Se ha descubierto que un agente de acceso inicial previamente indocumentado proporciona puntos de entrada a tres actores de amenazas diferentes para generar intrusiones que van desde ataques de ransomware motivados financieramente hasta campañas de phishing.

El equipo de investigación e inteligencia de BlackBerry nombró a la entidad como Zebra2104, siendo este grupo responsable de ofrecer un medio de enfoque digital para los sindicatos de ransomware como MountLocker y Phobos, así como la Amenaza Persistente Avanzada (APT) rastreada bajo el nombre de StrongPity, también conocido como Prometeo.

El panorama de amenazas tal como lo conocemos ha estado cada vez más dominado por una categoría de jugadores conocidos como los agentes de acceso inicial (IAB), que son conocidos por proporcionar a otros grupos de ciberdelincuentes, incluidos los afiliados de ransomware, un punto de apoyo en un grupo infinito de organizaciones que pertenecen a diversas geografías y sectores a través de puertas traseras persistentes en las redes de víctimas, construyendo efectivamente un modelo de precios para el acceso remoto.

> *«Normalmente, los IAB primero obtienen acceso a la red de la víctima y luego venden ese acceso al mejor postor en foros clandestinos ubicados en la web oscura. Más adelante, el postor ganador a menudo implementará ransomware u otro malware con motivación financiera dentro de la organización de la víctima, según los objetivos de su campaña»*, dijeron los investigadores de BlackBerry.

Un análisis de agosto de 2021 de más de 1,000 listados de acceso anunciados para la venta por IAB en foros clandestinos en la web oscura, encontró que el costo promedio del acceso a la red fue de 5400 dólares para el período de julio de 2020 a junio de 2021, con las ofertas más valiosas que incluyen privilegios de administrador de dominio a los sistemas empresariales.

La investigación de la empresa canadiense de seguridad cibernética comenzó con un dominio llamado *«trashborting[.]com»*, que se encontró entregando CobaltStrike Beacons, usándolo para vincular la infraestructura más amplia a una serie de campañas de malspam que dieron

como resultado la entrega de cargas útiles de ransomware, algunas de las cuales se centraron en las empresas inmobiliarias australianas y los departamentos gubernamentales estatales en septiembre de 2020.

Además de eso, se descubrió que *«supercomb*inating[.]com», otro dominio hermano registrado junto con *trashborting[.]com*, estaba conectado a una actividad maliciosa de MountLocker y Phobos, incluso cuando el dominio se resolvió en una dirección IP «91.92.109[.]174», que a su vez, también se usó para alojar un tercer dominio *«mencionone*common*[.]com»* entre abril y noviembre de 2020 y se utilizó como un servidor de comando y control en una campaña de junio de 2020 asociada con StrongPity.

Las superposiciones y la amplia orientación de la IAB también han llevado a los investigadores a creer que el operador *«o tiene mucha mano de obra o ha instalado trampas grandes 'ocultas a la vista' en Internet»,* lo que permite a MountLocker, Phobos y StrongPity obtener su acceso a las redes específicas.

> *«La red interconectada de infraestructura maliciosa vista a lo largo de esta investigación ha demostrado que, de una forma que refleja el mundo empresarial legítimo, los grupos de ciberdelincuencia se administran en algunos casos de forma similar a las organizaciones multinacionales. Crean asociaciones y alianzas para ayudar a avanzar en sus objetivos. En todo caso, es seguro asumir que estas 'asociaciones comerciales' de grupos de amenazas se volverán aún más frecuentes en el futuro»,* dijeron los investigadores.