Diversos actores de amenazas con conexiones a China han sido asociados con la explotación zero-day de tres vulnerabilidades de seguridad que afectan a los dispositivos de Ivanti (CVE-2023-46805, CVE-2024-21887 y CVE-2024-21893).

Estos grupos están siendo monitoreados por Mandiant bajo los nombres UNC5221, UNC5266, UNC5291, UNC5325, UNC5330 y UNC5337. Otro grupo vinculado a esta oleada de explotación es UNC3886.

La subsidiaria de Google Cloud también ha observado que actores con motivaciones financieras están explotando CVE-2023-46805 y CVE-2024-21887, probablemente con el objetivo de realizar operaciones de minería de criptomonedas.

> *«UNC5266 coincide en parte con UNC3569, un actor de espionaje chino que ha sido visto explotando vulnerabilidades en Aspera Faspex, Microsoft Exchange y Oracle Web Applications Desktop Integrator, entre otros, para obtener acceso inicial a entornos objetivo»*, comentaron los investigadores de Mandiant.

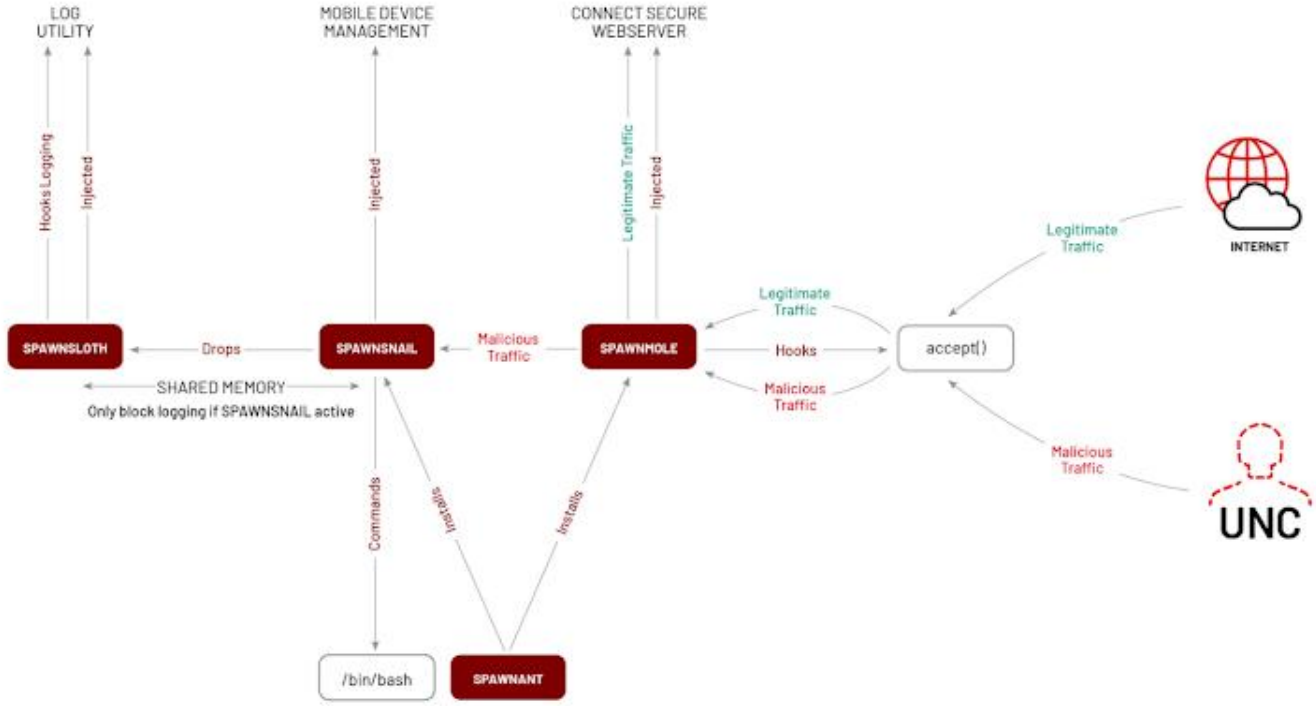
Este actor de amenazas ha sido relacionado con actividades posteriores a la explotación que llevan a la implementación del framework de comando y control (C2) Sliver, una variante del ladrón de credenciales WARPWIRE y un nuevo backdoor basado en Go llamado TERRIBLETEA que cuenta con funciones de ejecución de comandos, registro de teclas, escaneo de puertos, interacción con el sistema de archivos y captura de pantalla.

UNC5330, que ha sido observado combinando CVE-2024-21893 y CVE-2024-21887 para comprometer dispositivos de VPN Ivanti Connect Secure al menos desde febrero de 2024, ha utilizado malware personalizado como TONERJAM y PHANTOMNET para facilitar acciones posteriores a la compromiso.

- PHANTOMNET: un backdoor modular que se comunica mediante un protocolo de comunicación personalizado sobre TCP y emplea un sistema basado en complementos para descargar y ejecutar cargas útiles adicionales.

- TONERJAM: un lanzador diseñado para desencriptar y ejecutar PHANTOMNET.

Además de utilizar la Instrumentación de Administración de Windows (WMI) para realizar reconocimiento, movimiento lateral, manipulación de entradas de registro y establecimiento de persistencia, UNC5330 también se sabe que compromete cuentas de enlace LDAP configuradas en los dispositivos infectados para obtener acceso de administrador de dominio.



Otro actor notable de espionaje vinculado a China es UNC5337, que se dice que ha infiltrado dispositivos Ivanti desde enero de 2024 utilizando CVE-2023-46805 y CVE-2024 para entregar un conjunto de herramientas de malware personalizado conocido como SPAWN que comprende cuatro componentes distintos que trabajan en conjunto para funcionar como un backdoor sigiloso y persistente:

- SPAWNSNAIL: un backdoor pasivo que escucha en localhost y está equipado para

lanzar una shell interactiva de bash, así como lanzar SPAWNSLOTH.

- SPAWNMOLE: un utilitario de túnel capaz de dirigir tráfico malicioso a un host específico mientras pasa tráfico benigno sin modificar al servidor web Connect Secure.
- SPAWNANT: un instalador responsable de garantizar la persistencia de SPAWNMOLE y SPAWNSNAIL aprovechando una función de instalador de coreboot.
- SPAWNSLOTH: un programa de manipulación de registros que desactiva el registro y el reenvío de registros a un servidor syslog externo cuando el implante SPAWNSNAIL está en ejecución.

Mandiant ha evaluado con mediana confianza que UNC5337 y UNC5221 son el mismo grupo de amenazas, y señala que la herramienta SPAWN está *«diseñada para permitir el acceso a largo plazo y evitar la detección».*

UNC5221, que anteriormente se atribuyó a web shells como BUSHWALK, CHAINLINE, FRAMESTING y LIGHTWIRE, también ha desatado una web shell basada en Perl llamada ROOTROT que está incrustada en un archivo .ttc legítimo de Connect Secure ubicado en «/data/runtime/tmp/tt/setcookie.thtml.ttc» al explotar CVE-2023-46805 y CVE-2024-21887.

El despliegue exitoso de la web shell es seguido por el reconocimiento de red y el movimiento lateral, lo que en algunos casos resulta en la compromiso de un servidor vCenter en la red de la víctima mediante un backdoor de Golang llamado BRICKSTORM.

«BRICKSTORM es un backdoor de Go dirigido a servidores VMware vCenter. Admite la capacidad de configurarse como un servidor web, realizar manipulación del sistema de archivos y directorios, realizar operaciones de archivo como cargar/descargar, ejecutar comandos de shell y realizar retransmisiones SOCKS», explicaron los investigadores de Mandiant.

El último de los cinco grupos chinos vinculados al abuso de las fallas de seguridad de Ivanti es UNC5291, que Mandiant dijo que probablemente tenga asociaciones con otro grupo de piratas informáticos, UNC3236 (también conocido como Volt Typhoon), principalmente debido a su enfoque en los sectores académico, energético, de defensa y de salud.

> *«La actividad de este clúster comenzó en diciembre de 2023 enfocándose en Citrix Netscaler ADC y luego cambió para centrarse en los dispositivos Ivanti Connect Secure después de que se hicieran públicos los detalles a mediados de enero de 2024»,* dijo la empresa.

Estos hallazgos vuelven a resaltar la amenaza que representan los dispositivos perimetrales, con los actores de espionaje utilizando una combinación de vulnerabilidades zero-day, herramientas de código abierto y backdoors personalizados para adaptar su modus operandi según sus objetivos y evadir la detección durante períodos prolongados.