de referencia

[1] Personal de Fortinet. <<New Cybersecurity Threat Predictions for 2021>>. Blog de Fortinet, noviembre de 2020. Disponible en línea. https://www.fortinet.com/blog/threat-research/new-cybersecurity-threat-predictions-for-2021 (Fecha de consulta, 04/02/2021).

[2] Personal de Fortinet. <<Cyber Threat Predictions for 2021: An Annual Perspective by FortiGuard Labs>>. Paper de Fortinet, noviembre de 2020. Disponible en línea. https://www.fortinet.com/content/dam/fortinet/assets/white-papers/wp-cyber-threat-predictions-for-2021.pdf (Fecha de consulta, 05/02/2021).

[3] Personal de McAfee. <<2021 Threat Predictions Report>>. Blog de McAfee, enero de 2021. Disponible en línea. https://www.mcafee.com/blogs/other-blogs/mcafee-labs/2021-threat-predictions-report/ (Fecha de consulta, 05/02/2021).

[4] Personal de Kaspersky. <<What does 2021 have in store for cybersecurity?>>. Blog de Kaspersky, enero de 2021. Disponible en línea. https://www.kaspersky.com/blog/secure-futures-magazine/cybersecurity-predictions-2021/38136/ (Fecha de consulta, 08/02/2021).

[5] Personal de SecureList by Kaspersky. <<https://securelist.lat/apt-predictions-for-2021/91866/>>. Boletín de seguridad de Kaspersky, noviembre de 2020. Disponible en línea. https://securelist.lat/apt-predictions-for-2021/91866/ (Fecha de consulta, 10/02/2021).

[6] Personal de Trend Micro Research. <<Turning the Tide: Trend Micro Security Predictions for 2021>>. Report de Trend Micro, noviembre de 2020. Disponible en línea. https://documents.trendmicro.com/assets/rpt/rpt-turn-the-tide-trend-micro-security-predictions-for-2021.pdf (Fecha de consulta, 10/02/2021).

[7] Personal de Trend Micro. <<Takeaways from Trend Micro's 2021 Security Predictions>>. Blog de Trend Micro Research, noviembre de 2020. Disponible en línea. https://www.trendmicro.com/en_us/research/20/l/takeaways-from-trend-micro-2021-security-predictions.html (Fecha de consulta, 12/02/2021).

[8] Personal de Trend Micro Resarch. <<Predicciones de seguridad de Trend Micro para 2021>>. Report de Trend Micro, noviembre de 2020. Disponible en línea. https://documents.trendmicro.com/assets/rpt/rpt-Predicciones-Seguridad-2021-ES.pdf?_ga=2.43598893.924492789.1612430230-25570156.1592303320 (Fecha de consulta, 12/02/2021).

[9] Personal de Check Point. <<Check Point Software's Cyber-security Predictions for 2021: Securing the 'Next Normal'>>. Press de Check Point, diciembre de 2020. Disponible en línea. https://www.checkpoint.com/press/2020/check-point-softwares-cyber-security-predictions-for-2021-securing-the-next-normal/ (Fecha de consulta, 13/02/2021).

[10] Personal de Check Point. <<Check Point Software´s predictions for 2021: Securing the 'next normal'>>. Blog de Check Point, diciembre de 2020.

Disponible en línea. https://blog.checkpoint.com/2020/11/10/check-point-softwares-predictions-for-2021-securing-the-next-normal/ (Fecha de consulta, 14/02/2021).

[11] Personal de ESET. <<Ransomware and fileless malware to present increased threat in 2021, predict ESET>>. Report de ESET, diciembre de 2020. Disponible en línea. https://www.eset.com/int/about/newsroom/press-releases/research/ransomware-and-fileless-malware-to-present-increased-threat-in-2021-predict-eset/ (Fecha de consulta, 15/02/2021).

[12] Personal de ESET. <<Cybersecurity Trends 2021: Staying secure in uncertain times>>. Paper de ESET, diciembre de 2020. Disponible en línea. https://www.welivesecurity.com/wp-content/uploads/2020/11/ESET_Cybersecurity_Trends_2021.pdf (Fecha de consulta, 17/02/2021).