LA CIBERDELINCUENCIA UTILIZA EL CORONAVIRUS PARA SEGUIR ACTUANDO

- **Estas últimas semanas ha aumentado exponencialmente el número de ciberamenazas que utilizan como pretexto el COVID-19.**
- **Es fundamental asumir buenas prácticas para prevenir la exposición frente a estas amenazas.**

Los ciberdelincuentes están en constante búsqueda de nuevas vías de comprometer la seguridad de los usuarios para obtener beneficio económico, por lo que desde hace varias semanas están aprovechando la tragedia que enfrenta el mundo con la pandemia del COVID-19 para llevar a cabo sus actividades maliciosas. A medida que el coronavirus comenzó a extenderse a nivel global también lo hicieron las acciones de los cibercriminales aprovechando esta situación. Estas últimas semanas hemos sido testigos de un aumento del phishing, del fraude en todas sus facetas y de la aparición de un buen número de programas maliciosos, que utilizan como pretexto el COVID-19, así como el aumento de los registros de dominio relacionados con el coronavirus y utilizados para llevar a cabo las acciones anteriormente descritas.

Diferentes modos de acción de los ciberdelincuentes

A continuación, vamos a enumerar una serie de ejemplos que, si bien no son un listado exhaustivo, son muy representativos del tipo de acciones maliciosas que están llevando a cabo los cibercriminales aprovechando la temática del COVID-19.

Ya en enero, con la crisis de China, empezaron los casos de **phishing y distribución de malware**. Los troyanos bancarios EMOTET y Lokibot se distribuyeron desde emails que suplantaban al Ministerio de Salud chino. AZORult se distribuyó como archivo de Microsoft Office explotando la vulnerabilidad CVE-2017-11882 que permitía ejecutar código malicioso en el ordenador infectado. Y últimamente, hay noticias de una campaña de phishing dirigida a empresas e instituciones gubernamentales en la que los correos electrónicos incluyen un archivo adjunto cuyo objetivo es hacerse con información sensible.

Las **amenazas para teléfonos móviles**, en especial dispositivos Android, están siendo muy explotadas. En concreto, el ransomware CovidLock, pasa por

ser una aplicación para rastrear información sobre el COVID-19, pero su función es bloquear los teléfonos hasta el pago de un rescate.

También se han detectado ataques dirigidos llevados a cabo por grupos organizados de ciberdelincuentes, las denominadas "Amenazas Persistentes Avanzadas" ("**Advanced Persistent Threats" – APTs**, en inglés), en los que se ha suplantado a la Organización Mundial de la Salud (OMS) con el objetivo de intentar sustraer información sensible. Hades APT ha sido uno de los más activos, Mustang Panda ha lanzado mensajes con supuestas declaraciones del Primer Ministro de Vietnam en los que incluía el malware conocido como "Vicious Panda", y en Libia, otro grupo está usando spyware para recopilar información sensible, distribuyendo un malware escondido en una app sobre coronavirus, SpyMax, la cual les permite obtener el registro de llamadas, los mensajes de texto, además de activar la cámara o micrófono del teléfono.

Otro caso que ha tenido especial repercusión es la suplantación a la Organización Mundial de la Salud (OMS) en una campaña en la que se solicitaba una donación que debía realizarse en forma de Bitcoins, con el objetivo de contribuir a la investigación de una cura contra el COVID-19.

Incluso la necesidad del **teletrabajo** en muchos países debido al confinamiento está siendo utilizado para generar VPNs falsas con el objetivo de robar datos personales y empresariales.

Las **estafas vía web** proliferan, sobre la compra de kits de prueba de virus, páginas fraudulentas orientadas a la recogida de donaciones, o portales que ofrecen y venden todo tipo de productos en los mercados de Darknet.

Los casos de **extorsión** afectan incluso a los hospitales, con la constancia de un ataque a un hospital de la República Checa. Aunque un buen número de grupos de ciberdelincuentes han "declarado" que no se atacarían instalaciones médicas o relacionadas con la salud, el grupo APT MAZE filtró datos confidenciales de una instalación del Reino Unido tras negarse a pagar el rescate.

Por otra parte, la **privacidad de los datos** de los usuarios es un tema que también está siendo sometido a debate, ya que algunas de las aplicaciones desarrolladas para contribuir en la lucha frente al COVID-19 se ha demostrado que no han contemplado la perspectiva de ciberseguridad en la fase de desarrollo y por tanto son vulnerables, o incluso que hacen un uso "dudoso" de la información que recopilan. De igual modo, se ha demostrado que algunos países ya rastrean a sus ciudadanos con la intención de controlar la infección, y que grandes empresas como Facebook, Apple, Amazon o Google, están generando información acerca del paradero de sus trabajadores, con quién hablan, hábitos, etc.

La concienciación y la cautela, los mejores consejos de seguridad

Por otro lado, hay una alta proliferación de **noticias falsas (fake news)** principalmente a través de las redes sociales y correo electrónico. La mejor forma de actuar pasa por mirar todo con lupa y confiar sólo en aquellas empresas, personas o instituciones de credibilidad solvente, así como en las agencias gubernamentales nacionales o locales.

El miedo a esta pandemia puede hacer que incluso los usuarios más cautelosos puedan pasar por alto peligros y convertirse en objetivo de los estafadores y ciberdelincuentes. Es imprescindible concienciarse de que un correo electrónico que provenga supuestamente de una fuente legítima puede contener algún programa malicioso (malware), y pensárselo mucho antes de abrir archivos adjuntos.

Finalmente, las empresas deben **garantizar la seguridad de sus empleados y de los datos** que éstos manejan a la hora de trabajar remotamente. Se deben establecer políticas que contribuyan a que la actividad se pueda realizar de una manera segura: utilización de VPN, contraseñas robustas, actualización de software, uso responsable de los dispositivos, etc.

Con el objetivo de ayudar a la protección de todos, hemos creado una página específica sobre el coronavirus, donde os iremos facilitando una serie de documentos que contribuyan a prevenir la exposición frente a las ciberamenazas.

info@bcsc.eus | 945 010 059

Parque Tecnológico de Álava
Albert Einstein. 46-3ª – Ed. E7 01510
Vitoria-Gasteiz