Un nuevo grupo de Amenaza Persistente Avanzada (APT), ha estado detrás de una serie de ataques contra hoteles en todo el mundo, junto con gobiernos, organizaciones internacionales, empresas de ingeniería y bufetes de abogados.

La compañía eslovaca de seguridad cibernética ESET, nombró al grupo de ciberespionaje como Famous Sparrow, y dijo que ha estado activo desde al menos agosto de 2019, con víctimas ubicadas en África, Asia, Europa, Oriente Medio y América, en varios países como Burkina Faso y Taiwán, Francia, Lituania, Reino Unido, Israel, Arabia Saudita, Brasil, Canadá y Guatemala.

Los ataques montados por el grupo involucran la explotación de vulnerabilidades conocidas en aplicaciones de servidor como SharePoint y Oracle Opera, además de la vulnerabilidad de ejecución remota de código ProxyLogon en Microsoft Exchange Server, que salió a la luz en marzo de 2021, lo que lo convierte en el último actor de amenazas en haber tenido acceso antes de que los detalles de la vulnerabilidad se hicieran públicos.

Según ESET, las intrusiones que explotan las vulnerabilidades comenzaron el 3 de marzo, lo que resultó en el despliegue de varios artefactos maliciosos, incluyendo dos versiones personalizadas del ladrón de credenciales Mimikatz, un escáner NetBIOS llamado Nbtscan y un cargador para un implante personalizado denominado SparrowDoor.

Se instala aprovechando una técnica llamada secuestro de orden de búsqueda de DLL, SparrowDoor funciona como una utilidad para excavar en nuevos rincones de la red interna del objetivo a los que los hackers también obtuvieron acceso para ejecutar comandos arbitrarios, así como para acumular y exfiltrar información confidencial a un servidor de comando y control (C2) bajo su control

Aunque ESET no atribuyó el grupo FamousSparrow a un país específico, sí encontró similitudes entre sus técnicas y las de SparklingGoblin, una rama del Grupo Winnti vinculado a China, y DRBControl, que también se superpone con el malware previamente identificado como Campañas Winnti y Emissary.

> *«Este es otro recordatorios de que es fundamental parchear las aplicaciones de Internet rápidamente o, si no es posible hacerlo rápidamente, no exponerlas a Internet en absoluto»,* dijeron los investigadores de ESET Tahseen Bin Taj y Matthieu Faou.