Se ha descubierto un nuevo actor de amenazas iraní que explota una falla crítica ya corregida en la plataforma Microsoft Windows MSHTML para apuntar a las víctimas que hablan farsi, con un nuevo ladrón de información basado en PowerShell diseñado para recolectar detalles extensos de las máquinas infectadas.

> *«El ladrón es un script de PowerShell, breve y con potentes capacidades de recopilación; en solo 150~ líneas, proporciona al adversario mucha información crítica, incluidas capturas de pantalla, archivos de Telegram, recopilación de documentos y datos extensos sobre el entorno de la víctima»*, dijo Tomer Bar, investigador de SafeBreach Labs.

Casi la mitad de los objetivos son de Estados Unidos, y la compañía de seguridad cibernética dijo que los ataques probablemente estén dirigidos a *«iraníes que viven en el extranjero y podrían ser vistos como una amenaza para el régimen islámico de Irán».*

Esta campaña de phishing comenzó en julio de 2021, e implicó la explotación la vulnerabilidad CVE-2021-40444, una falla de ejecución remota de código que podría explotarse utilizando documentos de Microsoft Office especialmente diseñados.

Microsoft corrigió la vulnerabilidad en septiembre de 2021, semanas después de que aparecieran informes de explotación activa en la naturaleza.

> *«Un atacante podría crear un control ActiveX malicioso para ser utilizado por un documento de Microsoft Office que aloja el motor de procesamiento del navegador. El atacante tendría que convencer al usuario para que abra el documento malicioso. Los usuarios cuyas cuentas estén configuradas para tener menos derechos de usuario en el sistema podrían verse menos afectados que los usuarios que operan*

> *con derechos de usuario administrativos»,* dijo Microsoft.

La secuencia del ataque descrita por SafeBreach comienza con los objetivos que reciben un correo electrónico de spear-phishing, que viene con un documento de Word como archivo adjunto. Al abrir dicho archivo, se activa el exploit para CVE-2021-40444, lo que da como resultado la ejecución de un script de PowerShell denominado *«PowerShortShell»*, que es capaz de almacenar información confidencial y transmitirla a un servidor de comando y control (C2).

Aunque se observaron infecciones relacionadas con el despliegue del ladrón de información el 15 de septiembre, un día después de que Microsoft emitiera parcheas para la vulnerabilidad, el servidor C2 también se utilizó para recolectar las credenciales de Gmail e Instagram de las víctimas como parte de dos campañas de phishing organizadas por el mismo adversario en julio de 2021.

Este desarrollo es el último de una serie de ataques que han sacado provecho del fallo del motor MSHTML, siendo Microsoft quien reveló previamente una campaña de phishing dirigida que abusa de la vulnerabilidad como parte de una campaña de acceso inicial para distribuir cargadores personalizados de Cobalt Strike Beacon.