Los sistemas Windows y Linux están siendo atacados por una variante de ransomware llamada HelloXD, y las infecciones también implican la implementación de una backdoor para facilitar el acceso remoto persistente a los hosts infectados.

> *«A diferencia de otros grupos de ransomware, esta familia de ransomware no tiene un sitio de fuga activo; en su lugar, prefiere dirigir a la víctima afectada a las negociaciones por medio del chat Tox y las instancias de mensajería basadas en onion»,* dijeron Daniel Bunce y Doel Santos, investigadores de seguridad de Unit42 de Palo Alto.

HelloXD apareció en la naturaleza el 30 de noviembre de 2021 y se basa en el código filtrado de Babuk, que se publicó en un foro de ciberdelincuencia en idioma ruso en septiembre de 2021.

La familia de ransomware no es una excepción a la norma en el sentido de que los operadores siguen el enfoque comprobado de la doble extorsión para exigir pagos en criptomonedas extrayendo los datos confidenciales de la víctima, además de cifrarlos y amenazar con publicar la información.

El implante en cuestión, llamado MicroBackdoor, es un malware de código abierto que se utiliza para comunicaciones de comando y control (C2), y su desarrollador Dmytro Oleksiuk, lo calificó como *«algo realmente minimalista con todas las características básicas en menos de 5,000 líneas de código».*

En particular, el atacante bielorruso denominado Ghostwritter (también conocidoc omo UNC1151) adoptó diferentes variantes del implante en sus operaciones cibernéticas contra organizaciones estatales ucranianas en marzo de 2022.

Las características de MicroBackdoor permiten a un atacante explorar el sistema de archivos, cargar y descargar archivos, ejecutar comandos y borrar evidencia de su presencia de las máquinas comprometidas. Se sospecha que el despliegue de la backdoor se lleva a cabo para *«monitorear el progreso del ransomware».*

Unit 42 dijo que vinculó al probable desarrollador ruso detrás de HelloXD, que usa los alias en línea x4k, L4ckyguy, unKn0wn, unk0w, _unkn0wn y x4kme, con otras actividades maliciosas como la venta de exploits de prueba de concepto (PoC) y distribuciones de Kali Linux reconstruyendo el rastro digital del atacante.

> *«x4k tiene una presencia en línea muy sólida, lo que nos ha permitido descubrir gran parte de su actividad en estos últimos años. Este actor de amenazas ha hecho poco para ocultar la actividad maliciosa y probablemente seguirá con este comportamiento»,* dijeron los investigadores.

Los hallazgos surgen cuando un nuevo estudio de IBM X-Force reveló que la duración promedio de un ataque de ransomware empresarial, es decir, el tiempo entre el acceso inicial y la implementación del ransomware, se redujo un 94.34% entre 2019 y 2021 de más de dos meses a solo 3.85 días.

Las tendencias de mayor velocidad y eficiencia en el ecosistema de ransomware como servicio (RaaS) se han atribuido al papel fundamental que desempeñan los intermediarios de acceso inicial (IAB) para obtener acceso a las redes de las víctimas y luego vender el acceso a los afiliados, quienes, a su vez, abusan del punto de apoyo para implementar cargas útiles de ransomware.

> *«La compra de acceso puede reducir de forma significativa la cantidad de tiempo que tardan los operadores de ransomware en realizar un ataque al permitir el reconocimiento de sistemas y la identificación de datos clave antes y con mayor facilidad»,* dijo Intel 471 en un informe que destaca las relaciones de trabajo entre

> los IAB y equipos de ransomware.

> *«Además, a medida que las relaciones se fortalecen, los grupos de ransomware pueden identificar a una víctima a la que desean apuntar y el comerciante de acceso podría proporcionarles el acceso una vez que esté disponible».*