Se han observado hasta 722 ataques de ransomware durante el cuarto trimestre de 2021, con LockBit 2.0, Conti, PYSA, Hive y Grief, emergiendo como las cepas más frecuentes, según una nueva investigación publicada por Intel 471.

Los ataques marcan un aumento de 110 y 129 ataques desde el tercer y segundo trimestre de 2021, respectivamente. En total, se detectaron 34 variantes de ransomware diferentes durante el período de tres meses entre octubre y diciembre de 2021.

> *«La cepa de ransomware más prevalente en el cuarto trimestre de 2021 fue LockBit 2.0, que fue responsable del 29.7% de todos los incidentes informados, seguida de Conti con el 19%, PYSA con el 10.5% y Hive con el 10.1%»,* dijeron los investigadores en un informe.

Algunos de los sectores más impactados durante el trimestre fueron productos de consumo e industriales, fabricación, servicios profesionales y consultoría, bienes raíces, ciencias de la vida y atención de la salud, tecnología, medios y telecomunicaciones, energía, recursos y agricultura, sector público, servicios financieros y entidades sin fines de lucro.

De todos los ataques de LockBit 2.0 registrados, los países más afectados fueron Estados Unidos, seguidos de Italia, Alemania, Francia y Canadá. La mayoría de las infecciones de Conti también se informaron en Estados Unidos, Alemania e Italia. Estados Unidos también siguió siendo el país más afectado por los ataques de ransomware PYSA y Hive.

> *«Los ataques que afectaron al sector de productos industriales y de consumo aumentaron un 22.2% desde el tercer trimestre de 2021, lo que lo convirtió en el sector más afectado durante el cuarto trimestre»,* dijeron los investigadores.

Estos hallazgos surgen cuando salió a la luz una cepa de ransomware relativamente

desconocida llamada Nokoyawa con *«sorprendentes similitudes»* con el ransomware Hive, con la mayoría de sus objetivos ubicados principalmente en Argentina.

> *«Tanto Nokoyawa como Hive incluyen el uso de Cobalt Strike como parte de la fase de llegada del ataque, así como el uso de herramientas legítimas, pero comúnmente abusadas, como los escáneres anti-rootkit GMER y PC Hunter para la evasión de la defensa»*, dijeron los investigadores de Trend Micro.