La inteligencia militar rusa encabezó una campaña de ataque de fuerza bruta en curso dirigida a entornos empresariales en la nube desde mediados de 2019, según un aviso conjunto publicado por agencias de inteligencia en el Reino Unido y Estados Unidos.

La Agencia de Seguridad Nacional (NSA), la Agencia de Seguridad de Infraestructura y Ciberseguridad (CISA), la Oficina Federal de Investigaciones (FBI) y el Centro Nacional de Seguridad Cibernética del Reino Unido (NCSC), atribuyeron formalmente las incursiones a la Dirección Principal de Inteligencia del Estado Mayor de Rusia (GRU) y el 85° Centro Principal de Servicios Especiales (GTsSS).

El actor de las amenazas también se rastrea bajo varios apodos, como APT28 (FireEye Mandiant), Fancy Bear (CrowdStrike), Sofacy (Kaspersky), STRONTIUM (Microsoft) y Iron Twilight (Secureworks).

APT28 tiene un largo historial en aprovechar la aplicación de contraseñas y los intentos de inicio de sesión por fuerza bruta para saquear credenciales válidas que permitan futuras operaciones de vigilancia o intrusión.

En noviembre de 2020, Microsoft reveló actividades de recolección de credenciales organizadas por el adversario dirigidas a empresas involucradas en la investigación de vacunas y tratamientos para COVID19.

Lo que es diferente esta vez, es la dependencia del atacante por los contenedores de software para escalar sus ataques de fuerza bruta.

> *«La campaña utiliza un clúster de Kubernetes en intentos de acceso de fuerza bruta contra los entornos empresariales y de nube de objetivos gubernamentales y del sector privado en todo el mundo. Después de obtener las credenciales a través de la fuerza bruta, GTsSS utiliza una variedad de vulnerabilidades conocidas para un mayor acceso a la red mediante la ejecución remota de código y el movimiento lateral»,* dijo CISA.

Algunas de las otras vulnerabilidades de seguridad explotadas por APT28 para pivotar dentro de las organizaciones violadas y obtener acceso a los servidores de correo electrónico incluyen:

- CVE-2020-0688 – Vulnerabilidad de ejecución remota de código de clave de validación de Microsoft Exchange.
- CVE-2020-17144 – Vulnerabilidad de ejecución remota de código de Microsoft Exchange.

También se cree que el actor de amenazas ha utilizado distintas técnicas de evasión en un intento de disfrazar algunos componentes de sus operaciones, incluido el enrutamiento de intentos de autenticación de fuerza bruta por medio de Tor y servicios VPN comerciales, como CactusVPN, IPVanish, NordVPN, ProtonVPN, Surfshark y WorldVPN.

Las agencias afirmaron que los ataques se centraron principalmente en Estados Unidos y Europa, dirigidos al gobierno y al ejército, contratistas de defensa, empresas de energía, educación superior, empresas de logística, bufetes de abogados, empresas de medios, consultores políticos o partidos políticos y grupos de expertos.

> *«Los administradores de red deberían adoptar y expandir el uso de la autenticación multifactor para ayudar a contrarrestar la efectividad de esta capacidad. Las mitigaciones adicionales para garantizar controles de acceso sólidos incluyeron funciones de tiempo de espera y bloqueo, el uso obligatorio de contraseñas seguras, la implementación de un modelo de seguridad Zero Trust que utiliza atributos adicionales al determinar el acceso y análisis para detectar acceso anómalos»,* dice el aviso.