El grupo de hackers respaldado por el gobierno iraní, conocido como Charming Kitten, agregó una nueva herramienta a su arsenal de malware que le permite recuperar datos de usuarios de cuentas de Gmail, Yahoo! y Microsoft Outlook.

Nombrado como HYPERSCRAPE por Google Threat Analysis Group (TAG), el software malicioso en desarrollo activo se usó contra menos de dos docenas de cuentas en Irán, y la muestra más antigua conocida data de 2020. La herramienta se descubrió por primera vez en diciembre de 2021.

Charmin Kitten, una prolífica amenaza persistente avanzada (APT), está asociada con el Cuerpo de la Guardia Revolucionaria Islámica (IRGC) de Irán, y tiene un historial de espionaje alineado con los intereses del gobierno.

Rastreados como APT35, Cobalt Illusion, ITG18, Phosphorus, TA453 y Yellow Garuda, los elementos del grupo también llevaron a cabo ataques de ransomware, lo que sugiere que los motivos del atacante son tanto el espionaje como financieros.

> *«HYPERSCRAPE requiere que las credenciales de la cuenta de la víctima se ejecuten usando una sesión de usuario válida y autenticada que el atacante haya secuestrado, o las credenciales que el atacante ya haya adquirido»,* dijo Ajax Bash, investigador de Google TAG.

Escrita en .NET y diseñada para ejecutarse en la máquina Windows del atacante, la herramienta viene con funciones para descargar y exfiltrar el contenido de la bandeja de entrada del correo electrónico de la víctima, además de eliminar los correos electrónicos de seguridad enviados desde Google para alertar el objetivo de cualquier inicio de sesión sospechoso.

Si un mensaje no se leyó originalmente, la herramienta lo marca como no leído después de abrirlo y descargarlo como un archivo *«.eml».* Además, se cree que las versiones anteriores de HYPERSCRAPE incluían una opción para solicitar datos de Google Takeout, una función

que permite a los usuarios exportar sus datos a un archivo de almacenamiento descargable.

Los hallazgos siguen al reciente descubrimiento de una herramienta «*grabber*» de Telegram, basada en C++ por parte de PwC utilizada contra objetivos nacionales para obtener acceso a mensajes y contactos de Telegram de cuentas específicas.

Anteriormente, se vio al grupo implementando un software de vigilancia de Android personalizado llamado LittleLooter, un implante rico en funciones capaz de recopilar información confidencial almacenada en los dispositivos comprometidos, así como grabar audio, video y llamadas.

> *«Al igual que muchas de sus herramientas, HYPERSCRAPE no se destaca por su sofisticación técnica, sino por su eficacia para lograr los objetivos de Charming Kitten»,* dijo Bash.

Desde entonces, las cuentas afectadas se han vuelto a asegurar y se notificó a las víctimas.