Según investigadores del equipo de Inteligencia de Amenazas Mandiant, de FireEye, el grupo de hackers conocido como FIN11 se ha involucrado en un patrón de campañas de ciberdelincuencia al menos desde 2016, con implicaciones como monetizar su acceso a las redes de organizaciones, además de implementar malware en el punto de venta (PoS) dirigido a los sectores financiero, minorista, restaurante y farmacéutico.

> *«Las recientes intrusiones de FIN11 han provocado con mayor frecuencia el robo de datos, la extorsión y la interrupción de las redes de las víctimas a través de la distribución del ransomware CLOP»*, dijo Mandiant.

Aunque las actividades de FIN11 en el pasado se han relacionado con malware como FlawedAmmyy, FRIENDSPEAK y MIXLABEL, Mandiant explica una superposición significativa en los TTP con otro grupo de amenazas que los investigadores de seguridad cibernética llaman TA505, que está detrás del troyano bancario Dridex y el ransomware Locky, que se entrega a través de campañas de malspam por medio de la botnet Necurs.

Cabe mencionar que Microsoft orquestó la eliminación de la botnet Necurs a inicios de marzo de este año, como un intento por evitar que los operadores registren nuevos dominios para ejecutar más ataques en el futuro.

Campañas de spam de alto volumen

FIN11, además de aprovechar un mecanismo de distribución de correo electrónico malicioso de alto volumen, amplió su orientación a los señuelos del idioma nativo junto con la información del remitente del correo electrónico manipulada, como nombres para mostrar y direcciones del remitente del correo electrónico falsificados, para que los mensajes parezcan más legítimos, con una gran inclinación a atacar a las organizaciones alemanas en sus campañas de 2020.

Por ejemplo, el adversario desencadenó una campaña de correo electrónico con asuntos

como *«informe de investigación N-xxxxx» o «accidente de laboratorio»* en enero de 2020, seguido de una segunda ola en marzo utilizando correos electrónicos de phishing con el asunto *«[Empresa farmacéutica] Hoja de cálculo de facturación 2020 YTD».*

> *«Las campañas de distribución de correo electrónico de alto volumen de FIN11 han evolucionado continuamente a lo largo de la historia del grupo»,* dijo Andy Moore, analista técnico senior de Mandiant Threat Intelligence.
>
> *«Aunque no hemos verificado independientemente la conexión, existen informes públicos sustanciales que sugieren que hasta algún momento de 2018, FIN11 dependía en gran medida de la botnet Necurs para la distribución de malware. Particularmente, el tiempo de inactividad observado en la botnet Necurs se ha correspondido directamente con pausas en la actividad, atribuida a FIN11».*

Según la investigación de Mandiant, las operaciones de FIN11 parecen haber cesado por completo desde mediados de marzo de 2020 hasta finales de mayo de 2020, antes de recuperarse en junio por medio de correos electrónicos de phishing que contienen archivos adjuntos HTML maliciosos de Microsoft Office.

Los archivos de Office, a su vez, utilizaron macros para recuperar el cuentagotas MINEDOOR y el descargador FRIENDSPEAK, que luego envió la puerta trasera MIXLABEL al dispositivo infectado.

Sin embargo, en los últimos meses, los esfuerzos de monetización de FIN11 resultaron en una serie de organizaciones infectadas por el ransomware CLOP, además de recurrir a ataques de extorsión híbridos, que combinada el ransomware con el robo de datos, en un intento por obligar a las empresas a aceptar pagos de extorsión que van desde unos cientos de miles de dólares hasta 10 millones de dólares.

> *«La monetización de las intrusiones por parte de FIN11 a través de ransomware y extorsión sigue una tendencia más amplia entre los actores motivados financieramente»*, dijo Moore.
>
> *«Las estrategias de monetización que históricamente han sido más comunes, como la implementación de malware en el punto de venta, limitan a los delincuentes a atacar a las víctimas en ciertas industrias, mientras que la distribución de ransomware puede permitir a los actores beneficiarse de una intrusión en la red de casi cualquier organización. Esa flexibilidad, en combinación con informes cada vez más frecuentes de pagos de rescates disparados, lo convierte en un esquema extremadamente atractivo para los actores motivados financieramente»,* agregó.

Mandiant también explicó algo sobre el origen de FIN11, asegurando que el grupo opera desde la Comunidad de Estados Independientes (CEI) debido a la presencia de metadatos de archivos en ruso, la evitación de despliegues de CLOP en países de la CEI y la dramática caída en la actividad coincidiendo con el año nuevo ruso y el período de vacaciones de Navidad ortodoxa entre el 1 y el 8 de enero.

> *«Salvo algún tipo de interrupción en sus operaciones, es muy probable que FIN11 siga atacante a las organizaciones con el objetivo de implementar ransomware y robar datos para utilizarlos en la extorsión»*, dijo Moore.
>
> *«Debido a que el grupo actualiza periódicamente sus TTP para evadir las detecciones y aumentar la eficacia de sus campañas, también es probable que estos cambios incrementales sigan. Sin embargo, a pesar de estos cambios, las campañas de FIN11 recientes se han basado constantemente en el uso de macros integrados en documentos de Office maliciosos para entregar sus cargas útiles. Junto con otras mejores prácticas de seguridad, las organizaciones pueden minimizar el riesgo de verse comprometidas por FIN11 al capacitar a los usuarios*

> *para identificar correos electrónicos de phishing, deshabilitar las macros de Office e implementar detecciones para el descargador de FRIENDSPEAK»,* agregó.