En otro indicador más de cómo los grupos de hackers aprovechan rápidamente los eventos mundiales e improvisan sus campañas de ataque para lograr el máximo impacto, se ha descubierto que los actores de amenazas se hacen pasar por Amnistía Internacional para distribuir malware que pretende ser un software de seguridad diseñado para proteger contra el software de vigilancia Pegasus de NSO Group.

> *«Los adversarios crearon un sitio web falso que se parece al de Amnistía Internacional, una organización no gubernamental centrada en los derechos humanos, y apunta a una herramienta antivirus prometida para protegerse contra la herramienta Pegasus de NSO Group. Sin embargo, la descarga instala el malware Sarwent poco conocido»*, dijeron los investigadores de Cisco Talos.

Los países más afectados por la campaña incluyen Reino Unido, Estados Unidos, Rusia, India, Ucrania, República Checa, Rumania y Colombia. Aunque no está claro cómo se engaña a las víctimas para que visiten el sitio web falso de Amnistía Internacional, la compañía de seguridad cibernética supuso que los ataques podrían estar dirigidos a usuarios que pueden estar buscando específicamente protección contra esta amenaza.

El desarrollo se produce inmediatamente después de una investigación explosiva en julio de 2021, que reveló un abuso generalizado del *«software espía de grado militar»* de la compañía israelí Pegasus, para facilitar las violaciones de derechos humanos al vigilar a jefes de estado, activistas, periodistas y abogados de todo el mundo. Desde entonces, la ONG también lanzó un kit de herramientas de verificación móvil (MVT) para ayudar a las personas a escanear sus dispositivos iPhone y Android en busca de evidencia de compromiso.

Además de hacer uso de trucos de ingeniería social al diseñar un sitio web fraudulento con una apariencia idéntica a la del portal legítimo de Amnistía Internacional, el modus operandi tiene como objetivo engañar al visitante para que descargue un *«software Anti Pegasus de Amnistía»* bajo la apariencia de una herramienta antivirus que incluye capacidades para permitir que el actor malintencionado encuentre un camino remoto hacia la máquina comprometida y exfiltre información confidencial, como las credenciales de inicio de sesión.

La muestra de Sarwent utilizada en la campaña de bajo volumen es una variante altamente personalizada codificada en Delphi, y es capaz de permitir el acceso al escritorio remoto a través de VNC o RDP y ejecutar la línea de comandos o instrucciones de PowerShell recibidas de un dominio controlado por un atacante, cuyos resultados se envían de vuelta al servidor.

Talos atribuyó las infecciones con gran confianza a un actor de habla rusa que se encuentra en el país y es conocido por los crecientes ataques que involucran la puerta trasera de Sarwent desde al menos enero de 2021 en una variedad de víctimas, y dijo que el nivel de modificaciones realizadas al supuesto antivirus es probable evidencia de que *«el operador tiene acceso al código fuente del malware Sarwent».*

> *«La campaña está dirigida a personas que podrían estar preocupadas de que sean el objetivo del software espía Pegasus. Esta focalización plantea problemas de posible participación estatal, pero no hay información suficiente para tomar una determinación sobre qué estado o nación. Es posible que este sea simplemente un factor motivado financieramente que busca aprovechar los titulares para obtener un nuevo acceso»,* dijeron los investigadores.