Hackers del gobierno iraní se hicieron pasar por periodistas para llegar a sus objetivos a través de LinkedIn y llamadas de WhatsApp para ganar su confianza, antes de compartir enlaces a páginas web de phishing y archivos infectados con malware.

Los ataques ocurrieron en julio y agosto de 2020, según la compañía de seguridad cibernética israelí ClearSky, que publicó hoy un informe detallado sobre esta campaña.

Los hackers son miembros del grupo iraní CharmingKitten, también conocido como APT35, NewsBeef, Newscaster o Ajax, según Ohad Zaidenberg, investigador principal de inteligencia cibernética de ClearSky.

Zaidenberg afirma que la campaña reciente se dirigió a expertos académicos, activistas de derechos humanos y periodistas especializados en asuntos iraníes.

El investigador de ClearSky afirma que los hackers se comunicaron con las víctimas primero a través de mensajes de LinkedIn, donde se hicieron pasar por periodistas de habla persa, que trabajaban para la empresa de radiodifusión alemana, Deutsche Welle, y la revista israelí Jewish Journal.

Después de hacer contacto, los atacantes intentaría establecer una llamada de WhatsApp con el objetivo y discutir los asuntos iraníes para ganarse la confianza del objetivo.

Después de la llamada inicial, las víctimas eventualmente recibirían un enlace a un dominio de Deutsche Welle comprometido, que albergaba una página de phishing o un archivo ZIP con malware capaz de obtener sus credenciales.

Zaidenberg asegura que la reciente operación del grupo es una escalada de otros ataques realizados a fines de 2019 y principios de 2020, cuando el mismo grupo también se hizo pasar por periodistas de Wall Street Journal.

Sin embargo, en ataques anteriores, ChamingKitten utilizó correos electrónicos y SMS para comunicarse con las víctimas, pero nunca llamó a sus objetivos.

> *«Este TTP (técnica, táctica, procedimiento) es poco común y pone en peligro la identidad falsa de los atacantes»*, dijo Zaidenberg en el informe de ClearSky.
>
> *«sin embargo, si los atacantes han superado con éxito el obstáculo telefónico, pueden ganar más confianza de la víctima, en comparación con un mensaje de correo electrónico»*, agregó.

También dijo que las tácticas que utilizó el grupo de hackers no fueron originales. Los hackers norcoreanos han estado utilizando esta técnica en particular por años, además de organizar entrevistas de trabajo falsas en Skype para violar la red de cajeros automáticos de Chile, o establecer entrevistas falsas por teléfono o llamadas de WhatsApp con empleados que trabajan en defensa.