investigadores de seguridad desenmascararon este viernes una nueva infraestructura de comando y control (C2) perteneciente al actor de amenazas ruso denominado APT29, también conocido como Cozy Bear, que ha sido detectado sirviendo activamente el malware WellMess como parte de una campaña de ataque en curso.

Se han descubierto más de 30 servidores C2 operados por la inteligencia extranjera rusa, dijo la filial de seguridad cibernética de Microsoft, RiksIQ.

Se cree que APT29, el apodo asignado a los agentes gubernamentales que trabajan para el Servicio de Inteligencia Exterior de Rusia (SVR), fue el cerebro detrás del ataque masivo de la cadena de suministro SolarWinds que salió a la luz a fines del año pasado, con los gobiernos de Reino Unido y Estados Unidos sobre Rusia a inicios de abril.

La comunidad de ciberseguridad está rastreando la actividad bajo varios nombres en clave, incluyendo UNC2452 (FireEye), Nobelium (Microsoft), SolarStorm (Unit42), StellarParticle (CrowdStrike), Dark Halo (Volexity) y Iron Ritual (Secureworks), citando diferencias en las tácticas, técnicas y procedimientos (TTP) empleados por el adversario con el de perfiles de atacantes conocidos, incluyendo APT29.

Identificado por primera vez por JPCERT/CC de Japón en 2018, WellMess (también conocido como WellMail), se desplegó previamente en campañas de espionaje emprendidas por el actor de amenazas para saquear la propiedad intelectual de múltiples organizaciones involucradas en la investigación y el desarrollo de vacunas COVID-19 en el Reino Unido, Estados Unidos y Canadá.

> *«El grupo utiliza una variedad de herramientas y técnicas para apuntar de forma predominante a objetivos gubernamentales, diplomáticos, de grupos de expertos, de atención médica y de energía para obtener inteligencia»*, dijo el Centro Nacional de Seguridad Cibernética (NCSC) del Reino Unidos en un aviso publicado en julio de 2020.

RiskIQ dijo que comenzó su investigación sobre la infraestructura de ataque de APT29 luego de una divulgación pública sobre un nuevo servidor WellMess C2 el 11 de junio, lo que llevó al descubrimiento de un clúster de no menos de 30 servidores C2 activos. Se cree que uno de los servidores estuvo activo el 9 de octubre de 2020, aunque no está claro cómo se utilizan estos servidores o quiénes son los objetivos.

Esta no es la primera vez que RiskIQ identifica la huella de comando y control asociada con los hackers de SolarWinds. En abril, descubrió un conjunto adicional de 18 servidores con alta confianza que probablemente se comunicaron con las cargas útiles secundarias de Cobalt Strike entregadas a través del malware TEARDROP y RAINDROP implementado en los ataques.

> *«El equipo Atlas de RiskIQ evalúa con gran confianza que estas direcciones IP y certificados están en uso activo por ATP29. No pudimos localizar ningún malware que se comunicara con esta infraestructura, pero sospechamos que probablemente sea similar a las muestras identificadas anteriormente»,* dijo Kevin Livelli, director de inteligencia de amenazas de RiskIQ.