Investigadores de seguridad cibernética descubrieron hoy nuevos detalles sobre ataques de pozos de agua contra la comunidad kurda en Siria y Turquía con fines de vigilancia y exfiltración de inteligencia.

La amenaza persistente avanzada detrás de la operación, denominada StrongPity, se ha modificado con nuevas tácticas para controlar máquinas comprometidas, dijo la compañía de seguridad cibernética Bitdefender en un informe.

> *«Utilizando tácticas de abrevaderos para infectar selectivamente a las víctimas y desplegando una infraestructura de C&C de tres niveles para frustrar las investigaciones forenses, el grupo APT aprovechó herramientas populares troyanizadas, como archivadores, aplicaciones de recuperación de archivos, aplicaciones de conexiones remotas, utilidades e incluso software de seguridad, para cubrir una amplia gama de opciones que las víctimas específicas podrían buscar»*, dijeron los investigadores.

Con las marcas de tiempo de las muestras de malware analizadas utilizadas en la campaña que coincidieron con la ofensiva turca en el noreste de Siria, bajo el nombre en código de Operation Peace Spring en octubre pasado, Bitdefender dijo que los ataques podrían haber sido motivados políticamente.

StrongPity o Promethium, fue informado por primera vez públicamente en octubre de 2016 luego de ataques contra usuarios en Bélgica e Italia, que utilizaron abrevaderos para entregar versiones maliciosas del software de cifrado de archivos WinRAR y TrueCrypt.

Desde entonces, la APT se relaciona con una operación de 2018 que abusó de la red de Türk Telekom para redirigir a cientos de usuarios en Turquía y Siria a versiones maliciosas de StrongPity de software auténtico.

Por lo tanto, cuando los usuarios objetivo intentan descargar una aplicación legítima en el sitio web oficial, se lleva a cabo un ataque de pozo de agua o una redirección HTTP para

comprometer los sistemas.

En julio pasado, AT&T Alien Labs encontró evidencia de una nueva campaña de software espía que explotó las versiones troyanizadas del software de administración de enrutadores WinBox y el archivador WinRAR para instalar StrongPity y comunicarse con la infraestructura del adversario.

El nuevo método de ataque identificado por Bitdefender sigue siendo el mismo: atacar a las víctimas en Turquía y Siria mediante una lista de IP definida aprovechando instaladores manipulados, como McAfee Security Scan Plus, Recuva, TeamViewer, WhatsApp y CCleaner de Piriform, alojados en agregados y compartidores de software localizados.

> *«Curiosamente, todos los archivos investigados relacionados con las aplicaciones contaminadas parecen haber sido compilados de lunes a viernes, durante las horas normales de trabajo de 9 a 6 UTC +2. Esto fortalece la idea de que StrongPity podría ser un equipo de desarrolladores patrocinado y organizado al que se le paga por entregar ciertos proyectos»*, agregaron los investigadores.

Una vez que se descarga y ejecuta el cuentagotas de malware, se instala la puerta trasera, que establece la comunicación con un servidor de comando y control para la filtración de documentos y para recuperar comandos a ejecutar.

También implementa un componente *«File Searcher»* en la máquina de la víctima que recorre cada unidad y busca archivos con extensiones específicas.

Este archivo ZIP se divide en múltiples archivos cifrados «.stf» ocultos, se envían al servidor de C&C y finalmente se eliminan del disco para cubrir cualquier pista de la exfiltración.

Aunque Siria y Turquía pueden ser los objetivos recurrentes, el actor de la amenaza detrás de

StrongPity parece estar expandiendo su operación para infectar a usuarios en Colombia, India, Canadá y Vietnam, utilizando versiones infectadas de Firefox, VPN PRO, DriverPack y 5kPlayer.

Por otro lado, bajo el nombre de StrongPity3, los investigadores de Cisco Talos describieron este lunes un conjunto de herramientas de malware en evolución que emplea un módulo llamado *«winprint32.exe»* para iniciar la búsqueda de documentos y transmitir los archivos recopilados. Además, el falso instalador de Firefox también comprueba si está instalado el software antivirus ESET o BitDefender antes de eliminar el malware.

> *«Estas características pueden interpretarse como signos de que este actor de amenazas podría de hecho, ser parte de una operación de contratación de servicios empresariales. Creemos que esto tiene el sello distintivo de una solución empaquetada profesionalmente debido a que la similitud de cada pieza de malware es extremadamente similar pero se usa en diferentes objetivos con cambios menores»,* dijeron los investigadores.