Ransomware en tiempos del Coronavirus

Durante los últimos meses, tanto en Chile como en el resto del mundo, la transformación digital tuvo una importante aceleración por la crisis sanitaria a causa del Covid-19. Esto, junto al constante y masivo uso de las tecnologías de la información y al desarrollo creciente de la economía digital, pone a los países del mundo en una situación de alerta para unificar esfuerzos y mejorar los estándares de ciberseguridad. Por eso es que, en medio del panorama actual, los ciberataques se han transformado en "la otra pandemia", pues de forma silenciosa son capaces de vulnerar todo tipo de organizaciones e información confidencial, dejando tras de sí una serie de repercusiones económicas y de daño reputacional.

En particular, el tipo de ataque que ha tenido el aumento más significativo en este último año han sido los de Ransomware. Este es un programa de software malicioso que infecta dispositivos de procesamiento de datos (computadores, servidores o teléfonos móviles), bloquea su funcionamiento y exige el pago de dinero para restablecer el sistema. Este tipo de malware es un sistema criminal para ganar dinero que se puede instalar a través de enlaces engañosos incluidos en un mensaje de correo electrónico, mensaje instantáneo o sitio web. El Ransomware tiene la capacidad de bloquear sin permitir acceso a ninguna funcionalidad y cifrar archivos importantes predeterminados con una contraseña.

Siempre se menciona que el punto débil en todos los ataques son las personas y esto es efectivo. La mayoría de los ataques comienzan con mensajes de phishing, que ni siquiera contienen malware, pero inducen a los usuarios a hacer click en links, archivos o sitios web de dudosa reputación que, posteriormente, descargan el software malicioso en su objetivo. Estos mensajes son cada vez más sofisticados y dirigidos. A través de ingeniería social, los atacantes obtienen información personal de la víctima y crean mensajes que parecen reales, de acuerdo a su situación personal.

Durante 2020 los ataques de Ransomware han aumentado de forma exponencial a nivel global, afectando a todo tipo de geografías y organizaciones. Según estadísticas de CheckPoint, compañía líder mundial en el desarrollo de sistemas de protección ciberseguridad, durante Q3 de 2020, este tipo de ataques ha tenido un 50% de aumento en la cantidad de ataques diarios, en comparación con los observados durante la primera mitad del año. Estadísticamente, este tipo de crímenes cobra una nueva víctima cada 10 segundos a nivel global.

Con el aumento de las intrusiones de Ransomware también han aparecido nuevas técnicas, como la doble extorsión. A partir del primer trimestre de 2020, estas amenazas han agregado una etapa adicional a sus ataques. Antes de encriptar los datos en el computador atacado, los cibercriminales extraen volúmenes importantes de información sensitiva de la organización y amenazan a sus víctimas con divulgarla públicamente a no ser que sus demandas de pago sean satisfechas.

En los últimos meses, varias empresas de la región han sido afectadas por estos ataques. Un ejemplo es el Ransomware denominado Sodinokibi. Este malware, que afectó a varias compañías en Brasil y Chile, actúa aprovechándose de una vulnerabilidad de un servidor de aplicaciones de

mercado. Una vez explotada, realiza escalamiento de privilegios de Windows y procede a encriptar los archivos para pedir un posterior rescate.

Según el CSIRT del Ministerio del interior, Sodinokibi utiliza como métodos de propagación campañas de phishing que contengan archivos adjuntos maliciosos, tratando de engañar a los usuarios para que los abran. Estos suelen ser documentos Microsoft Office, archivos como ZIP, RAR, JavaScript, ficheros PDF, ejecutables, entre otros. Una vez abiertos, descargan malware tipo troyano para propagarse por la red atacada y generar infecciones en cadena.

Las principales recomendaciones que podemos entregar para que las organizaciones no sean afectadas por este tipo de ciberataques se pueden agrupar en dos:

1.- Buenas prácticas:

- Educación. La mayor parte de los ataques de Ransomware utilizan el phishing y la ingeniería social como mecanismo de descarga del software malicioso. Es por esto que, la mejor forma de evitar este tipo de ataques es con la educación y concientización de los usuarios.
- Respaldos. La realidad es que, a pesar de todos los esfuerzos que las empresas realizan, existen grandes posibilidades que alguno de estos ataques sea finalmente exitoso. Por lo tanto, es fundamental que las organizaciones tengan sus sistemas de respaldo de datos funcionando correctamente. Esto les permitirá recuperarse de un ataque, sin necesidad de pagar un rescate de los datos.
- Gestión de Vulnerabilidad y Parchado de Sistemas. Los ataques de Ransomware se aprovechan de las últimas vulnerabilidades encontradas en los sistemas y aplicaciones de mayor uso a nivel global, por lo que es fundamental que las compañías cuenten con programas constantes de revisión y gestión de vulnerabilidades, que tomen en cuenta el riesgo potencial de que esta sea explotada en un ataque. Manteniendo los sistemas y aplicativos claves siempre parchados, se cierra la principal puerta de acceso a los cibercriminales.

2.- Recomendación de ciberseguridad:

- Protección de End Point. Un tradicional antivirus es el punto de partida de los mecanismos de protección contra ataques conocidos. Hoy se sugiere agregar a los tradicionales antivirus componentes adicionales de protección denominados EDR (End Point Detection and Response) que permiten detectar y bloquear ataques de día cero y comportamientos sospechosos clásicos del Ransomware, que los tradicionales antivirus no necesariamente detectan.

- Protección de Red. Tecnologías avanzadas de protección de red, como los IPS, Antivirus de Red y Antibot, son componentes tecnológicos que las empresas deben agregar a sus tradicionales protecciones de red, para bloquear ataques de Ransomware. Las tecnologías más avanzadas de Sand Boxing permiten hoy analizar malwares conocidos o desconocidos, ejecutarlos en tiempo real, buscando código malicioso y, finalmente, si es necesario bloquear el ataque, previniendo de esta forma que los end-points sean afectados y el ataque se expanda por la organización. Esto adquiere vital importancia por la capacidad de

detectar ataques de “día cero”, que no son conocidos y que herramientas tradicionales de detección no pueden identificar.

Hoy en día vivimos una nueva realidad producto de la pandemia global y hemos tenido que adaptarnos a ella. Esta se encuentra transformando nuestros hábitos, forma de relacionarnos y forma de trabajar. Los ciberdelincuentes saben de esto y también están adaptando sus estrategias para atacar a las organizaciones y aumentar sus ingresos con sus ataques. Como personas y como organizaciones debemos adaptarnos y prepararnos para estas nuevas amenazas. Chile no es diferente al resto del mundo, pero siempre existen características especiales que nos diferencian de lo que sucede en otros países. Como en todos los problemas que enfrentamos, la solución no es única, es una combinación de temas humanos, tecnológicos y de procesos. Lo fundamental es estar siempre alertas y preparados. Preparados no sólo previniendo, sino que además preparados para saber cómo reaccionar y reponernos de forma rápida, efectiva y con el menor daño posible. Porque lo que es seguro es que en algún momento seremos víctimas de un ciberataque.

Miguel Pérez
Director Alianza Chilena de Ciberseguridad
Gerente General de NovaRed