Un error de OPSEC cometido por un hacker iraní, dejó al descubierto el funcionamiento interno del grupo de piratas informáticos al proporcionar una visión de la *«mirada detrás de escena de sus métodos».*

Los Servicios de Inteligencia de Respuesta a Incidentes (IRIS) X-Force de IBM, obtuvieron casi cinco horas de grabaciones de video del grupo patrocinado por el estado, al que llama ITG18, también conocido como Charming Kitten, Phosphorous o APT35, que utiliza para capacitar a sus operadores.

Algunas de las víctimas en los videos incluyeron relatos personales del personal de la marina de Estados Unidos y Grecia, además de intentos fallidos de phishing dirigidos contra funcionarios del departamento de estado de Estados Unidos y un filántropo iraní-estadounidense no identificado.

> *«Algunos de los videos mostraban al operador administrando cuentas creadas por el adversario, mientras que otros mostraban al operador probando el acceso y extrayendo datos de cuentas previamente comprometidas»*, dijeron los investigadores.

Los investigadores de IBM también dijeron que encontraron los videos en un servidor de nube privada virtual, que quedó expuesto debido a una configuración incorrecta de seguridad. El servidor, que también encontró varios dominios ITG18 a inicios del año, contenía más de 40 Gb de datos.

Los archivos de video descubiertos muestran que ITG18 tenía acceso al correo electrónico de los objetivos y las credenciales de las redes sociales obtenidas por medio de la suplantación de identidad, utilizando la información para iniciar sesión en las cuentas, eliminar notificaciones de inicios de sesión sospechosos para no alertar a las víctimas y filtrar contactos, fotos y documentos de Google Drive.

> *«El operador también pudo iniciar sesión en Google Takeout de las víctimas, lo que permite a un usuario exportar contenido de su cuenta de Google, para incluir el historial de ubicaciones, la información de Chrome y los dispositivos Android asociados»*, agregaron los investigadores.

Además, los videos capturados con la herramienta de grabación Bandicam, también muestran que los actores detrás de la operación conectaron las credenciales de las víctimas al software de colaboración por correo electrónico de Zimbra con la intención de monitorear y administrar las cuentas de correo electrónico comprometidas.

Fuera de las cuentas de correo electrónico, los investigadores afirmaron que encontraron a los atacantes empleando una gran lista de nombres de usuario y contraseñas comprometidas contra al menos 75 sitios web diferentes que van desde bancos hasta transmisión de música y video.

Otros videoclips muestran al grupo ITG18 aprovechando cuentas ficticias de Yahoo, que incluyen un número de teléfono con el código de país de Irán (+98), que las utiliza para enviar correos electrónicos de phishing, algunos de los cuales fueron recuperados, lo que sugiere que los correos electrónicos no llegaron a la bandeja de entrada de la víctima.

> *«Durante los videos en los que el operador validaba las credenciales de las víctimas, si el operador se autenticaba con éxito en un sitio configurado con autenticación multifactor (MFA), se detenían y pasaban a otro conjunto de credenciales sin obtener acceso»*, dijeron los investigadores.

ITG18 tiene un gran historia de ataques al personal militar, diplomático y gubernamental de Estados Unidos y Medio Oriente, para la recolección de inteligencia y espionaje para servir a intereses geopolíticos de Irán.

> *«El compromiso de los archivos personales de los miembros de la Armada griega y estadounidense podría respaldar las operaciones de espionaje relacionadas con numerosos procedimientos que ocurren en el Golfo de Omán y el Golfo Arábigo. El grupo ha mostrado persistencia en sus operaciones y la creación constante de nueva infraestructura a pesar de las múltiples revelaciones públicas y la amplia información sobre su actividad»*, agregaron los investigadores de IBM X-Force.