SEGURIDAD INFORMÁTICA

**Las telecomunicaciones son utilizadas como principal vía de ataque cibernético**

*La disponibilidad y velocidad de las redes son un factor para crear campañas maliciosas más potentes y con mayor alcance.*

**Por Julián M. Zappia.  
Diplomatic Week.**

El sector de telecomunicaciones es una de las industrias de mayor crecimiento pese a los embates macroeconómicos y a la crisis de salud pública, convirtiéndose en un mercado de gran interés para la ciberdelincuencia.

Los atacantes no solo se limitan a comprometer la disponibilidad y/o acceso a la información del proveedor de servicio, sino también puede dirigir un ataque a un cliente o socio de negocio usando la infraestructura del carrier.

Durante 2022 más de siete de cada 10 empresas de telecomunicaciones sufrieron hasta seis ataques de ciberseguridad en sus redes 5G, incluyendo empresas de Latinoamérica, de acuerdo con el estudio Encuesta de seguridad gestionada 5G 2022, realizado por la consultora GlobalData.

También detalla que uno de cada tres proveedores de servicios tuvo ocho o más incidentes que vulneraron su seguridad cibernética durante los últimos 12 meses.

**Opinión experta.**

Oswaldo Palacios, Senior Account Executive para Akamai, mencionó que el crecimiento de ciberataques al sector de telecomunicaciones ha sido impulsado de manera significativa por las redes 4G y 5G.

“La disponibilidad y velocidad de las redes son un factor para crear campañas maliciosas más potentes y con mayor alcance, con lo cual se deben “patrullar” los tráficos en los carriers para evitar que su infraestructura sea usada con fines delictivos, y cuyas consecuencias podrían derivar en pérdidas financieras, caída de servicios y sistemas, e impacto en la calidad de los servicios”, destacó el directivo.

“Uno de los principales retos para los carriers es tener una alta disponibilidad y velocidad de servicio, esto es aprovechado por los ciberdelincuentes para llegar a más víctimas potenciales. De tal forma que el carrier además de ser atacado por su información valiosa y poca tolerancia a fallos, también es usado como vía de ataque. Lo anterior supone una doble labor por parte de los responsables de ciberseguridad ya que además de blindar su infraestructura y sistemas informáticos, deben asegurarse de que ésta no sea usada por los atacantes para llegar a más usuarios finales y culminar su labor”, agregó.

De acuerdo a los dichos de Oswaldo Palacios, los principales ataques dirigidos al sector de telecomunicaciones son: ataques de denegación de servicio o DDoS, ransomware, malware en IoT, phishing y ataques dirigidos.

Sin duda alguna, el ransomware ocupa el primer lugar en ciberataques por la forma en la que se distribuye y activa, sigue usando al factor humano como principal ruta de instalación y ataque.

El experto de Akamai destacó que un proveedor de servicio de telecomunicaciones debe tomar cuidados especiales al momento de proteger los activos informáticos, ya que pueden ser víctimas y/o afectar a terceros en un amplio grado de alcance.

Dependiendo de la estructura y organización del carrier pueden tener afectaciones internas, es decir que los atacantes se limiten solo a comprometer la disponibilidad y/o acceso a la información del carrier.

Otro escenario es que se dirija un ataque a un cliente o socio de negocio usando la infraestructura del Carrier; de cualquier modo estos ataques implican el nombre y prestigio de la compañía comprometida.

A fin de contrarrestar los ciberataques hacia las redes avanzadas de telecomunicaciones, Oswaldo Palacios recomendó “microsegmentar” los centros de datos de los carriers, ya que es el siguiente paso en una estrategia de ciberseguridad debido a que otorga una visibilidad a nivel de proceso de comunicación que no se logra con herramientas tradicionales de ciberseguridad.

“Debemos tener especial cuidado en elegir una herramienta de Microsegmentación, ésta debe ser capaz de cubrir entornos On-Premise, nubes públicas y privadas, contenedores, IoT, etcétera. Una vez que tenemos esa visibilidad podemos tomar decisiones informadas y microsegmentar nuestras aplicaciones o entornos críticos, de tal forma que si alguno de ellos se ve comprometido, no afecte la operación y seamos capaces de reconocer una amenaza en una etapa temprana, recordemos que no podemos proteger lo que no podemos ver o saber que existe”, finalizó el experto de Akamai.

**Otros análisis.**

Proyecciones más recientes de la consultora Omdia indican que las conexiones 5G globales continuarán su aceleración en 2023 para acercarse a los 2.000 millones y alcanzar los 5.900 millones al término de 2027.

Se prevé que 4G LTE continúe fuerte en América Latina y el Caribe hasta finales de 2023. En el último trimestre de 2022, había 537 millones de conexiones LTE de 4G, lo que representó un crecimiento anual del 9,3% con la suma de 46 millones de suscripciones nuevas a LTE.

América Latina y el Caribe registraron 12 millones de conexiones 5G al término de 2022 y se estima que alcancen 400 millones en 2027.

Uno de los ciberataques más sonados al sector de telecomunicaciones en América Latina fue realizado en contra de Telecom Argentina en 2020, el cual pudo haber afectado a más de 18.000 equipos.

El ataque se llevó a cabo bajo el uso de ransomware en el que los cibercriminales restringieron el acceso a empleados a sus cuentas de Office 365 y OneDrive, estos hackers pidieron 7.5 millones de dólares en la criptomoneda Monero (XMR) a la empresa para desbloquear los archivos encriptados. El ataque se habría efectuado a través del ransomware “REv”.

De acuerdo con datos de TeleGeography y 5G Americas, en total, la cantidad de redes 5G comerciales del mundo alcanzó las 259.

Se prevé que esa cifra llegue a 390 al término de 2023 y a 403 a finales de 2025, lo que representa un fuerte crecimiento de la inversión en redes 5G en muchas regiones del mundo.

Hasta el pasado mes de marzo, América Latina y Caribe había registrado 28 redes 5G comerciales y 128 redes 4G LTE.

Pie de foto 3

ARSAT reforzó sus acciones de ciberseguridad, tanto preventivas como proactivas.