Los piratas informáticos siguen aprovechando el pánico provocado por COVID-19 para propagar malware en distintas formas mediante estafas y sitios falsos de seguimiento del coronavirus.

Los desarrolladores de aplicaciones de Android de terceros también están aprovechando la situación para utilizar palabras clave relacionadas con el coronavirus en sus nombres de aplicaciones, descripciones o en nombres de paquetes para eliminar malware, realizar robos financieros y clasificar más arriba en las búsquedas de Google PlayStore relacionadas con el tema.

> *«La mayoría de las aplicaciones maliciosas encontradas son amenazas de paquetes que van desde ransomware hasta envío de SMS, e incluso spyware diseñado para limpiar el contenido de los dispositivos de las víctimas en busca de datos personales o financieros»*, dijeron investigadores de Bitdefender en un informe de análisis de telemetría.

A medida que los usuarios buscaban más aplicaciones que proporcionaran informació sobre COVID-19, los autores de malware lograron infiltrarse en el adware, troyanos bancarios y ladrones de información bajo la apariencia de aplicaciones de seguimiento en vivo y aquellas que ayudan a los usuarios a identificar síntomas comunes de la enfermedad.

> *«A partir del 1 de enero de 2020, encontramos 579 aplicaciones que contienen palabras clave relacionadas con el coronavirus en su manifiesto (nombre del paquete, actividades, receptores, etc.)»*, dijeron los investigadores.
>
> *«Esto significa que un componente principal de la aplicación fue nombrado de una forma, o la aplicación contiene cadenas, que lo relaciona con el brote reciente. En*

> *total, 560 están limpios, 9 son troyanos y 10 son riskware»*, agregaron.

Además, algunas aplicaciones como Bubble Shooter Merge y Galaxy Shooter, Falcon Squad, incluso han cambiado su nombre y descripción para enfrentarse a la pandemia de coronavirus al incluir palabras clave que aseguran que sus aplicaciones tengan una clasificación más alta cuando las personas buscan coronavirus en la tienda de Play Store.

Esto ocurre aún con la estricta política de Google contra la capitalización de eventos sensibles y sus ajustes en los resultados de búsqueda de Google Play para filtrar intencionalmente aplicaciones potencialmente maliciosas cuando se buscan palabras clave como *«corona» o «coronavirus».*

Desde ataques cibernéticos hasta estafas de phishing, desde correos electrónicos de extorsión hasta sitios web maliciosos, una larga lista de amenazas digitales se está aprovechando del brote del coronavirus en las últimas semanas.

- Hackeo de routers: Un ataque recientemente descubierto dirigido a enrutadores domésticos y de pequeñas oficinas para redirigir a los usuarios a sitios maliciosos que se hacen pasar por recursos informativos sobre COVID-19, como un intento por instalar malware «Oski» que roba contraseñas y credenciales de criptomonedas.
- Estafas por correo electrónico y suplantación de identidad (phishing): Los correos electrónicos no deseados relacionados con el problema de salud ocuparon cerca del 2.5 por ciento del volumen total de correo no deseado, lo que indica cómo las estafas por correo electrónico vinculadas a la pandemia aumentaron constantemente solo en el mes de marzo. Además, al menos 42,578 nombres de dominio «covid» o «corona» se han registrado recientemente desde el comienzo del mes, con más de 2,500 dominios nuevos registrados en promedio todos los días en las últimas dos semanas.
- Ataques de Spear Phishing: Se ha descubierto que los atacantes abusan activamente

de los nombres y logotipos de muchas empresas y organizaciones en campañas de extorsión y phishing, incluida la Organización Mundial de la Salud (OMS) y los Centros de Control de Enfermedades de Estados Unidos (CDC), y envían documentos RTF especialmente diseñados en un intento de engañar a sus víctimas para que descarguen ladrones de información, troyanos de acceso remoto (RAT), recolectores de credenciales, entre otros.

- Ataques de ransomware: Los delincuentes cibernéticos detrás del ransomware Maze atacaron la red de TI de Hammersmith Medicines Research (HMR), un centro médico en espera para ayudar a llevar a cabo ensayos de cualquier posible vacuna contra el coronavirus, y publicaron los detalles personales de miles de ex pacientes luego de que la compañía declinara el pago de un rescate. El desarrollo se produjo después de que el grupo de hackers hizo una promesa pública no realizar ataques contra organizaciones de investigación médica durante la pandemia del coronavirus.
- Aplicaciones falsas: Las campañas de estafa y aplicaciones falsas que intentan vender curas de COVID-19 o máscaras faciales, han ido en aumento, además de aquellos que buscan solicitar inversiones en compañías fraudulentas que afirman estar desarrollando vacunas, o instar a los usuarios a realizar donaciones para organizaciones benéficas falsas.
- Malware bancario y piratería de tarjetas de pago: Los operadores del troyano bancario Ginp comenzaron a utilizar información sobre personas infectadas con coronavirus como un cebo para atraer a los usuarios de Android en España para regalar datos de tarjetas de crédito.

Métodos de protección

Todos estos hechos han llevado a la Agencia de Seguridad Cibernética e Infraestructura de Estados Unidos (CISA) a emitir advertencias sobre el aumento de las estafas temáticas de coronavirus, y a la Organización Mundial de la Salud (OMS) para emitir advertencias de estafas de suplantación de identidad que se hacen pasar por su organización.

Para protegerse de estas amenazas, se recomienda instalar aplicaciones solo de tiendas legítimas, buscar información en fuentes oficiales y desconfiar de correos electrónicos que

intenten hacer que el usuario abra archivos adjuntos o hacer clic en enlaces.

El FBI también emitió un aviso, donde persuade a los usuarios a estar atentos a correos electrónicos falsos de los CDC y correos electrónicos de phishing pidiendo a los destinatarios verificar su información personal:

> *«Los estafadores están aprovechando la pandemia COVID-19 para robar su dinero, su información personal o ambas cosas. No los dejen. Protéjase e investigue antes de hacer clic en los enlaces que pretenden proporcionar información sobre el virus; donar a una organización benéfica en línea o a través de redes sociales, contribuyendo a una campaña de crowdfunding, comprando productos en línea o dando su información personal para recibir dinero u otros beneficios».*