Un actor de amenazas no identificado ha estado explotando una vulnerabilidad de día cero recientemente parcheada en el navegador web Internet Explorer, con el fin de ofrecer un troyano de acceso remoto (RAT) basado en VBA capaz de acceder a archivos almacenados en sistemas Windows comprometidos y descargar y ejecutar cargas útiles maliciosas como parte de una campaña *«inusual».*

La puerta trasera se distribuye a través de un documento señuelo llamado *«Manifest.docx»*, que carga el código de explotación para la vulnerabilidad desde una plantilla incrustada, que a su vez, ejecuta shellcode para implementar el RAT, según la compañía de seguridad cibernética Malwarebytes, que detectó el Word sospechoso el 21 de julio de 2021.

El documento con malware asegura ser un *«Manifiesto de los habitantes de Crimea»*, que pide a los ciudadanos que se opongan al presidente ruso Vladimir Putin y «creen una plataforma unificada llamada *«Resistencia del Pueblo».*

La vulnerabilidad de Internet Explorer, rastreada como CVE-2021-26411, es notable por el hecho de que fue abusada por el Grupo Lazarus, respaldado por Corea del Norte, para apuntar a investigadores de seguridad que trabajan en investigación y desarrollo de vulnerabilidades.

A inicios de febrero, la compañía de seguridad cibernética de Corea del Sur, ENKI, reveló que el colectivo de hackers alineado con el estado había hecho un intento fallido de apuntar a sus investigadores de seguridad con archivos MHTML maliciosos que, al abrirse, descargan dos cargas útiles de un servidor remoto, uno de los cuales contenía un día cero contra Internet Explorer. Microsoft abordó el problema como parte de sus actualizaciones de Patch Tuesday de marzo.

El exploit de Internet Explorer es una de las dos formas que se utilizan para implementar el RAT, y el otro método se basa en un componente de ingeniería social que implica descargar y ejecutar una plantilla de macro armamentizada remota que contiene el implante. Independientemente de la cadena de infección, es probable que el uso de vectores de doble ataque sea un intento por aumentar la probabilidad de encontrar un camino hacia las

máquinas objetivo.

> *«Aunque ambas técnicas se basan en la inyección de plantillas para eliminar un troyano de acceso remoto con todas las funciones, el exploit IE (CVE-2021-26411) utilizado anteriormente por Lazarus APT es un descubrimiento inusual. Los atacantes pueden haber querido combinar la ingeniería social y la explotación para maximizar sus posibilidades de infectar objetivos»,* dijo Hossein Jazi, investigador de Malwarebytes.

Además de recopilar metadatos del sistema, VBA RAT está orquestado para identificar los productos antivirus que se ejecutan en el host infectado y ejecutar los comandos que recibe un servidor controlado por el atacante, incluida la lectura, eliminación y descarga de archivos arbitrarios, y exfiltrar los resultados de esos comandos al servidor.

Malwarebytes también descubrió un panel basado en PHP apodado «Ekipa», que utiliza el adversario para rastrear a las víctimas y ver información sobre el modus operandi que condujo a la infracción exitosa, destacando la explotación exitosa usando el día cero de IE y la ejecución del RAT.

> *«A medida que continúa el conflicto entre Rusia y Ucrania por Crimea, los ataques cibernéticos también aumentaron. El documento señuelo contiene un manifiesto que muestra un posible motivo (Crimea) y un objetivo (individuos rusos y prorrusos) detrás de este* ataque. Sin embargo, también podría haber sido utilizado como una bandera falsa», dijo Jazi.