Vendrán más ciberataques de Estado

En 2020, el mundo tendrá que prepararse para una nueva Guerra Fría de TI. Esto es lo que revela Check Point en sus pronósticos sobre ciberataques para 2020.

Según la compañía de seguridad cibernética, **la nueva "guerra" ciberfría se intensificará y tendrá lugar en línea**, mientras que las potencias occidentales y orientales compartirán cada vez más sus tecnologías e inteligencia.

La guerra comercial en curso entre Estados Unidos y China, y la brecha creciente entre las dos súper economías, es un claro indicador de esta tendencia. **Los ataques cibernéticos se utilizarán cada vez más como guerras indirectas**, tal como sucede en el caso de conflictos entre países menores, pero en realidad financiados y permitidos por grandes naciones "protectoras" que buscan fortalecer y extender sus esferas de influencia, como se ha observado en operaciones recientes de TI contra Irán, tras los ataques a estructuras petroleras en Arabia Saudita.

También el próximo **aumentará la difusión de noticias falsas basadas en inteligencia artificial**, Check Point señala que, desde las elecciones estadunidenses de 2016, los opositores políticos han progresado enormemente al crear equipos ad hoc que crean y difunden historias ficticias para socavar el apoyo a los oponentes. Por esta razón, los candidatos estadunidenses esperan que los movimientos políticos en el extranjero ya estén implementando estrategias para influir en las elecciones de 2020.

Servicios públicos

Según los analistas de Check Point, los ataques cibernéticos a servicios públicos esenciales e infraestructuras estratégicas continuarán creciendo. No es sorprendente, como se ha visto este año por **ataques a compañías de servicios públicos de Estados Unidos y Sudáfrica, los servicios esenciales continúan sujetos a ataques cibernéticos.**

En muchos casos, las infraestructuras que han demostrado ser las más sensibles son las de distribución de energía y agua, dado que utilizan una tecnología más atrasada que ha resultado vulnerable a amenazas remotas, porque la actualización podría haber causado la interrupción de los servicios. Los Estados deberán tratar de fortalecer en gran medida las protecciones de TI para su infraestructura.

Con respecto a la seguridad informática en 2020, los pronósticos técnicos de Check Point dicen que los ataques de ransomware dirigidos están en aumento: en 2019, este malware se dirigió cada vez más a empresas específicas, administraciones locales y organizaciones de atención médica.

Los piratas informáticos dedican mucho tiempo a recopilar información personal sobre sus víctimas para garantizar que el daño sea visible y que los rescates sean, en consecuencia, mucho mayores.

Los ataques se han vuelto tan impactantes que el FBI ha suavizado su posición sobre el pago de rescates: ahora reconoce que, en algunos casos, l**as empresas necesitan examinar todas las soluciones posibles para proteger a sus accionistas, empleados y clientes.** Esto conducirá en el

futuro a un aumento en las organizaciones que suscriben pólizas de seguro contra ransomware, lo que a su vez generará más solicitudes de redención por parte de los atacantes.

Los **ataques de phishing van más allá del correo electrónico**, pues si bien sigue siendo el principal vector de ataque, los ciberdelincuentes también recurren a una variedad de otros canales de ataque para inducir a las víctimas a vender información personal, credenciales de inicio de sesión o incluso enviar dinero.

El **phishing implica cada vez más ataques a través de SMS** en teléfonos móviles o el uso de mensajes directos en las redes sociales y plataformas de juegos.

Los ataques de malware en dispositivos móviles se han intensificado: en la primera mitad de 2019 hubo un aumento de 50% en los ataques de malware en la banca móvil en comparación con 2018.

El **código malicioso puede robar datos de pago, credenciales y fondos de las cuentas bancarias de las víctimas**, hay nuevas variantes disponibles que pueden ser ampliamente distribuidas por cualquiera que esté dispuesto a financiar desarrolladores de malware. Los ataques de phishing también se volverán más complejos y efectivos, tratando de convencer a los usuarios móviles de que hagan clic en enlaces web maliciosos.