Una entidad gubernamental no identificada asociada con los Emiratos Árabes Unidos (EAU), fue atacada por un probable actor de amenazas iraní para violar el Microsoft Exchange Server de la víctima con una puerta trasera *«simple pero efectiva»* denominada PowerExchange.

Según un nuevo informe de Fortinet FortiGuard Labs, la intrusión se basó en el phishing de correo electrónico como vía de acceso inicial, lo que condujo a la ejecución de un ejecutable .NET contenido con un archivo adjunto ZIP.

El binario, que se hace pasar por un documento PDF, funciona como un cuentagotas para ejecutar la carga útil final, que después inicia la backdoor.

PowerExchange, escrito en PowerShell, emplea archivos de texto adjuntos a correos electrónicos para la comunicación de comando y control (C2). Permite que el hacker ejecute cargas útiles arbitrarias y cargue y descargue archivos desde y hacia el sistema.

El implante personalizado logra esto haciendo uso de la API de Exchange Web Services (EWS) para conectarse al Exchange Server de la víctima y usa un buzón en el servidor para enviar y recibir comandos codificados de su operador.

> *«Se puede acceder al Exchange Server desde Internet, lo que ahorra la comunicación C2 a servidores externos desde los dispositivos de las organizaciones. También actúa como un proxy para que el atacante se enmascare»,* dijeron los investigadores de Fortinet.

Actualmente no se sabe cómo el actor de amenazas logró obtener las credenciales de dominio para conectarse al servidor Exchange de destino.

La investigación de Fortinet también descubrió servidores de Exchange que tenían una backdoor con varios shells web, uno de los cuales se llama ExchangeLeech (también conocido como System.Web.ServiceAuthentication.dll), para lograr un acceso remoto

persistente y robar las credenciales de los usuarios.

Se sospecha que PowerExchange es una versión mejorada de TriFive, que fue usada anteriormente por el grupo de hackers APT34 (también conocido como OilRig) en intrusiones contra organizaciones gubernamentales en Kuwait.

Además, la comunicación por medio de servidores Exchange orientados a Internet es una táctica probada y comprobada adoptada por los actores de OilRig, como se observó en el caso de Karkoff y MrPerfectionManager.

> *«Usar el servidor Exchange de la víctima para el canal C2 permite que la puerta trasera se mezcle con el tráfico benigno, lo que garantiza que el atacante pueda evitar fácilmente casi todas las detecciones y remediaciones basadas en la red dentro y fuera de la infraestructura de la organización objetivo»,* dijeron los investigadores.