Entidades ubicadas en Afganistán, Malasia y Pakistán se encuentran en el punto de mira de una campaña de ataque que tiene como objetivo los servidores Microsoft Exchange sin parches como un vector de acceso inicial para implementar el malware ShadowPad.

La compañía rusa de seguridad cibernética Kaspersky, que detectó por primera vez la actividad a mediados de octubre de 2021, la atribuyó a un actor de amenazas de habla china previamente desconocido. Los objetivos incluyen organizaciones en los sectores de telecomunicaciones, manufactura y transporte.

> *«Durante los ataques iniciales, el grupo explotó una vulnerabilidad de MS Exchange para implementar el malware ShadowPad y se infiltró en los sistemas de automatización de edificios de una de las víctimas. Al tomar el control de estos sistemas, el atacante puede llegar a otros sistemas aún más sensibles de la organización atacada»,* dijo la compañía.

ShadowPad, que surgió en 2015 como el sucesor de PlugX, es una plataforma de malware modular de venta privada que ha sido utilizada por muchos actores de espionaje chinos a lo largo de los años.

Aunque su diseño permite a los usuarios implementar de forma remota complementos adicionales que pueden extender su funcionalidad más allá de la recopilación de datos encubierta, lo que hace que ShadowPad sea peligroso es la técnica anti forense y anti análisis incorporada en el malware.

> *«Durante los ataques del actor observado, la puerta trasera ShadowPad se descargó en las computadoras atacadas bajo la apariencia de software legítimo. En muchos casos, el grupo atacante explotó una vulnerabilidad conocida en MS Exchange e ingresó los comandos manualmente, lo que indica la naturaleza altamente específica de sus campañas»,* dijo Kaspersky.

La evidencia sugiere que las intrusiones organizadas por el adversario comenzaron en marzo de 2021, justo cuando las vulnerabilidades de ProxyLogon en los servidores de Exchange se hicieron de conocimiento púbico. Se cree que algunos de los objetivos se violaron al explotar CVE-2021-26855, una vulnerabilidad de falsificación de solicitud del lado del servidor (SSRF) en el servidor de correo.

Además de implementar ShadowPad como «mscoree.dll», un componente auténtico de Microosft .NET Framework, los ataques también involucraron el uso de Cobalt Strike, una variante de PlugX llamada THOR y shells web para acceso remoto.

Aunque se desconocen los objetivos finales de la campaña, se cree que los atacantes están interesados en recopilar información de inteligencia a largo plazo.

> *«Los sistemas de automatización de edificios son objetivos raros para los actores de amenazas avanzados. Sin embargo, esos sistemas pueden ser una fuente valiosa de información altamente confidencial y pueden proporcionar a los atacantes una backdoor a otras áreas de infraestructuras más seguras»,* dijo Kirill Kruglov, investigador de Kaspersky ICS CERT.