Se ha observado que actores de amenazas están apuntando a empresas de semiconductores en Asia Oriental mediante señuelos que se hacen pasar por la empresa Taiwan Semiconductor Manufacturing Company (TSMC) con el propósito de entregar beacons de Cobalt Strike.

Este grupo de intrusión, según el informe de EclecticIQ, utiliza una puerta trasera denominada HyperBro, la cual luego se emplea como un conducto para desplegar software de simulación de ataques comerciales y un conjunto de herramientas de postexplotación.

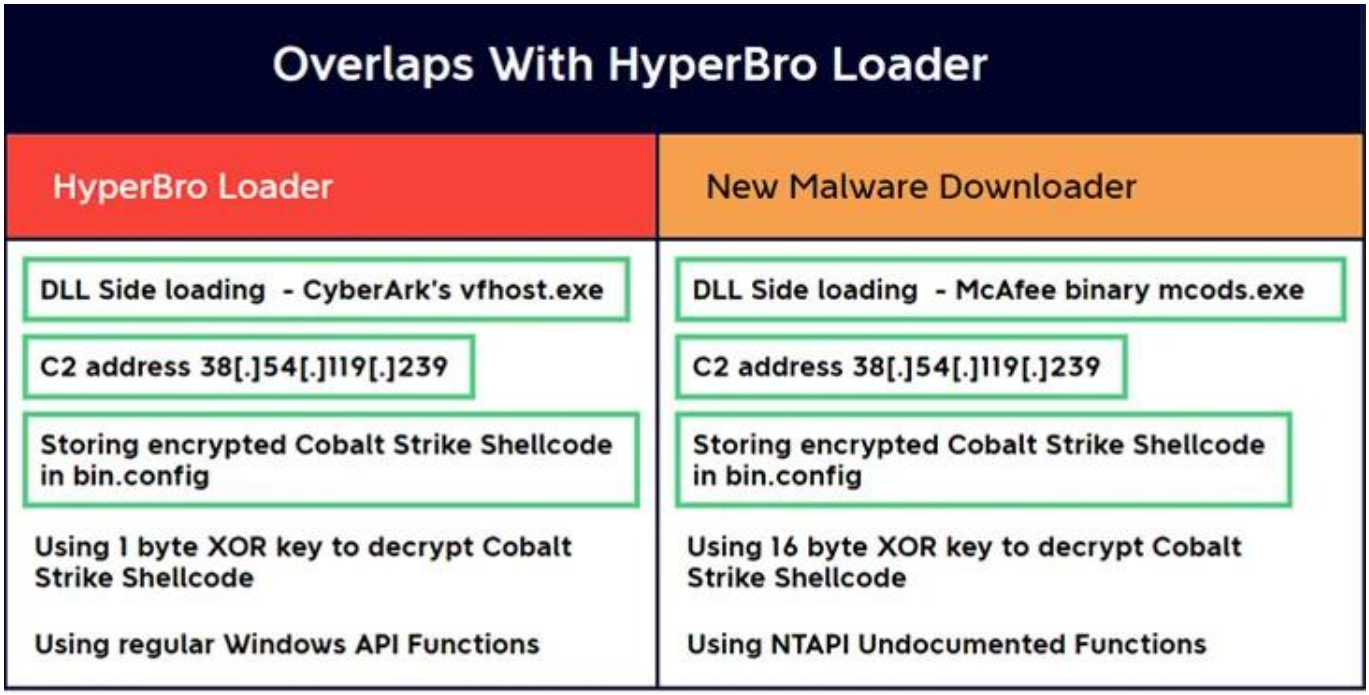
Se ha identificado una secuencia de ataque alternativa que utilizó previamente un malware para descargar no documentado para desplegar Cobalt Strike, lo que sugiere que los actores de amenazas diseñaron múltiples enfoques para infiltrarse en los objetivos de su interés.

La firma de ciberseguridad neerlandesa atribuye esta campaña a un actor de amenazas vinculado a China debido al uso de HyperBro, una herramienta que ha sido utilizada casi exclusivamente por un grupo de amenazas conocido como Lucky Mouse (también llamado APT27, Budworm y Emissary Panda).

También se han encontrado coincidencias tácticas entre el adversario responsable de estos ataques y otro grupo rastreado por RecordedFuture bajo el nombre de RedHotel, que también tiene similitudes con un grupo de piratas informáticos conocido como Earth Lusca.

Otra conexión china se relaciona con el uso de un servidor web Cobra DocGuard que probablemente haya sido comprometido para alojar binarios de segunda etapa, incluyendo un implante basado en Go llamado ChargeWeapon, que se distribuye mediante el programa de descarga.

> Según Arda Büyükkaya, investigador de EclecticIQ, *«ChargeWeapon está diseñado para obtener acceso remoto y enviar información sobre dispositivos y redes desde un host infectado a un servidor de comando y control controlado por el atacante».*




Es importante destacar que una versión adulterada del software de encriptación Cobra DocGuard de EsafeNet también ha sido vinculada con la implementación de PlugX, y Symantec lo relaciona con un actor sospechoso de tener conexiones con China, conocido como Carderbee.

En la cadena de ataque documentada por EclecticIQ, se utiliza un documento PDF con temática de TSMC como señuelo después de la ejecución de HyperBro, lo que indica el uso de técnicas de ingeniería social para activar la infección.

> Büyükkaya explica que *«al presentar un PDF aparentemente normal mientras se ejecuta en secreto el malware en segundo plano, se minimiza la probabilidad de que la víctima sospeche».*

Un aspecto destacado del ataque es que la dirección del servidor de comando y control (C2)

codificada en el beacon de Cobalt Strike se camufla como una CDN de jQuery legítima en un intento de burlar las defensas del firewall.

Esta información se hace pública mientras que el Financial Times informa que la Agencia de Inteligencia y Seguridad del Estado de Bélgica (VSSE) está trabajando en *«detectar y combatir posibles actividades de espionaje y/o interferencia llevadas a cabo por entidades chinas, incluido Alibaba»*, en el aeropuerto de carga de Liège en el país.

> *«Las acciones de China en Bélgica no se limitan al típico espionaje para robar secretos de Estado ni al ciberataque que paraliza una industria esencial o un departamento gubernamental desde la computadora de un hacker. En un esfuerzo por influir en los procesos de toma de decisiones, China emplea una variedad de recursos, tanto estatales como no estatales»*, señaló la agencia en un informe de inteligencia.

Un informe publicado el mes pasado por el Departamento de Defensa de los Estados Unidos (DoD) describió a China como una *«amenaza amplia y omnipresente de espionaje cibernético»* y afirmó que roba secretos tecnológicos y realiza esfuerzos de vigilancia para obtener una ventaja estratégica.

> *«Mediante medios cibernéticos, la República Popular China (PRC, por sus siglas en inglés) ha llevado a cabo campañas prolongadas de espionaje, robo y compromiso contra redes fundamentales de defensa y la infraestructura crítica más amplia de los Estados Unidos, en especial la Base Industrial de Defensa (DIB, por sus siglas en inglés)»*, declaró el DoD.