La Agencia de Seguridad de Infraestrutctura y Ciberseguridad (CISA), emitió hoy un aviso de seguridad en el que advierte sobre una ola de ataques llevados a cabo por grupos de piratería afiliados al Ministerio de Seguridad del Estado de China (MSS).

CISA asegura que durante el año pasado, los hackers chinos han escaneado las redes del gobierno de Estados Unidos en busca de la presencia de dispositivos de red populares y luego utilizaron exploits para vulnerabilidades recientemente reveladas para afianzarse en redes sensibles.

La lista de dispositivos objetivo incluye equilibradores de carga F5 Big-IP, dispositivos Citrix y Pulse Secure VPN, además de servidores de correo electrónico Microsoft Exchange.

Para cada uno de estos dispositivos, se revelaron públicamente vulnerabilidades importantes durante los últimos 12 meses, como CVE-2020-5902, CVE-2019-19781, CVE-2019-11510 y CVE-2020-0688, respectivamente.

Según una tabla que resume la actividad china dirigida a estos dispositivos publicada este lunes por CISA, algunos ataques han tenido éxito y permitieron a los hackers vulnerar redes federales.

Algunos de los ataques no son nuevos realmente, ya que el año pasado, se informó que los hackers chinos patrocinados por el estado, se estaban dirigiendo a los servidores VPN Pulse Secure y Fortinet a menos de un mes de haberse hecho públicas las vulnerabilidades.

Además, los hackers chinos no son los únicos que se dirigen a estos dispositivos de red en particular. Los dispositivos enumerados anteriormente también han sido atacados por actores estatales iraníes, según un informe del sector privado de seguridad cibernética y una alerta de seguridad cibernética publicada por el FBI el mes pasado.

Un grupo iraní comprometió masivamente este tipo de dispositivos y luego proporcionó acceso a otros grupos iraníes, lo que les permite seleccionar las redes que quieren

comprometer para las operaciones de recopilación de inteligencia. Los dispositivos comprometidos que no fueron seleccionados, se pusieron a la venta en foros de piratería, según un informe de Crowdstrike.

La alerta de CISA también advierte al sector privado y agencias gubernamentales de Estados Unidos, que apliquen parches a los dispositivos F5, Citrix, Pulse Secure y Microsoft Exchange. Sin embargo, la alerta también advierte que los hackers chinos están empleando un amplio espectro de métodos de intrusión.

Estos incluyen el uso de correos electrónicos de spear-phishing, un ataque clásico empleado por actores estatales chinos, y el uso de ataques de fuerza bruta que aprovechan las credenciales débiles o predeterminadas.

Una vez que los piratas informáticos chinos están dentro de las redes específicas, también implementan herramientas comerciales y de código abierto para moverse lateralmente a través de las redes y filtrar datos. Esto incluye el uso de herramientas legítimas de prueba de penetración como Cobalt Strike y Mimikatz.

Cuando los ataques apuntan a sistemas web públicos, como VPN, servidores web y de correo electrónico, CISA dijo que por lo general, detectaba a los hackers chinos implementando el shell web China Chopper, una herramienta común que han utilizado por casi diez años.

Los funcionarios de CISA recomiendan que los equipos de seguridad de empresas privadas y del sector privado y agencias gubernamentales lean su informe, tomen nota de las tácticas, técnicas y procedimientos (TTP) comunes utilizados por los actores estatales chinos, apliquen parches a los dispositivos e implementen reglas de detección.