Ciberdelincuencia y ciberseguridad en un mundo pos-COVID-19

julio 29, 2020
by Yotam Gutman

La primera mitad de 2020 llegó y pasó. Estoy convencido de que nadie en el ámbito de la ciberseguridad podía prever que un nuevo virus pondría el mundo patas arriba, cerrando países enteros, interrumpiendo todo el tráfico aéreo y obligando incluso a las empresas más grandes a enviar a sus empleados a teletrabajar desde casa.

Visto lo cual, es tarea ardua intentar predecir lo que nos espera en el segundo semestre. Sin embargo, hemos aprendido tanto en los últimos seis meses, que probablemente podamos plantear algunas hipótesis creíbles.

¿Solos en casa o en compañía de ciberdelincuentes?

Empecemos por los usuarios (o víctimas). La pandemia de COVID-19 ha enviado a millones de personas a casa; algunos de manera definitiva (han sido despedidos) y otros para teletrabajar. Esta transformación casi inmediata parece que perdurará. Efectivamente, algunas de las mayores empresas del mundo (Twitter, Facebook, Shopify, Zillow) ya han declarado que el teletrabajo será una opción viable para los empleados que lo prefieran.

Además, afecta incluso a los mercados más tradicionales. Fujitsu Ltd., uno de los mayores empleadores de Japón, va a reducir la superficie de oficinas en un 50 % en el curso de los próximos tres años, animando a sus 80 000 empleados a trabajar principalmente desde casa. Actualmente, el 42 % de los trabajadores estadounidenses están teletrabajando y, según algunas encuestas, incluso una vez superada la pandemia cuando reabran las oficinas, las empresas permitirán a algunos (cuando no a todos) sus empleados seguir trabajando de forma remota.

Con millones de personas teletrabajando, la superficie de ataque susceptible de ser aprovechada por los ciberdelincuentes es enorme. Proporcionar los mismos niveles de seguridad a todos estos empleados que trabajan fuera del perímetro (relativamente) seguro de sus oficinas y de la intranet local no es tarea sencilla. Además, con el tiempo y las numerosas «tentaciones» que ofrece la tecnología (como dejar a nuestros hijos utilizar nuestros ordenadores portátiles profesionales para navegar por Internet), el nivel de concienciación puede verse erosionado, aumentado la vulnerabilidad a la ciberdelincuencia.

> *Predicción:* El teletrabajo seguirá siendo un desafío de seguridad para las empresas, a menos que inviertan en la mejora y el mantenimiento de los niveles de seguridad de los empleados, con independencia de su lugar de trabajo.

Oportunidades que ofrece la pandemia a los ciberdelincuentes

Durante la pandemia de COVID-19, la ciberdelincuencia se ha disparado. El FBI Internet Crime Complain Center (IC3) ha comunicado un aumento del 300 % en las quejas asociadas a la ciberdelincuencia.

El tráfico hacia sitios web dedicados a la piratería, y las búsquedas de información y tutoriales sobre este tema se incrementaron drásticamente entre los meses de marzo y mayo, lo que indica que un buen número de aspirantes a hacker se están planteando una nueva orientación profesional. Muchas actividades ciberdelictivas de los últimos meses están relacionadas con el virus. Concretamente, la Telco Security Alliance comunicó un incremento del 2000 % de ciberamenazas asociadas a la COVID-19 solo en el mes de marzo.

Si bien el volumen general de actividades ciberdelictivas va en aumento, a determinados segmentos les va mejor que a otros. Por ejemplo, la demanda de tarjetas de crédito robadas ha descendido durante la pandemia, mientras que los timos «clásicos» (publicidad de medicamentos y equipos médicos falsos o inapropiados, oportunidades de inversión dudosas, etc.) están en pleno apogeo. En lo que respecta al mundo de la empresa, parece que los ciberdelincuentes se han vuelto más audaces. Recurren a técnicas más agresivas y demuestran un deseo de monetización rápida, en lugar de beneficios a largo plazo.

> *Predicción*: La ciberdelincuencia va a seguir aumentando. Los ciberdelincuentes dirigirán cada vez más sus ataques a empresas y organizaciones con malware más agresivo y ransomware personalizado diseñado tanto para robar datos como para paralizar las actividades. Tácticas como la extorsión bajo la amenaza de divulgar la información robada o la subasta de datos robados van a generalizarse como medio de ganar dinero rápidamente.

Ciberpolicía: aumento de efectivos

Las autoridades son conscientes de esta situación y trabajan para neutralizar esas amenazas, empezando por aumentar la cooperación entre los países, como es el caso de la alianza Partnership Against Cybercrime del Foro Económico Mundial. Lanzada en abril de 2020, esta iniciativa tiene por objetivo explorar las formas de mejorar la colaboración entre los sectores público y privado, así como luchar contra la ciberdelincuencia mundial. También se espera que se refuerce la cooperación entre las fuerzas de seguridad nacionales y ya se han observado resultados positivos, como el desmantelamiento de EncroChat (una red telefónica cifrada muy popular entre los ciberdelincuentes, desmantelada gracias a la colaboración entre las autoridades policiales y judiciales francesas y holandesas, Europol y Eurojust).

Entre tanto, las autoridades adoptan medidas concretas para facilitar la denuncia de los ciberdelitos. Por ejemplo, el National Cyber Security Center del Reino Unido ha creado una dirección de correo electrónico para denunciar los timos online, y ha recibido la asombrosa cantidad de un millón de quejas en menos de 2 meses.

Asimismo, el estado de Michigan ha inaugurado una línea telefónica exclusiva para que los ciudadanos reciban asistencia y consejos gratuitos sobre ciberdelincuencia, 24 horas al día. El Reino Unido también está recurriendo a medios más proactivos, como lanzar una campaña publicitaria online diseñada para llegar a los jóvenes que buscan servicios de ciberdelincuencia y ofrecerles alternativas legítimas.

> *Predicción*: Aumentará la colaboración entre las agencias nacionales e internacionales de lucha contra la ciberdelicuencia, así como su eficacia, lo que permitirá llevar ante los tribunales a un mayor número de ciberdelincuentes.

Hacktivismo: un juego peligroso

Aunque sus motivaciones no sean económicas, estos ciberactivistas ofensivos han dado mucho que hablar en los últimos tiempos. La agitación social reciente en EE. UU. ha desatado una oleada de ataques de hacktivistas, concretamente de tipo DDoS contra ayuntamientos y comisarías de policía. Este año, hemos observado la filtración de millones de documentos de la policía y el FBI, así como agresivos ataques a través de redes sociales contra la administración estadounidense, el presidente Trump e incluso la aplicación Tiktok.

Estas actividades, que no ponen directamente en peligro ni a empresas ni a personas, pueden dirigirse contra individuos y organizaciones que se consideran contrarios a los principios del colectivo de hackers.

> *Predicción:* Las acciones de los hacktivistas están estrechamente relacionadas con acontecimientos de actualidad y agitación social. Lo que ocurra próximamente dependerá en gran medida de la situación en Estados Unidos y de las elecciones de 2020. Una nación en guerra contra sí misma sin duda propiciará un aumento de la actividad de los hacktivistas.

Conclusión

Los seis últimos meses han sido realmente inauditos. Aunque todavía es demasiado pronto para evaluar las consecuencias que la COVID-19 va a tener en nuestro modo de vida a largo plazo, es muy probable que este período provoque el mayor cambio sufrido por el mundo laboral desde la invención de la oficina moderna y, como tal, ha incrementado extraordinariamente la vulnerabilidad de las empresas y usuarios ante las ciberactividades.

Sin embargo, no todo son malas noticias; las agencias de orden público empiezan a ser conscientes de la envergadura del problema, están mejorando su cooperación, y las empresas deben saber que la situación se les escapa de control. Gestione su riesgo, despliegue una solución de inteligencia artificial basada en el comportamiento capaz de prevenir, detectar y reparar los daños causados por las amenazas conocidas y desconocidas, y obligue a los ciberdelincuentes a buscar una presa fácil en otro sitio. Si desea descubrir cómo puede ayudarle SentinelOne a proteger su empresa, con independencia de si su personal trabaja en casa o en la oficina, póngase en contacto con nosotros hoy mismo o solicite una demostración gratuita.

¿Te gusta este artículo? Síguenos en LinkedIn, Twitter, YouTube or Facebook para ver el contenido que publicamos.

Lee acerca de Ciberseguridad

- Inteligencia artificial basada en el comportamiento: posibilidades ilimitadas a la hora de proteger a las empresas
- 10 maneras de proteger su Active Directory