cuentes imitarán la forma de autenticación de un sitio web legítimo como Microsoft365 o Google Drive mediante páginas fraudulentas con la finalidad de robar las credenciales enviadas por los usuarios. Asimismo, las VPN y RDP estarán en el punto de mira, aumentando el número de ciberataques hacia estas tecnologías, haciendo uso de *exploits*, ataques de fuerza bruta y uso de credenciales robadas. La sociedad en general seguirá luchando contra la pandemia, situación que será aprovechada por los grupos de ciberdelincuentes para programar ataques automatizados de spear *phishing* y de ingeniería social. Además, nos encontraremos con *ransomware* con técnicas cada vez más sofisticadas".

ICA SISTEMAS Y SEGURIDAD

Jesús Castellanos
Service Design & Compliance Cybersecurity Manager

"El apogeo por el uso del comercio-e y adopción de servicios en la nube por parte de sectores minoristas provocan el aumento de la superficie de ataque, motivado por los despliegues apresurados y la falta de cultura de ciberseguridad de la pyme, acuciados más por la viabilidad del negocio a corto plazo que por la de su seguridad. Los actores de amenazas aprovecharán el aprendizaje automático para acelerar ataques a sistemas y redes, los motores de *Machine Learning* se van a entrenar con datos de ataques exitosos para la detección de patrones de defensa e identificar más rápidamente vulnerabilidades, permitiendo a los delincuentes centrarse en vectores de ataque más eficientes, rápidos y sigilosos. Tampoco perdamos de vista a que las organizaciones emplean con más frecuencia ML en sus negocios. Ataques para secuestro previo y el posterior envenenamiento de datos, provocan pérdida de integridad en el negocio y pueden suponer un método de *ransomware* avanzado para la solicitud de rescates.

Los teletrabajadores, que operan más relajados en relación con las exigencias de los entornos profesionales, van a suponer un vector de ataque ampliamente usado por los ciberdelincuentes, que ya están intensificando ataques de ingeniería social y *ransomware* en combinación con IA para engañar al trabajador. La utilización de dispositivos personales y redes domésticas, junto al apogeo de uso de dispositivos inteligentes, habitualmente carentes de mecanismos de seguridad, y la expansión de la tecnología 5G, supone un contexto muy atractivo para los delincuentes, que lo pueden emplear para comprometer a un individuo y permitir el movimiento lateral hacia la propia empresa, un cliente o un proveedor.

Los ataques de ingeniería social implicarán, principalmente, varias formas de *phishing*, por correo-e, voz, texto, mensajería instantánea y aplicaciones de terceros. No debemos perder de vista el *Deepfake*, que ha registrado una mejora drástica en su calidad y realismo. Estaremos cada vez más en situaciones comprometidas en la comunicación con tecnología Deepfake, sin saber si estamos interactuando con una persona real".

INETUM

Rafael Ortega
Director Digital Risk

"En ciberseguridad no tiene que haber capacidad de sorpresa, porque no podemos permitírnoslo. Creo que veremos más casos de *insiders*, con el objetivo de crear puertas traseras en software comercial u *open source*, así como en empresas que tengan información comercializable en los mercados oscuros. Así mismo, se verán incrementados los éxitos en ataques por malas configuraciones de las aplicaciones en los entornos *cloud*. La reducción de los tiempos en la ejecución de los ataques, hace que el *protect* sea una pieza clave para detener los incidentes de seguridad y el *recovery*, el seguro de vida de las organizaciones".

INFOBLOX

José Canelada
Solution Architect Manager

"En 2021 esperamos un incremento sustancial de los ataques personalizados y dirigidos al edge, así como contra los dispositivos IoT existentes, fundamentalmente enfocados a la extracción y comercialización de los datos. El mundo de las amenazas se ha industrializado por completo y el 'cibercrimen como servicio' permite la optimización de los componentes involucrados en un ataque. Ataques más sofisticados implican mayor supervivencia de la amenaza, así como mayor coste por tiempo de exposición. Se hace crítico reducir este tiempo mediante técnicas que permitan tanto agregar fuentes de inteligencia, como aplicar seguridad con independencia del contexto de comunicaciones, en el *edge* o allá donde residan los datos".

INGENIA

José Miguel Ruíz Padilla
Director de Seguridad y Servicios Gestionados

"En 2021 tendrá un gran impacto la pandemia por la esperada bajada de inversión en ciberseguridad en pymes así como el alto grado de teletrabajo desde casa que se mantendrá. Los *ransomware* continuarán siendo protagonistas debido a que resulta relativamente sencillo maximizar las ganancias con alta automatización y bajo riesgo. En la gran empresa y Administraciones Públicas se está comenzando a observar cómo se busca más la extracción de información que el cifrado y rescate. En el caso de las empresas hay que estar también muy atentos al incremento que estamos detectando en los incidentes relacionados con el fraude del CEO o las técnicas BEC. Las tendencias de automatización en el *malware* también están resultando problemáticas para las soluciones actuales. Hay que seguir vigilantes a las posibilidades de la inteligencia artificial y el 5G/IoT pero no esperamos un gran cambio al respecto aún en 2021".