Los grupos de hackers que utilizan ransomware siguen evolucionando sus tácticas y técnicas para implementar el malware de cifrado de archivos en los sistemas comprometidos, a pesar de las acciones disruptivas de las autoridades contra los grupos de ciberdelincuentes.

> *«Ya sea debido a la aplicación de la ley, las luchas internas entre grupos o las personas que abandonan las variantes por completo, los grupos de RaaS (Ransomware as a Service) que dominan el ecosistema en este momento, son completamente diferentes a hace unos meses. Sin embargo, incluso con el cambio en las variantes, los incidentes de ransomware en su conjunto siguen aumentando»,* dijeron los investigadores de Intel 471.

Las amplias operaciones de aplicación de la ley realizadas por agencias gubernamentales en los últimos meses, han provocado cambios rápidos en el panorama de RaaS y han cambiado las tornas de los sindicatos de ransomware como Avaddon, BlackMatter, Cl0p, DarkSide, Egregor y REvil, lo que ha obligado a los atacantes a reducir la velocidad o detener sus actividades en conjunto.

Sin embargo, cuando estas variantes se van desvaneciendo, otros grupos emergentes intervienen para ocupar su lugar. Los hallazgos de Intel 471 descubrieron un total de 612 ataques de ransomware entre julio y septiembre de 2021, que se pueden atribuir a 35 variantes de ransomware diferentes.

Aproximadamente el 60% de las infecciones observadas estaban vinculadas solo a cuatro variantes, encabezadas por LockBito 2.0 (33%), Conti (15.2%), BlackMatter (6.9%) y Hive (6%), y afectaron principalmente a la fabricación, el consumidor y la industria de productos, servicios profesionales, consultoría y el sector inmobiliario.

Avos Locker es uno de los muchos cárteles de este tipo, que no solo han sido testigos de un aumento de ataques, sino que también han optado por nuevas tácticas para perseguir sus esquemas motivados financieramente, siendo el principal de ellos la capacidad de deshabilitar los productos de seguridad de terminales en los sistemas objetivo y arrancar en

Modo Seguro de Windows para ejecutar el ransomware. También se instala la herramienta de control remoto AnyDesk para mantener el acceso a la máquina mientras se ejecuta en modo seguro.

> *«La razón de esto es que muchos, si no la mayoría, de los productos de seguridad para endpoints no se ejecutan en modo seguro, una configuración de diagnóstico especial en la que Windows desactiva la mayoría de los controladores y software de terceros y puede hacer que las máquinas protegidas no sean seguras. Las técnicas implementadas por Avos Locker son simples pero inteligentes, y los atacantes se aseguran de que el ransomware tenga la mejor oportunidad de ejecutarse en modo seguro y permiten que los atacantes retengan el acceso remoto a las máquinas durante todo el ataque»,* dijo el investigador principal de seguridad de Sophos, Andrew Brandt.

El programa RaaS de Hive, por su parte, ha sido calificado de «agresivo» por su uso de tácticas de presión para hacer que las organizaciones víctimas paguen rescates, y Group-IB vinculó la tensión con los ataques a 355 empresas a partir del 16 de octubre desde que surgió en el panorama a finales de junio de 2021.

Mientras tanto, el grupo de ransomware ruso Everest, está llevando sus tácticas de extorsión al siguiente nivel al amenazar con vender el acceso a sistemas específicos si no se cumplen sus demandas, dijo NCC Group.

> *«Aunque la venta de ransomware como servicio ha experimentado un aumento en la popularidad durante el último año, este es un caso raro de un grupo que renuncia a una solicitud de rescate y ofrece acceso a la infraestructura de TI, pero es posible que veamos ataques de imitación en 2022 y más allá»,* dijo la compañía de ciberseguridad.

Además, una familia de ransomware relativamente nueva denominada Pysa (también conocida como Mespinoza), ha desbancado a Conti como uno de los principales grupos de amenazas de ransomware para el mes de noviembre junto con LockBit 2.0.

El ransomware experimentó un aumento del 50% en el número de empresas objetivo y un aumento del 400% en los ataques contra los sistemas del sector gubernamental en comparación con el mes de octubre.

> *«Aunque las fuerzas del orden en todo el mundo se han vuelto más agresivas en sus esfuerzos por arrestar a quienes están detrás de los ataques, los desarrolladores aún siguen cerrando fácilmente las variantes populares, manteniendo un perfil bajo y regresando con malware finalmente ajustado utilizado por ellos mismos y sus afiliados. Mientras los desarrolladores puedan permanecer en países donde se les otorga un puerto seguro, los ataques seguirán, aunque con diferentes variantes»,* dijeron los investigadores de Intel 471.