TENDENCIAS EN CIBERSEGURIDAD PARA EL 2021:

Mantenerse seguro en tiempos de incertidumbre

TABLA DE CONTENIDOS

INTRODUCCIÓN

La pandemia del COVID-19 provocó una conmoción para el "sistema", empujando a muchos de nosotros a una espiral de preocupación y dándole un nuevo significado a la permanencia del cambio. Con el 2020 terminando pronto, una de las grandes preguntas en boca de todos es: ¿cómo será el 2021?

2020 fue el año que nadie vio venir, y claramente no estamos hablando únicamente en materia de seguridad de la información. La pandemia del COVID-19 fue un cimbronazo para todo el mundo y representó un cambio de paradigma y de hábitos que seguramente tendrá consecuencias muy profundas que todavía no podemos avizorar. La pregunta entonces es: ¿cómo hablar de lo que podría llegar a suceder en 2021 después de un año como el que acabamos de transitar? Y lo cierto es que a pesar de representar todo un desafío, creemos que la mejor manera de poder estimar tendencias es relatar algunos hechos que vienen ocurriendo para poder comprenderlos de una mejor manera y así intentar establecer un posible desarrollo de lo que podemos esperar de cara al futuro.

Este año un campo en el que vimos uno de los mayores cambios es en el ámbito del trabajo, y podríamos afirmar que se cristalizó algo que ya venía asomándose con suceder desde hace tiempo. El problema es que la implementación del teletrabajo de manera masiva, en lugar de darse de manera paulatina, sucedió de una manera brutal, a las apuradas y mezclándose con una vida cotidiana y una situación social absolutamente convulsionada. A esto se le suma el hecho de que los cibercriminales se adaptan rápido a estas situaciones y buscaron empezar a explotar las oportunidades que la improvisada implementación del teletrabajo le presentaban. Empresas poco preparadas a nivel técnico y de conocimiento, empleados no concientizados en un uso seguro y correcto de las herramientas a disposición, y una situación extrema obligan a adaptarse y repensar algunas de las lógicas y paradigmas que se venían manejando en torno al trabajo. En la sección "*El futuro del trabajo*", Jake Moore nos plantea las diferentes aristas de seguridad de uno de los temas más debatidos durante 2020 y que seguramente seguirá siendo discutido el próximo año.

A esta altura no cabe ninguna duda sobre el hecho de que la tecnología se ha logrado entrelazar en todos los aspectos de la vida humana, y el año 2020 fue la muestra más clara de cómo hoy la gran mayoría de los procesos y prácticas humanas tienen alguna conexión con lo tecnológico. Ya desde hace algunos años que venimos hablando de la Internet de las Cosas (IoT), pero una faceta de la que quizás no se menciona demasiado es la aplicación de la tecnología en la sexualidad. La aparición de juguetes sexuales conectados a Internet no fueron una novedad durante 2020, aunque sí lo ha sido el aumento en las ventas de este tipo de dispositivos a raíz de las diferentes medidas de distanciamiento social generadas a partir de la pandemia del COVID-19. Lo que tampoco es una novedad es que los cibercriminales buscan todo el tiempo lograr el acceso a información privada y sensible de los usuarios, algo que pueden obtener de un dispositivo vulnerable como una computadora, un teléfono móvil o un juguete sexual. En "*El sexo en la era digital*", Denise Giusto y Cecilia Pastorino indagan sobre este tema y qué nos depara para el futuro.

El ransomware por su parte viene pisando fuerte desde hace ya varios años. Dado que su infección se vuelve evidente para los usuarios, su funcionamiento es bastante llamativo y definitivamente se trata de un código malicioso que no pasa desapercibido tal como sucede con muchos otros. Pero más allá de su "popularidad", cuyo pico máximo pudo haber sido WannaCry y su infección global en 2017, en los últimos años hemos asistido a algunos cambios en el comportamiento de las bandas que crean y propagan este tipo de amenazas. A su funcionamiento "tradicional" que implicaba el secuestro de información y el pedido de un rescate para restaurar el acceso a la misma, ahora se le suman mecanismos extorsivos y la amenaza de difundir la información secuestrada. En la sección "*Ransomware con una vuelta de tuerca*", Tony Anscombe hace un repaso de esta tendencia y que nos depara para el futuro respecto de este código malicioso.

Y así como los creadores de ransomware no se mantienen quietos, tampoco lo hacen aquellos que se valen de otros códigos maliciosos para obtener réditos fraudulentos. Es por eso que en el último tiempo hemos asistido al uso cada vez más habitual de los LOLBaS (Living Off the Land Binaries and Scripts), que consisten en la utilización de binarios propios del sistema para llevar adelante actividades maliciosas. En "*Más allá de las tecnologías de prevención*", Camilo Gutiérrez relata cómo funciona este tipo de amenaza que se ha convertido en un desafío para las organizaciones dada la dificultad que supone su detección, y que podría llegar a convertirse en un problema aún mayor si no la tiene en cuenta al a hora de establecer los controles de seguridad correspondientes.

Luego de un año que a futuro seguramente sea visto como un punto inflexión para muchos cambios sociales, creemos que hacer un repaso de diferentes situaciones como las que se plantean en las cuatro secciones del presente informe, se vuelve una tarea imprescindible para intentar develar qué es lo que puede llegar a ocurrir en un futuro cercano.

1

EL FUTURO DEL TRABAJO:

ABRAZANDO UNA NUEVA REALIDAD

2020 fue el año en que las empresas pasaron al trabajo remoto, pero ¿quién las ayudó realmente en este proceso de digitalización acelerada? ¿Fue el CEO, el CTO o, más sinceramente, el COVID-19? ¿Y cómo será el trabajo después de la pandemia?

Jake Moore
ESET Security Specialist

Desde que los gobiernos de todo el mundo implementaron cuarentenas por el COVID-19, la cultura del trabajo ha cambiado drásticamente en formas que la mayoría de la gente nunca se habría imaginado. ¿Cuál fue el resultado? La *masiva implementación del trabajo remoto* que ha tenido una dependencia tecnológica como nunca antes, junto con una resultante disrupción de las infraestructuras tecnológicas de muchas empresas. Los sistemas centrales de TI han sido sustituidos por una red de individuos dispares, que tienen una mayor responsabilidad debido al uso que hacen de la tecnología y la necesidad de contar con seguridad cibernética. Las empresas con sistemas de seguridad fracturados son sumamente vulnerables, pero aquellas que depositan toda la confianza en los empleados para manejar la ciberseguridad también corren un riesgo grave.

En tiempos en los que la continuidad del negocio dependen de la capacidad de adaptación de cada empresa, los actores maliciosos están aprovechando continuamente las vulnerabilidades de seguridad que surgen del trabajo remoto. Por supuesto, hay formas de hacer que nuestros nuevos entornos sean más seguros. Aunque se pueden implementar medidas simples para reducir la posibilidad de un ataque cibernético, pasar de tener una o dos oficinas a docenas o incluso cientos de oficinas domésticas generalmente tiene un precio.

LO QUE APRENDIMOS CON EL COVID-19

La pandemia no solo nos enseñó que es posible trabajar desde casa, sino también que las empresas son capaces de crear políticas y hacerlas cumplir en cuestión de semanas. La reubicación de toda la fuerza laboral de una empresa en una situación normal habría requerido meses de planificación, consultas interminables a asesores y luego más planificación antes de obtener la aprobación de las múltiples partes involucradas. Pero cuando el mismo gobierno es el que informa que ya no está permitido ingresar a las oficinas, es sorprendente la rapidez con la que estos cambios pueden entrar en vigor y hasta lograr que la empresa siga operando sin interrupciones cuando las cosas se ponen difíciles.

No obstante, aún tenemos algunas preguntas pendientes: ¿Cómo podemos proteger a los trabajadores remotos? ¿Trabajar desde casa es tan seguro como trabajar en la oficina? ¿Volveremos alguna vez a la vida de oficina de 2019?

Para poder resistir los ataques cibernéticos, muchas empresas cuentan con políticas sólidas y evaluaciones de riesgo, y muchas también tienen medidas de protección para combatir la gran mayoría de las amenazas que cualquier empresa normal esperaría encontrar. Sin embargo, es poco probable que alguna organización en el mundo estuviera completamente preparada para afrontar este enorme y rápido cambio laboral cuando el COVID-19 sacudió al mundo. Las paredes físicas de la oficina actúan como un gran Firewall y, en general, cualquier movimiento anormal en la red se destaca fácilmente. Pero cuando todos los integrantes de la organización se conectan desde una red que se encuentra fuera del perímetro de seguridad habitual, el Director de Seguridad de la Información (CISO) y otros responsables pueden enfrentarse a algunas tareas desalentadoras, por decir lo menos.

Está claro que el trabajo remoto de una forma u otra llegó para quedarse en el largo plazo, pero para operar de manera eficiente se requiere contar con una excelente gestión corporativa, así como políticas de seguridad perfectamente integradas. Para que las empresas funcionen sin problemas con una interrupción mínima, deben darle la misma importancia a las prácticas de gestión y a las de seguridad, lo que a su vez protege al personal y a la empresa. Algunas organizaciones se desviaron de su curso cuando se dio la instrucción de enviar a su personal a casa, pero otras aceptaron el cambio e incluso descubrieron que era más productivo.

La capacitación puede resultar muy útil para proteger al personal y funciona mejor cuando se imparte con frecuencia y en pequeñas dosis. Por ejemplo, se puede llevar a cabo a través de recordatorios breves sobre la importancia de las redes privadas virtuales (VPN) y la concientización sobre los correos electrónicos de phishing para que las personas se mantengan atentas sin frustrarse ni asustarse.

ANTES VS. DESPUÉS

Antes del COVID-19, los ataques cibernéticos ya estaban aumentando, y la pandemia y la cuarentena resultante no hicieron más que incrementar aún más este riesgo. Desde las estafas de phishing hasta el malware relacionado con el COVID-19, los ciberdelincuentes se han abalanzado sobre las vulnerabilidades que se desprenden del trabajo descentralizado y los sistemas de TI para encontrar grietas por donde filtrarse.

El trabajo remoto ha aportado flexibilidad, pero también ha alterado drásticamente los procesos y sistemas empresariales para atender a una fuerza de trabajo geográficamente dispersa. La relación de los empleados con los departamentos de TI ha cambiado. La colaboración y el trabajo en equipo se facilitan virtualmente, y la falta de comunicación cara a cara puede obstaculizar los canales directos de comunicación. Algunas de las medidas de seguridad básicas que se dan por sentado en la oficina deben compensarse en casa, como exigir que los trabajadores remotos utilicen la ***autenticación multifactor*** o una VPN para acceder a las redes internas. Recordarles a los trabajadores que habiliten las actualizaciones automáticas y que verifiquen la seguridad de sus propias redes de Wi-Fi también es crucial como primera línea de defensa contra los ciberdelincuentes. Lo ideal es que los trabajadores remotos siempre utilicen dispositivos entregados por la empresa y permanezcan completamente alertas a las amenazas constantes y persistentes.

El cambio de la noche a la mañana en nuestra cultura de trabajo remoto ha sido fundamental para muchas organizaciones, ya que demostró que el trabajo

remoto es útil y que lo seguirá siendo en el futuro. Sin embargo, no debemos volvernos complacientes. Pronto extrañaremos las charlas al lado del expendedor de agua fría o durante el almuerzo, donde conversábamos sobre la última estafa de phishing u otros consejos prácticos de seguridad que a menudo ayudan a las personas a tomar las decisiones correctas.

PREPARAR LA ORGANIZACIÓN PARA EL FUTURO

Las empresas que ya operaban totalmente en forma digital estaban sin duda mejor preparadas para trasladar su fuerza de trabajo a casa, pero no todas fueron tan afortunadas. Hay que recordar que para miles de empresas hoy en día es un requisito que sus empleados trabajen desde casa. No obstante, si la seguridad está bien integrada a la política institucional, no hay ninguna razón por la que la mayoría de las organizaciones del mundo no puedan seguir trabajando de manera segura fuera de la oficina.

¿Pero qué pasará si hay una vacuna? ¿Volverá todo a la normalidad? No lo creo. Todos hemos aprendido que el trabajo remoto puede beneficiar a las organizaciones y que es posible hacer la transición en forma segura. Pero por otra parte, tampoco creo que trabajemos remotamente los cinco días de la semana. Lo que descubrimos es que, mientras funcione, seguiremos trabajando desde casa cuando nos convenga... lo que sin duda beneficiará nuestra salud y bienestar.

Personalmente, noté que trabajar desde casa mejora enormemente mi vida familiar. Nunca había pasado tanto tiempo con mis hijos pequeños, y me han dicho varias veces lo agradable que es verme en casa más seguido. El ajetreo del lunes a viernes de 9 a 5 ha terminado para siempre, y el COVID-19 fue el responsable de *acelerar el proceso con tanta rapidez*, que de otra forma probablemente habría tardado años, si es que ocurría. Más empleados en todo el mundo seguirán implementando de manera natural y sin esfuerzo la forma de trabajo que mejor funcione para ellos y sus negocios, lo que a su vez creará un mejor entorno para todos. El hecho de que el proceso pueda tomarse en serio y en forma segura lo hace posible.

Independientemente de lo que depare el futuro, dos cosas son ciertas: la forma en que trabajamos se ha alterado permanentemente y los ataques cibernéticos no van a desaparecer. La pandemia del COVID-19 solo aceleró la implementación de tecnología en todas las facetas de la vida y, a medida que más y más partes de nuestra vida laboral y doméstica se digitalicen, la seguridad cibernética seguirá siendo el eje de la seguridad empresarial.

Los ataques cibernéticos son una amenaza persistente para las organizaciones, y las empresas deben crear equipos y sistemas de TI resistentes para evitar los daños financieros y a la reputación que estos ataques ocasionan. Entender la fuerza laboral tiene un papel fundamental en la estrategia de ciberseguridad de cualquier negocio, ya que permite mejorar la eficacia de la capacitación y a su vez ayuda a incentivar a los empleados para que inviertan más en su propia formación y habilidades. Si comprendemos que el elemento humano en la seguridad cibernética es tan importante como el técnico, habremos dado el primer paso en la construcción de protocolos holísticos que tengan en cuenta las fortalezas individuales y los puntos débiles.

2

RANSOMWARE CON UNA VUELTA DE TUERCA:

PAGA O TUS DATOS SERÁN FILTRADOS

Con los operadores de ransomware aumentando los valores de los rescates y buscando nuevas maneras de forzar a las víctimas para que paguen, las víctimas cada vez tienen más en juego. ¿Cómo va a evolucionar la escena del ransomware en 2021?

Tony Anscombe
ESET Chief Security Evangelist

Algo que considero que debería cambiar en el 2021 es la *definición de "ransomware"*:

> ***"El Ransomware es un programa informático ilegal que impide que una computadora funcione o que el usuario obtenga información hasta que haya pagado algo de dinero."***
>
> ***(Collins English Dictionary)***

¿Por qué debería cambiar la definición?

Los años 80 son recordados por muchas cosas: las cintas con compilados de canciones, las hombreras, el cubo de Rubik y los conciertos de Live Aid, por nombrar algunas, pero pocos asociarían esa década con el ransomware. En 1989 nació una nueva amenaza informática llamada el troyano del SIDA, que infectaba los dispositivos a través de un disquete, ocultaba directorios, y cifraba los nombres y las extensiones de los archivos almacenados en el disco rígido. El usuario recibía un mensaje indicando que debía enviar 189 dólares a un apartado de correos en Panamá, con lo que renovaría su licencia y resolvería el problema. Treinta y un años después, tras varios giros y matices en su evolución, el término "ransomware" ya es de uso común en todo el mundo.

Hoy en día, el ransomware se asocia más que nada con un programa malicioso que cifra archivos y datos, y bloquea el acceso hasta que el usuario paga el rescate solicitado a cambio del método de descifrado, o al menos uno espera que eso haya sido todo. Durante su evolución, el ransomware ha ido adoptando diversas formas, por ejemplo, en ciertos casos bloquea el dispositivo completo sin cifrar nada y muestra un mensaje que exige el pago de un rescate para recuperar el acceso; en otros casos bloquea la pantalla del dispositivo, muestra imágenes pornográficas y exige el pago a través de un SMS Premium para recuperar el acceso y evitar que se muestren las imágenes.

La gran cuota de mercado de Microsoft Windows crea un entorno de ataque ideal para los ciberdelincuentes que buscan obtener dinero de sus víctimas. Sin embargo, es importante señalar que otras plataformas no son inmunes, ya que también hay ataques de ransomware dirigidos a OS X de Apple y al sistema operativo Android de Google.

NUEVOS MÉTODOS DE PRESIONAR A LAS VÍCTIMAS

Si bien la exfiltración y la extorsión no son prácticas nuevas, ciertamente es una tendencia creciente. Los ataques están adoptando una nueva modalidad: los delincuentes primero extraen una copia de los datos confidenciales de la víctima y la guardan en su propio entorno. A continuación, cifran los datos y bloquean el acceso en los servidores de la víctima. Luego amenazan con publicar y vender o subastar los datos confidenciales robados si el usuario se rehúsa a pagar el rescate. Esta técnica requiere que el atacante invierta bastante tiempo, ya que necesita obtener acceso a la red, identificar los datos confidenciales y extraer una copia para guardar en su propio entorno.

Consideremos por un momento el ataque desde el punto de vista del ciberdelincuente: las empresas se están volviendo cada vez más inteligentes, despliegan tecnologías que frustran sus ataques, crean procesos resistentes de backup y restauración, y se muestran menos dispuestas a pagar por el rescate. Por lo tanto, necesitan un "Plan B" para poder monetizar su esfuerzo y crear mayor resistencia en lugar de depender de una sola forma de amenaza (el típico ransomware que infecta el equipo y cifra los datos). Al guardarse previamente una copia de los datos, logran mayor resistencia y un argumento de venta infranqueable para cerrar el trato con su "cliente", es decir, la víctima.

El grupo de ciberdelincuentes Maze, por ejemplo, se hizo famoso por sus ataques de exfiltración y extorsión. A finales de 2019, el grupo publicó detalles de datos que afirmaba haberle robado a Southwire, una fábrica estadounidense de cables que se negó a pagar el rescate de 6 millones de dólares. A continuación, el grupo prosiguió con su actividad nefasta publicando una lista de empresas que se negaron a cooperar y las amenazó con publicar documentos y datos confidenciales. En marzo de 2020, cuando el mundo estaba desbordado por el caos de la pandemia del COVID-19, el grupo Maze supuestamente envió un tweet donde decía que, debido a la crisis mundial, ofrecerían un descuento a todas las empresas que no cooperaran y se abstendrían de atacar a las organizaciones médicas hasta que la situación mejorara.

El prolongado escenario de exfiltración de datos y la posterior extorsión requiere un conjunto de habilidades diferentes y una cierta cuota de paciencia por parte de los ciberdelincuentes. Si bien muchos de los ataques de ransomware solo consisten en negarle el acceso a la víctima, ya sea mediante el bloqueo o el cifrado, la nueva tendencia creciente de extraer previamente una copia de la información requiere que los atacantes se infiltren en una red y se desplacen sin ser detectados de modo de poder identificar y copiar los datos confidenciales. Ya no se trata de un empleado o consumidor desprevenido que abre un simple enlace o archivo adjunto de phishing en un correo electrónico, desatando sin querer un ataque de ransomware. No obstante, sigue siendo necesario el punto de entrada inicial, ya sea mediante técnicas para explotar el protocolo de escritorio remoto (RDP), forzando el acceso mediante ataques de relleno de credenciales o a través de mecanismos más tradicionales de phishing e ingeniería social.

Una vez dentro de la red, busca permanecer sin ser detectado, reunir información y recopilar credenciales y contraseñas adicionales para asegurarse de conservar este acceso incluso aunque se cierre la ruta inicial. El trabajo preliminar y la inteligencia para trazar el mapa de una red y comprender lo que es valioso lleva tiempo y requiere recursos especializados para lograr el objetivo final de identificar las joyas digitales de la empresa, cuya vulneración, bloqueo o publicación generarán la máxima perturbación en la organización. Recién una vez que el atacante haya extraído sigilosamente los datos de interés, pasará a la implementación más tradicional del ransomware. Con su acceso privilegiado

a la red, el ciberdelincuente incluso tiene la oportunidad de desactivar el software de protección para garantizar el éxito del ataque.

LAS DEMANDAS CAMBIANTES

Los ciberdelincuentes necesitan financiar el conjunto de aptitudes adicionales y el tiempo necesario para perpetrar estos ataques, lo que claramente se traduce en el aumento de los valores de los rescates. En 2018, la ciudad estadounidense de Atlanta sufrió un ataque de ransomware al estilo tradicional. Los servidores de su infraestructura clave fueron cifrados y los atacantes exigieron 51.000 dólares a cambio del método de descifrado. Atlanta hizo lo correcto: se negó a pagar y reconstruyó sus sistemas, aunque según dicen le costó 9,5 millones de dólares.

En los últimos 18 meses, el monto de los rescates ha aumentado, aunque desafortunadamente no con la inflación normal. Lake City y Riviera Beach City en Florida pagaron 500.000 y 600.000 dólares respectivamente. Lion, una empresa de bebidas australiana, se negó a pagar un rescate de 1 millón de dólares y a la Universidad de California en San Francisco le pidieron un rescate de 3 millones de dólares y pagó 1,1 millones. En poco más de dos años, el rescate pedido a Atlanta parece insignificante; definitivamente hay un aumento no deseado en el valor de los rescates, una tendencia que es muy probable que continúe.

La demanda de pagos en Bitcoins no es la única métrica que ha cambiado. Coalition, una empresa de seguros cibernéticos que atiende a 25.000 pequeñas y medianas empresas en América del Norte, publicó recientemente un *informe* donde resume los pedidos de rescate para la primera mitad de 2020, que por supuesto incluye el inicio de la pandemia. El informe señala que "la gravedad media de los reclamos hechos por los asegurados de Coalition aumentó en un 65% de 2019 a 2020, en gran parte debido al aumento de los costos del ransomware". El informe además detalla que el 41% de todos los reclamos son por ransomware y afirma que "en el último tiempo un mayor número de grupos de ransomware está robando los datos de las organizaciones antes de cifrarlos para luego amenazar con exponer públicamente los datos robados si no se paga el rescate". Los datos independientes del informe de Coalition ofrecen una perspectiva diferente y confirman el cambio en el modus operandi utilizado por los ciberdelincuentes, así como el aumento del costo de los rescates.

LOS VALORES SUBEN

Ahora avancemos rápidamente a Agosto de 2020, donde encontraremos otra historia de vulneración de datos: Blackbaud, una empresa de servicios en la nube que provee software para la recaudación de fondos a organizaciones de todo el mundo, *anunció que había sorteado con éxito un ataque de ransomware*. En cooperación con un experto forense digital y con la policía, el equipo de seguridad cibernética de Blackbaud había impedido que el ciberdelincuente cifrara los datos y los bloqueara en sus propios sistemas. Sin embargo, el atacante pasó rápidamente a un Plan B: si pagaban el importe que exigía, eliminaría los datos confidenciales de los clientes que había extraído de los sistemas corporativos antes de que el equipo de seguridad cibernética eliminara con éxito la amenaza.

Blackbaud, sorprendentemente, pagó una suma no revelada a los cibercriminales con la condición de que le proporcionara una prueba de la eliminación. La existencia del Plan B rindió sus frutos para los atacantes, a pesar de los heroicos esfuerzos de los equipos que frustraron el ataque. Si el ataque se hubiera limitado al escenario más tradicional de infección y cifrado, tal vez nunca habríamos oído hablar de él. No obstante, como los datos copiados (robados) incluían información personal identificable de individuos, la empresa estaba obligada en algunos lugares, gracias a las leyes sobre protección de la privacidad, a informar a los clientes y a los organismos reguladores que se había producido una vulneración de datos.

Lograr frustrar un ataque o contar con adecuados procesos de backup y restauración pueden no ser suficientes para defenderse de un ciberdelincuente que exige el pago de un rescate. El éxito para rentabilizar la operación como consecuencia del cambio de técnica (por más que consuma muchos recursos y paciencia) les ofrece a los ciberdelincuentes una mayor posibilidad de obtener un retorno de la inversión (ROI); sí, es un "negocio" donde también se tiene en cuenta el ROI. En el escenario de Blackbaud, el ataque de ransomware no implementó software malicioso ni bloqueó el acceso a los sistemas o datos: así que estamos presenciando otra evolución del término "ransomware", una tendencia que, lamento decir, estoy seguro de que se repetirá en 2021.

3

MÁS ALLÁ DE LAS TECNOLOGÍAS DE PREVENCIÓN:

SIGUIENDO DE CERCA EL ESCENARIO CAMBIANTE DE LAS CIBERAMENAZAS

Los actores maliciosos siempre ven la forma de lograr que sus ataques sean más difíciles de detectar y frustrar, incluso mediante el uso de herramientas legítimas del sistema para fines nefastos. ¿De qué manera debemos prepararnos?

Camilo Gutiérrez Amaya
ESET Head of Awareness
& Research LATAM

Desde que apareció el concepto de 'virus informático' hace *más de 30 años*, las amenazas informáticas no han dejado de evolucionar y llegaron a convertirse incluso en uno de los riesgos con mayor impacto para la humanidad en los próximos diez años, afirma el Foro Económico Mundial en el *Global Risks Report 2020*. Por otra parte, la situación de la pandemia por el COVID-19 provocó un incrementó en el riesgo de sufrir un incidente de seguridad. Esto lo confirmó el aumento de los intentos de ataque durante este año, según afirmó la *ONU* y organizaciones como el *National Cyber Security Center* (NCSC) del Reino Unido.

Frente a este panorama vale la pena mencionar que en los últimos años hemos visto cómo los grupos de cibercriminales se han volcado al uso de técnicas cada vez más complejas para lograr ataques cada vez más certeros. Es así como desde hace algún tiempo comenzamos a hablar de ataques 'Fileless Malware', que son aquellos en los cuales se hace uso de herramientas y procesos propios del sistema operativo para ejecutar la actividad maliciosa utilizando elementos preinstalados y sin droppear ejecutables adicionales en el sistema de la víctima. A estos binarios se comenzó a denominarlos LOLBaS (Living Off the Land Binaries and Scripts) y desde finales del 2017 el término se empezó a utilizar para

hacer referencia a las técnicas aprovechadas por los cibercriminales para utilizar este tipo de binarios que son propios del sistema. El objetivo detrás del uso de estas técnicas es maximizar la efectividad de sus ataques dada la dificultad para ser detectados.

DONDE TODO COMENZÓ

Es importante destacar que el uso de este tipo de técnicas no es algo nuevo. Ya desde 2001 con la aparición del *gusano CodeRed* empezamos a ver cómo algunas familias de códigos maliciosos empezaron a abusar de estas características, pero en los últimos años estas técnicas comenzaron a utilizarse cada vez con mayor frecuencia en diferentes campañas de ciberespionaje y por diferentes actores maliciosos; principalmente para ataques a blancos de alto perfil como son entidades gubernamentales. Este fue el caso de *Operation In(ter)Ception* y los ataques dirigidos a compañías militares y aeroespaciales en Europa y Medio Orienta o el caso reciente de *Evilnum* y sus ataques al sector financiero.

Muchas de las técnicas, tácticas y procedimientos (TTP) de estos grupos están reseñadas en el framework ATT&CK® de *MITRE*. Algunos de los mejor documentados por la industria quizás sean los relacionados con *APT34*, también conocido como Lazarus Group, que fue ganando relevancia en el ámbito del cibercrimen con casos como el ataque a *Sony Pictures* en 2014, pasando por los ataques a *cadenas de casinos en Centroamérica* en 2017 y más acá en el tiempo por ataques a *entidades financieras en Europa*. Más recientemente, de acuerdo a informes del equipo de investigación de ESET, el grupo *Invisimole* también basa sus operaciones en el uso técnicas "living off the land" con un completo set de herramientas para realizar campañas de ciberespionaje aprovechando, por ejemplo, aplicaciones vulnerables como Total Video Player o speedfan.sys, además de componentes legítimos como *rundll32* y *womapiexec* para tratar de evadir las tecnologías de defensa.

Pero basta con buscar información dentro de MITRE ATT&CK® acerca del uso malicioso de binarios como *certutil*, *esentutl* o *regsvr32*, por mencionar solamente algunos, para encontrar un número mayor de grupos de APT que utilizan estas técnicas. Solamente revisando los grupos que usan estos tres binarios, encontramos más de 100 actores maliciosos diferentes que las utilizan, dentro de los cuales destacan algunos como Turla, Machete, Fancy Bear o Cobalt Group.

Por lo tanto, y dados los antecedentes mencionados, puede esperarse que 2021 sea un año en el que los incidentes relacionados con este tipo de técnicas tengan un mayor impacto, siendo sectores como el de infraestructuras críticas o el financiero los que posiblemente sean más apuntados.

ENTENDIENDO LOS MODELOS DE ATAQUE PARA SABER CÓMO PROTEGERSE

Una de las principales características de este tipo de ataques basado en el uso de programas legítimos es que logra reducir de manera significativa los rastros de los cibercriminales, cargando y ejecutando la acción maliciosa desde la memoria del equipo sin afectar el sistema de archivos. En consecuencia, genera nulos o escasos artefactos forenses que se puedan analizar posteriormente.

Esto hace que sea más difícil la detección y, por lo tanto, la prevención de los ataques. Asimismo, son particularmente efectivos cuando la seguridad de una organización está orientada a tecnologías de detección basadas en listas blancas o no cuenta con una heurística que brinde capacidades avanzadas de detección.

Otra de las principales características es que este tipo de ataques suelen ser bastante sigilosos, ya que buscan evadir la mayoría de las soluciones de seguridad y además limitar las posibilidades de hacer un análisis forense. En este contexto el uso de herramientas como PowerShell y WMI (Windows Management Instrumentation) por parte de los atacantes es recurrentes debido principalmente a sus características, ya que facilitan la automatización de tareas y la gestión de la configuración del sistema operativo.

Por sus características, los atacantes suelen utilizar este tipo de técnicas para lograr persistencia, escalación de privilegios e incluso exfiltración de información. Los accesos iniciales siguen estando asociados a explotación de vulnerabilidades o campañas de ingeniería social. Por lo tanto, esto empieza a generar la necesidad de considerar otros modelos para la gestión de la seguridad que vayan más allá de las tecnologías de prevención, y que además consideren la detección y respuesta ante incidentes.

RETOS DE SEGURIDAD PARA LAS EMPRESAS

La clave para que las empresas puedan hacer frente a este tipo de ataques durante el 2021 es fortalecer la estructura de procesos y procedimientos que permita integrar tecnologías y personas para el seguimiento de todo el ciclo de una amenaza, desde que un atacante busca el acceso inicial a un sistema hasta que logra la exfiltración de información o algún otro tipo de impacto. Para esto se vuelve fundamental considerar varias capas de tecnologías que permitan tener visibilidad antes, durante y después de un ataque.

Este tipo de capacidades se logran con tecnologías como EDR, que amplía las capacidades para entender lo que está sucediendo dentro de una infraestructura y que junto con las tecnologías de detección permitirán aumentar la capacidad para controlar las actividades sospechosas deteniendo comportamientos considerados como peligrosos, investigar posibles incidentes que pueden ser parte de un ataque o incluso permitir aislar aquellos dispositivos que pudieran estar implicados.

La evolución de amenazas basada en LOLBaS ha sido bastante rápida, tanto es así que en menos de cinco años las técnicas han ido evolucionando y es de esperarse que para 2021 se utilicen en ataques cada vez más complejos y a mayor escala. Esta situación plantea la necesidad de que los equipos de seguridad al interior de las empresas desarrollen procedimientos asociados con herramientas y tecnologías que permitan no solamente prevenir infecciones con códigos maliciosos, sino también que puedan detectar y responder incluso antes de que estos ataques cumplan su cometido. Si bien el 2020 aceleró los procesos de transformación digital debido a los cambios provocado por la pandemia, 2021 trae nuevos retos para que las empresas sigan con la adopción de tecnologías que les permita ampliar sus capacidades de visibilidad y monitoreo de comportamientos sospechosos. Para esto es clave contar con las herramientas apropiadas y un equipo de personas capacitadas que ayuden en la detección temprana de incidentes y en la rápida respuesta ante incidentes.

4

MALAS VIBRACIONES:

VULNERABILIDADES EN JUGUETES SEXUALES INTELIGENTES

¿Qué tan seguros son los juguetes sexuales? ¿Los fabricantes están haciendo lo necesario para proteger los datos y la privacidad de las personas? ¿Por qué la seguridad es tan crítica cuando se trata de juguetes para adultos?

Cecilia Pastorino
ESET Security Researcher

Denise Giusto Bilić
ESET Security Researcher

No es ninguna novedad que los dispositivos de la Internet de las cosas (IoT) tienen vulnerabilidades. ESET ya ha analizado fallas graves encontradas en varias *centrales inteligentes* y *cámaras inteligentes*. Además, *los investigadores de ESET recientemente descubrieron KRØØK*, una grave vulnerabilidad que afectó el cifrado de más de mil millones de dispositivos de Wi-Fi.

Aunque los dispositivos IoT han sido el objetivo de innumerables brechas de seguridad que provocaron la exposición de los datos de inicio de sesión, información financiera y ubicación geográfica de los usuarios, entre otras cosas, existen pocos tipos de datos con tanto potencial para dañar a un usuario, si se publican, que los relacionados con la conducta sexual.

Como todo el tiempo ingresan al mercado nuevos modelos de juguetes inteligentes para adultos, uno imaginaría que los fabricantes también se están ocupando de fortalecer los mecanismos para asegurar las buenas prácticas en el procesamiento de la información de los usuarios. No obstante, muchas investigaciones han demostrado que estamos muy lejos de poder utilizar juguetes sexuales inteligentes sin exponernos al riesgo de un ciberataque. Ahora, estos hallazgos son más relevantes que nunca, ya que estamos viendo un rápido *aumento en las ventas de juguetes sexuales* que refleja la crisis de salud global y las medidas de distanciamiento social relacionadas con el COVID-19.

Entonces, ¿qué tan seguros son los juguetes para adultos en este momento y qué nos depara el futuro? ¿Se han tomado las precauciones necesarias para proteger los datos y la privacidad de las personas? ¿Por qué la seguridad es tan crítica cuando se trata de los juguetes sexuales?

CÓMO ENTRA EN JUEGO LA SEGURIDAD

Como es de imaginar, la información procesada por los juguetes sexuales inteligentes es extremadamente confidencial: nombres, preferencias y orientaciones sexuales, lista de parejas sexuales, información sobre el uso del dispositivo, fotos y videos íntimos; toda esta información puede tener consecuencias desastrosas si cae en manos equivocadas.

¿Quién podría estar interesado en este tipo de información? Muchos países tienen *leyes que les prohíben expresamente a los ciudadanos participar en determinadas prácticas sexuales*. ¿Qué pasaría si las autoridades locales lanzaran una campaña opresiva basada en la expropiación forzosa de los datos de las empresas que los procesan, o en el aprovechamiento de vulnerabilidades o errores en los dispositivos sexuales con el objetivo de identificar, localizar y perseguir a homosexuales, adúlteros o cualquier otra minoría o grupo social por sus elecciones sexuales? Por otra parte, los juguetes sexuales no están exentos de ser comprometidos por ciberdelincuentes. Si tenemos en cuenta el material íntimo accesible a través de las aplicaciones que controlan estos dispositivos, aparecen nuevas formas de *sextorsión* en el radar.
Además de las preocupaciones sobre la confidencialidad de los datos, debemos considerar la posibilidad de que vulnerabilidades en la app permitan la instalación de malware en el teléfono o el cambio de firmware en los juguetes. Estas situaciones podrían conducir a ataques de denegación de servicio (DoS) que bloquean la ejecución de cualquier comando, como ocurrió con una *jaula de castidad masculina inteligente que recientemente ha demostrado tener una vulnerabilidad*: les permitiría a los atacantes bloquear los dispositivos en forma masiva, con el potencial de dejar atrapadas a miles de personas. Estos dispositivos inteligentes también podrían utilizarse para llevar a cabo acciones maliciosas y propagar malware, o incluso modificarse en forma deliberada para causar daño físico al usuario, por ejemplo, haciendo que se sobrecalienten y exploten.

Paralelamente, no podemos hablar de las implicaciones de un ataque a un dispositivo sexual sin reconsiderar también la trascendencia del abuso sexual en el contexto de la transformación digital que atraviesa la sociedad. ¿Cuáles serían las consecuencias de que alguien tomara el control de un dispositivo sexual sin el consentimiento del usuario? ¿Se podría describir como un acto de agresión o abuso sexual? La noción del delito cibernético adquiere una apariencia diferente si la miramos desde la perspectiva de la invasión de la privacidad, el abuso del poder y la falta de consentimiento para un acto sexual. El consentimiento obtenido mediante el fraude no es consentimiento en absoluto, y esta laguna legislativa en las normativas vigentes deberá resolverse para garantizar la seguridad sexual, física y psicológica de los usuarios en el ámbito digital.

SUPERFICIE DE ATAQUE DE LOS JUGUETES SEXUALES INTELIGENTES

En cuanto a su arquitectura, la mayoría de estos dispositivos se pueden controlar a través de *Bluetooth Low Energy* (BLE) desde una app instalada en un teléfono inteligente. De esta forma, los juguetes sexuales actúan como sensores, que solo recopilan datos y los envían a la app para su procesamiento. La app es la encargada de configurar cualquier opción en el dispositivo y controlar el proceso de autenticación del usuario. Para ello, se conecta a través de Wi-Fi a un servidor en la nube que almacena la información de la cuenta. En algunos casos, la aplicación también actúa como intermediaria entre varios usuarios que utilizan funciones de chat, videoconferencia y transferencia de archivos, o que desean ceder el control de su dispositivo a usuarios remotos compartiendo sus tokens.

Algunos fabricantes les ofrecen a los usuarios la posibilidad de conectarse a sus dispositivos desde un software instalado en sus computadoras y utilizando un dongle BLE especial. También se puede usar la API BLE en ciertos navegadores para conectarse a los juguetes sexuales mediante una app web. Las numerosas posibilidades de conexión con los dispositivos brindan más flexibilidad, pero también aumentan la superficie de ataque.

Entonces, ¿qué podría salir mal? Esta arquitectura presenta varios puntos débiles que podrían usarse para comprometer la seguridad de los datos procesados: interceptar la comunicación local entre la app de control y el dispositivo, entre la app y la nube, entre el teléfono remoto y la nube, o atacando directamente el backend. Por supuesto, no todos los ataques se llevan a cabo a través de conexiones de red; algunos escenarios maliciosos podrían iniciarse utilizando malware previamente instalado en el teléfono o mediante la explotación de una falla en el sistema operativo.

Muchos investigadores de seguridad (*[1]*, *[2]*, *[3]*, *[4]*, entre otros) han demostrado que estos dispositivos contienen fallas que podrían amenazar la seguridad de los datos almacenados así como la del usuario. Las fallas van desde procedimientos de autenticación deficientes hasta dispositivos que anuncian constantemente su presencia, lo que permite que cualquiera pueda conectarse a ellos.

En 2016, dos investigadores presentaron una charla titulada "*Breaking the Internet of Vibrating Things*" en la que mostraron cómo la aplicación *We-Connect* recopilaba información como la intensidad, los patrones, la temperatura y los hábitos de los usuarios y la enviaba directamente a los servidores sin anonimizar los datos. El año pasado, un investigador demostró *lo fácil que podría ser para un atacante hackear un tapón anal* controlado por BLE. También fue la primera prueba de concepto en la que un dispositivo sexual inteligente podría utilizarse como instrumento para dañar a la persona que lo usa.

Este año, el equipo de investigación de ESET Latinoamérica presentó en DEF CON IoT Village una *nueva investigación sobre juguetes sexuales inteligentes no seguros*. La investigación se basó en dos dispositivos: un dispositivo portátil llamado Jive, fabricado por We-Vibe, y el masturbador masculino Max de Lovense.

Descubrimos que ambos dispositivos tenían vulnerabilidades en la implementación de las comunicaciones por BLE, permitiendo a un atacante interceptar los datos que se envían y controlar de manera remota los dispositivos a través de ataques MitM (Man-in-the-Middle) por BLE, lo que implica que cualquiera puede usar un simple escáner de Bluetooth para localizar y controlar los juguetes sexuales inteligentes que se encuentran cerca, algo similar a lo que hizo el investigador Alex Lomas en 2017: *¡iba caminando por las calles de Berlín detectando juguetes sexuales*. Esta vulnerabilidad es muy común en los dispositivos IoT, dado que la mayoría de los modelos disponibles en el mercado no implementan el emparejamiento de forma segura, lo que permite que cualquiera pueda conectarse y controlarlos.

Con respecto a la app *Lovense Remote*, encontramos varias opciones controvertidas configuradas de fábrica que pueden amenazar la confidencialidad de las imágenes íntimas enviadas por los usuarios. No había cifrado de extremo a extremo, las capturas de pantalla no estaban deshabilitadas, la opción "eliminar" en el chat en realidad no borraba los mensajes del teléfono remoto, y los usuarios podían descargar y reenviar contenido de otras personas sin ninguna advertencia. Además, los usuarios malintencionados podrían extraer las direcciones de correo electrónico asociadas con cualquier nombre de usuario y viceversa. Estos hallazgos constituyen problemas muy graves de privacidad, en especial en una app diseñada específicamente para compartir contenido sexual.

La app les permite a los usuarios otorgar el control remoto de sus dispositivos a través de una URL, que incluye un token de 4 dígitos. También encontramos problemas de seguridad con este token que permitiría a los atacantes secuestrar dispositivos remotos de forma aleatoria sin consentimiento.

En la app *We-Connect*, nos dimos cuenta de que los metadatos confidenciales no se eliminaban de los archivos antes de enviarlos, lo que significa que los usuarios pueden haber estado enviando inadvertidamente información sobre sus dispositivos y su geolocalización exacta cuando se comunican con otros usuarios. Esto podría ser muy peligroso, dado que muchos usuarios otorgan el control de sus dispositivos a completos extraños al compartir sus tokens online, ya sea como preferencia personal o como parte de un servicio de "cam girl/boy".

MEJORES PRÁCTICAS PARA EVITAR RIESGOS

Los juguetes sexuales inteligentes están ganando popularidad como parte del concepto de "sexnología", una combinación de sexo y tecnología. Es posible que estas prácticas hayan llegado para quedarse, pero no debemos olvidar las posibles amenazas a la privacidad e intimidad de los usuarios.

Para minimizar los riesgos asociados con el uso de dispositivos sexuales inteligentes, recomendamos tener en cuenta los siguientes consejos:

1. Algunas aplicaciones ofrecen la posibilidad de controlar dispositivos localmente a través de BLE sin crear una cuenta de usuario. Si no planea permitir que otros usuarios controlen su dispositivo en forma remota a través de Internet, busque uno de estos dispositivos.

2. En la medida de lo posible, evite compartir fotos o videos en los que pueda ser identificado y no publique tokens de control remoto en Internet.

3. Evite registrarse en apps sexuales con un nombre o dirección de correo electrónico oficial que pueda identificarlo.

4. Lea siempre los términos y condiciones de las apps y los sitios web en los que se registre.

5. Utilice juguetes sexuales inteligentes en un entorno protegido y evite usarlos en lugares o áreas públicas donde puede haber muchas personas que pasan cerca (como los hoteles).

6. Descargue las apps y pruebe sus funciones antes de comprar el dispositivo. Esto le dará una idea de qué tan seguro es el producto. Utilice los motores de búsqueda para saber si el modelo que piensa comprar ya tuvo vulnerabilidades en el pasado.

7. Proteja siempre los dispositivos móviles que utiliza para controlar estos juguetes, manténgalos actualizados y tenga una solución de seguridad instalada en ellos.

8. Proteja la red de Wi-Fi doméstica que utiliza para la conexión con contraseñas seguras, algoritmos cifrados y actualizaciones periódicas del firmware del router.

¿QUÉ NOS DEPARA EL FUTURO?

La era de los juguetes sexuales inteligentes apenas comienza. Los últimos avances en la industria incluyen *modelos con capacidades de realidad virtual* y robots sexuales con tecnología de inteligencia artificial que incluyen cámaras, micrófonos y funcionalidades de análisis de voz basadas en técnicas de inteligencia artificial. El *uso de estos robots como sustitutos de las trabajadoras sexuales en los burdeles* ya es una realidad.

Estos juguetes sexuales son solo una pequeña expresión de la sexualidad en el mundo digital —área que podríamos argumentar también incluye apps de citas y otros dispositivos como las "*novias virtuales*". Son la manifestación tecnológica de un fenómeno sociológico más grande que está transformando nuestra sociedad a medida que los dispositivos IoT siguen filtrándose en nuestra vida.

Como se ha demostrado una y otra vez, el desarrollo seguro y la concientización pública serán la clave para garantizar la protección de los datos confidenciales. Es necesario capacitar a los usuarios para que se conviertan en consumidores inteligentes que puedan exigirles a los fabricantes la implementación de mejores prácticas para mantener el control de su intimidad digital en los próximos años.

CONCLUSIÓN

Incluso cuando la marea comience a cambiar y retomemos una vida más cerca de lo que era previo a la pandemia, no debemos bajar la guardia.

Está claro que la pandemia generó cambios en prácticamente todas nuestras actividades, y por carácter transitivo, en nuestro uso y relacionamiento con la tecnología. Algunos de estos cambios fueron más evidentes y directos, como el teletrabajo o las clases a distancia debido al aislamiento social, mientras que otros surgieron como efecto colateral de los anteriores, alterando nuestros hábitos de consumo y de comportamiento en formas que no hubiéramos imaginado previamente. Todo esto tuvo y tendrá un fuerte impacto en la ciberseguridad al sumarle a empresas y organizaciones nuevos desafíos -a los ya existentes- para intentar protegerse de los ataques e imponiendo una necesidad de acelerar los tiempos de acción ante un escenario tan dinámico como el propio COVID-19 y con consecuencias que en algunos casos llegaron para quedarse.

En este contexto la tecnología tuvo un rol protagónico al ser el recurso que ha permitido atravesar con la mayor normalidad posible las consecuencias del aislamiento social. Sin embargo, muchas tecnologías y organizaciones, al igual que las personas, no estaban lo suficientemente preparadas desde el punto de vista de la seguridad para afrontar una nueva realidad que, si bien no es verdaderamente nueva, sí nos permitió observar, y de forma evidente, algo que sucede desde hace ya bastante tiempo: la velocidad y el dinamismo con el que los cibercriminales se adaptan para aprovechar las oportunidades. Entre las particularidades del 2020 que hicieron que este comportamiento salte a la vista fue el incremento en la adopción de servicios y tecnologías por parte de una masa crítica que obligaron a usuarios y a empresas a reaccionar velozmente ante los cambios para no verse comprometidos.

En este sentido, como se explica en el capítulo "El futuro del trabajo", la pandemia forzó la aceleración de los procesos de transformación digital y dejó en claro la necesidad de que la seguridad esté en el centro de muchas decisiones. La actividad maliciosa tuvo un importante crecimiento durante el 2020 con actores maliciosos de todo tipo intentando aprovecharse de un escenario que presentaba a más usuarios conectados, por más tiempo, y dispuestos a adoptar el uso de tecnologías y servicios online que no tenían tanta demanda previamente.

El caso de Zoom es un buen ejemplo para describir las consecuencias del impacto acelerado de esta transformación, no solo por el repentino crecimiento en la cantidad de usuarios que pasó de ser 10 millones en diciembre a 200 millones en marzo de este año, sino porque esta demanda y atención por parte de usuarios y empresas también atrajo el interés de los cibercriminales que lanzaron campañas de ingeniería social y descubrieron múltiples fallos de seguridad y de privacidad que llegaron incluso a provocar que pese a su popularidad y adopción masiva, varias empresas prohibieran su uso.

Otro ejemplo que evidencia el oportunismo de los cibercriminales durante la pandemia ha sido el ransomware y su crecimiento desde que se decretó la misma, atacando incluso a hospitales y organizaciones del sector de la salud en un momento tan delicado. Además de que distintos grupos de ransomware incrementaron sus intentos por explotar el protocolo de escritorio remoto (RDP) que utilizan los trabajadores para conectarse desde su hogar a redes corporativas, se suma que varias familias de ransomware ya desde el año pasado modificaron su estrategia sumando a los ataques más dirigidos y al cifrado de los archivos, la exfiltración de información sensible de las empresas y la posterior extorsión en caso de que decidan no pagar el rescate demandado.

Más allá de que haya sido una tendencia que se consolidó durante el 2020, esto también habla de estrategias más complejas en las que los atacantes ingresan a la red y se muevan dentro de la misma con paciencia y sin ser detectados, hasta que identifican la información sensible y realizan copias para luego hacer evidente su presencia desencadenando el ataque. En el capítulo sobre Ransomware explicamos cómo los cambios implementados por las bandas que operan estos códigos maliciosos son un claro ejemplo de la constante evolución de los cibercriminales y su intento por adoptar nuevas estrategias y desarrollar nuevas habilidades para estar vigentes y lograr sus objetivos, desafiando los mecanismos de defensa permanentemente y dejando en claro lo importante que es analizar el escenario actual pero proyectando hacia el futuro, dejando abierta la puerta a la necesidad de tomar medidas rápidas que se adapten a la realidad criminal del momento.

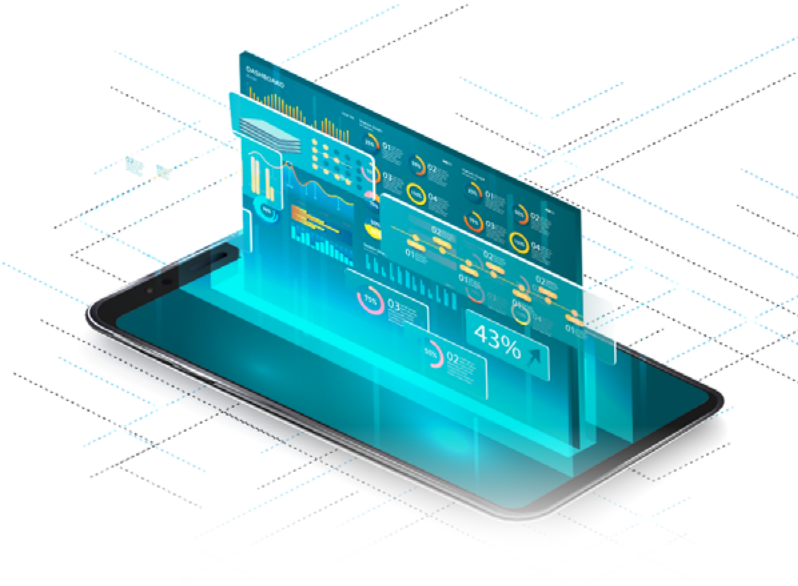
Otro ejemplo de la dinámica con la que trabajan los actores maliciosos y los desafíos de cara al futuro los podemos observar en el capítulo "Más allá de las tecnologías de prevención". Aquí se hace referencia a los retos actuales y los que vendrán si tomamos como ejemplo la rápida adopción que han tenido los denominados LOLBaS (Living Off the Land Binaries and Scripts). Este concepto hace referencia al uso de binarios propios del sistema para ejecutar actividad maliciosa utilizando elementos preinstalados. El uso de LOLBaS hace difícil la tarea de detección y por ende prevenir ataques, y son muy efectivos cuando la seguridad de una organización está orientada a tecnologías de detección basadas en listas blancas y no cuenta con capacidades de detección avanzadas.

Si bien a partir de que se determinaran las medidas de aislamiento social muchos podíamos imaginar un aumento en el uso de nuestros dispositivos para comunicarnos con nuestros seres queridos o con fines de entretenimiento, el crecimiento en la venta de juguetes sexuales inteligentes nos debería hacer pensar en lo que aumentó la superficie de ataque y lo complejo que cada vez más se volverá asegurar la vida digital de los usuarios con las distintas posibilidades que tienen los cibercriminales de realizar un ataque.

En este sentido, las especialistas Denise Giusto y Cecilia Pastorino, respaldadas por una investigación que realizaron y en la que descubrieron varias vulnerabilidades en dispositivos sexuales inteligentes, muestran con otro ejemplo lo importante que se ha convertido hoy en día —y sobre todo de cara al futuro— pensar en la seguridad de manera proactiva. Estos dispositivos procesan grandes cantidades de información sensible de los usuarios y forman parte de una industria de juguetes sexuales inteligentes que está en crecimiento y que avanza con modelos que incluyen tecnología de realidad aumentada e inteligencia artificial. Por ende, trabajar en concientizar acerca del valor y la importancia que tiene la seguridad es una necesidad de ayer pero que hoy se vuelve más evidente que nunca.

Una vez que termine la pandemia muchas organizaciones habrán corroborado que con el trabajo remoto la productividad no se ve afectada o que incluso mejora. Lo mismo tal vez ocurra en sectores como la educación, o el de la salud con las consultas médicas virtuales, por nombrar algunos. Como decíamos al inicio, algunos cambios probablemente llegaron para quedarse y con ellos están planteados los desafíos post pandemia desde el punto de vista de la seguridad.

Esperamos que el presente documento sirva para poder comprender algunos de los cambios ocurridos y que posibilite ver cuáles son los pasos a seguir para lo que se viene.



CYBERSECURITY
EXPERTS ON YOUR SIDE