CIBERDELITO Y EL INCREMENTO ALARMANTE DEL *MALWARE*

César Pallavicini
CEO de Pallavicini Consultores y presidente Comunidad Riesgo Operacional

A principios de 2019, los analistas hicieron predicciones respecto al aumento de ciberataques y mencionaron que las vulnerabilidades producto de malware crecerían exponencialmente. Lamentablemente, así fue, ya que el negocio de la ciberdelincuencia es y será más rentable que el tráfico y venta de drogas.

En el primer semestre de 2019, según "Threat Landscape Report", de S21Sec, se detectó un incremento en el malware bancario para dispositivos móviles, respecto al del 2018. Y se destacan dos "bankers" dirigidos a dispositivos Android:

Asacub: se trata de un banker ruso que llegó a infectar a 13 mil usuarios diarios. El vector de infección es mediante un botnet de móviles infectados que envía enlaces maliciosos a los contactos del dispositivo.

Svpeng: en este caso se realiza la infección publicando anuncios en Google Adsence. Una vez que se visita la página del banner, el malware se descarga sin conocimiento del usuario en la tarjeta SD (de memoria) del dispositivo. Su funcionalidad principal es el robo de credenciales bancarias mediante técnicas de phishing y el control de SMS. Recopila, además, otra información sensible como historial de llamadas de navegador y datos de contacto.

El malware Tritón, conocido desde su ataque a una planta petroquímica de Arabia Saudita, en 2017, tenía como objetivo la caída de los servicios

Ataque a infraestructuras críticas

El poder del malware tiene su más agresiva faceta cuando apunta a las infraestructuras críticas, potenciales objetivos de grupos de atacantes con motivaciones como el espionaje o, incluso, el daño físico, tanto a las estructuras tecnológicas como a las industrias.

Muchos de estos grupos son financiados por gobiernos que tienen intereses más allá de lo económico, coordinando ataques a infraestructura crítica de compañías eléctricas o de gas y transporte, por citar algunos ejemplos. Lo más grave es que estos ataques no sólo representan un riesgo para las empresas atacadas, sino un impacto directo en la sociedad.

Un caso: el malware Tritón (creado por el grupo de hackers Xenotime) es conocido desde su ataque a una planta petroquímica de Arabia Saudita, en 2017. Su objetivo no era el ciberespionaje, sino la caída de los servicios de las infraestructuras críticas.

Adicionalmente, el ransomware Lockergoga ha afectado a empresas relacionadas a la producción de aluminio y de energías renovables, mediante un proceso de infección que se inicia cuando un archivo malicioso, proveniente de un correo electrónico, se ejecuta. Este caso evidencia la importancia de contar con una educación preventiva para los usuarios, con el objetivo de evitar la en apariencia inofensiva acción de abrir un correo electrónico. Para eso, se recomienda hacer ethical phishing (educativo) para disminuir el riesgo de que más usuarios ignorantes caigan en la trampa.

Con todo, mientras las empresas avanzan en la llamada transformación digital e implementan nuevas tecnologías, las organizaciones criminales invierten grandes sumas de dinero para seguir adelante en su negocio, que es muy rentable y lucrativo. Poseen un modelo de trabajo 24 por 7. Atacan a organizaciones de todo tipo, aprovechando la falta de educación que existe entre los usuarios y la falta de conciencia de directivos que postergan presupuestos para invertir en la gestión de riesgo operacional, que por cierto incluye la gestión integral de la seguridad de la información y la ciberseguridad.

Finalmente, es urgente insistir en que la capacitación de profesionales de las áreas TIC, auditorias y de riesgos, son fundamentales para avanzar, en especial cuando las predicciones indican que los riesgos a los que se exponen las empresas podrían aumentar producto de la falta de profesionales y certificaciones en gestión de riesgos y seguridad de la información.