Publicado en Madrid el 20/05/2020

# [Global Threat Intelligence Report de NTT Ltd.: la cantidad de ataques aumentan a medida que los ciberdelincuentes innovan más rápido y automatizan los ataques](http://www.notasdeprensa.es)

## Cibercriminales que utilizan la pandemia COVID-19 para lanzar ataques contra organizaciones vulnerables
Las tecnológicas encabezan la lista de las industrias más atacadas por primera vez para desbancar a las financieras

 NTT Ltd., proveedor mundial líder de servicios de tecnología global, lanza hoy su informe Global Threat Intelligence Report 2020 (GTIR), que revela que a pesar de los esfuerzos de las organizaciones para colocar sus ciberdefensas, los ciberdelincuentes continúan innovando más rápido que nunca y automatizando sus ataques. Haciendo referencia a la actual pandemia de COVID-19, el informe destaca los desafíos que enfrentan las empresas a medida que los delincuentes cibernéticos buscan obtener beneficios de la crisis global y la importancia que tiene la seguridad por diseño y la resiliencia cibernética. Los datos de ataque indican que más de la mitad (55%) de todos los ataques en 2019 fueron una combinación de ataques de aplicaciones web y ataques específicos de aplicaciones, en comparación con el 32% del año anterior, mientras que el 20% de los ataques se dirigieron a suites de CMS y más del 28% a tecnologías específicas que soportan sitios web. Para las organizaciones que dependen más de su presencia en la web durante COVID-19, como portales de clientes, sitios minoristas y aplicaciones web compatibles, corren el riesgo de exponerse a través de sistemas y aplicaciones que los ciberdelincuentes ya están atacando constantemente. Matthew Gyde, Presidente y CEO de la división de Seguridad, NTT Ltd., dice: “La actual crisis global nos ha demostrado que los ciberdelincuentes siempre se aprovecharán de cualquier situación y las organizaciones deben estar listas para cualquier cosa. Ya estamos viendo un mayor número de ataques de ransomware en organizaciones de atención médica y creemos que esta situación vaya a peor. Ahora más que nunca, es fundamental prestar atención a la seguridad que protege a su negocio; asegurarse que es ciber-resiliente y maximizar la efectividad de las iniciativas de seguridad por diseño". Sectores objetivos: las tecnológicas encabezan la lista más atacadaSi bien el volumen de ataques aumentó en todos los sectores durante el año pasado, los sectores público y tecnológico fueron los más atacados a nivel mundial. Las tecnológicas se convirtieron en el sector más atacado por primera vez, representando el 25% de todos los ataques (frente al 17%). Más de la mitad de los ataques dirigidos a este sector fueron ataques específicos de aplicación (31%) y DoS / DDoS (25%), así como un aumento de los ataques de IoT. El gobierno estaba en la segunda posición, impulsado en gran medida por la actividad geopolítica que representaba el 16% de la actividad de amenaza, y las finanzas eran terceros con el 15% de toda la actividad. Los servicios empresariales y profesionales (12%) y la educación (9%) completaron los cinco primeros. Mark Thomas, que dirige el Centro de Inteligencia de Amenazas Globales de NTT Ltd., comenta: “El sector de la tecnología experimentó un aumento del 70% en el volumen total de ataques. El aumento de los ataques de IoT también contribuyó a este aumento y, si bien ninguna actividad dominada por un único botnet, vimos volúmenes significativos de actividad tanto de Mirai como de IoTroop. Los ataques a organizaciones gubernamentales casi se duplicaron, incluidos los grandes saltos tanto en la actividad de reconocimiento como en los ataques específicos de aplicaciones, impulsados ​​por actores de amenazas que aprovechan el aumento de los servicios locales y regionales en línea que se dan a los ciudadanos ". Resultados clave de 2020 GTIR: - Sitios web que se hacen pasar por la fuente "oficial" de información COVID-19, pero que alojan kits de explotación y / o malware, creados a una velocidad increíble, que a veces supera los 2000 sitios nuevos por día. - Los tipos de ataque más comunes representaron el 88% de todos los ataques: ataques de aplicaciones específicas (33%), aplicaciones web (22%), reconocimiento (14%), DoS / DDoS (14%) y manipulación de red (5%). - Los atacantes están innovando: al aprovechar la inteligencia artificial y el aprendizaje automático e invertir en automatización. Alrededor del 21% del malware detectado tenía la forma de un escáner de vulnerabilidades, que respalda la premisa de que la automatización es un punto clave de los atacantes. - Armamento de IoT: Botnets como Mirai, IoTroop y Echobot han avanzado en automatización, mejorando las capacidades de propagación. Mirai e IoTroop también son conocidos por propagarse a través de los ataques de IoT, luego se propagan a través del escaneo y la posterior infección de los hosts identificados. - Las vulnerabilidades antiguas siguen siendo un objetivo activo: los atacantes aprovecharon las que tienen varios años, pero que no han sido actualizadas por las organizaciones, como HeartBleed, lo que ayudó a hacer de OpenSSL el segundo software más atacado con el 19% de los ataques a nivel mundial. Se identificaron un total de 258 nuevas vulnerabilidades en los entornos y software de Apache en los últimos dos años, lo que hace que Apache sea el tercero más atacado en 2019, lo que representa más del 15% de todos los ataques observados. - Los ataques a los sistemas de gestión de contenido (CMS) representaron aproximadamente el 20% de todos los ataques: dirigidos a plataformas CMS populares como WordPress, Joomla!, Drupal y noneCMS, los ciberdelincuentes los utilizaron como una ruta hacia las empresas para robar datos valiosos y lanzar ataques adicionales. Además, más del 28% de las tecnologías objetivo (como ColdFusion y Apache Struts) que soportan sitios web. El 2020 GTIR también denomina el año pasado como el "año de aplicación" ya que el número de iniciativas de Gobernanza, Riesgo y Cumplimiento (GRC) continúa creciendo, creando un panorama regulatorio global más desafiante. Varias leyes ahora influyen en cómo las organizaciones gestionan los datos y la privacidad, incluido el Reglamento General de Protección de Datos (GDPR), que ha establecido un alto estándar para el resto del mundo, y la Ley de Privacidad del Consumidor de California (CCPA) que entró en vigor recientemente. El informe continúa proporcionando varias recomendaciones para ayudar a entender la complejidad del cumplimiento, incluida la identificación de niveles de riesgo aceptables, la creación de capacidades de ciber-resistencia y la implementación de soluciones seguras por diseño en los objetivos de una organización. Para obtener más información sobre cómo GTIR ofrece a las organizaciones un marco sólido para abordar el panorama actual de amenazas cibernéticas, y para obtener más información sobre las tendencias emergentes en diferentes sectores y regiones, incluidas América, APAC y EMEA, siga el enlace para descargar GTIR 2020.

**Datos de contacto:**

Juan Maldonado

+34619743694

Nota de prensa publicada en: [https://www.notasdeprensa.es/global-threat-intelligence-report-de-ntt-ltd](http://www.notasdeprensa.es/educalivecom-disfruta-de-cursos-presenciales-y-clases-particulares-a-traves-de-internet)

Categorias: Telecomunicaciones E-Commerce Ciberseguridad Recursos humanos Innovación Tecnológica



[**http://www.notasdeprensa.es**](http://www.notasdeprensa.es)