Un análisis de 18 meses de duración de la operación de ransomware PYSA, reveló que el grupo del cribercrimen siguió un ciclo de desarrollo de software de cinco etapas a partir de agosto de 2020, en el que los autores del malware priorizaron las características para mejorar la eficiencia de sus flujos de trabajo.

Esto incluía una herramienta fácil de usar como un motor de búsqueda de texto completo para facilitar la extracción de metadatos y permitir que los atacantes encontraran y accedieran a la información de las víctimas de una forma rápida.

> *«Se sabe que el grupo investiga cuidadosamente objetivos de alto valor antes de lanzar sus ataques, comprometiendo los sistemas empresariales y obligando a las organizaciones a pagar grandes rescates para restaurar sus datos»,* dijo la compañía de ciberseguridad PRODAFT.

PYSA, abreviatura de *«Protect Your System, Amigo»,* y sucesor del ransomware Mespinoza, se observó por primera vez en diciembre de 2019 y se convirtió en la tercera cepa de ransomware más frecuente detectada durante el cuarto trimestre de 2021.

Desde septiembre de 2020, se cree que el grupo de ciberdelincuentes extrajo información confidencial perteneciente a hasta 747 víctimas hasta que sus servidores se desconectaron a inicios de enero.

La mayoría de sus víctimas se encuentran en Estados Unidos y Europa, y el grupo ataca principalmente a los sectores gubernamental, sanitario y educativo.

«Estados Unidos fue el país más afectado, representando el 59.2% de todos los eventos de PYSA informados, seguido del Reino Unido con un 13.1%», dijo Intel 471 en un análisis de los ataques de ransomware registrados entre octubre y diciembre de 2021.

Se sabe que PYSA, al igual que otras familias de ransomware, sigue el enfoque de *«caza mayor»* de la doble extorsión, que implica la publicación de información robada si la víctima

se niega a cumplir con las demandas del grupo.

Cada archivo elegible se cifra y se le otorga una extensión «.pysa», cuya decodificación requiere la clave privada RSA que solo se puede obtener luego de pagar el rescate. Se dice que casi el 58% de las víctimas de PYSA han realizado pagos digitales.

PRODAFT, que pudo ubicar una carpeta .git disponible públicamente administrada por operadores de PYSA, identificó a uno de los autores del proyecto como *«dodo@mail.pcc»,* un actor de amenazas que se cree que se encuentra en un país que observa el horario de verano basado en el historial de confirmación.

Al menos 11 cuentas, la mayoría de las cuales se crearon el 8 de enero de 2021, están a cargo de la operación general, reveló la investigación. De este modo, cuatro de estas cuentas, denominadas t1, t3, t4 y t5, representan más del 90% de la actividad en el panel de administración del grupo.

Otros errores de seguridad operacional cometidos por los miembros del grupo también permitieron identificar un servicio oculto que se ejecuta en la red de anonimato TOR, un proveedor de alojamiento (Snel.com BV) ubicado en los Países Bajos, que ofrece un vistazo a las tácticas del actor.

La infraestructura de PYSA también consta de contenedores dockerizados, que incluyen servidores públicos de fugas, bases de datos y servidores de administración, así como una nube de Amazon S3 para almacenar los archivos cifrados, que ascienden a 31.47 TB.

También se pone en uso un panel de gestión de fugas personalizado para buscar documentos confidenciales en los archivos extraídos de las redes internas de las víctimas antes del cifrado.

Además de usar el sistema de control de versiones Git para administrar los procesos de desarrollo, el panel en sí está codificado en PHP 7.3.12 usando el marco Laravel.

El panel de administración expone una variedad de puntos finales de API que permiten que el sistema enumere archivos, descargue archivos y analice los archivos para la búsqueda de texto completo, que está diseñado para categorizar la información de la víctima robada en categorías ampliar para una fácil recuperación.

> *«El grupo cuenta con el apoyo de desarrolladores competentes que aplican paradigmas operativos modernos al ciclo de desarrollo del grupo. Sugiere un entorno profesional con una división de responsabilidades bien organizada, en lugar de una red suelta de actores de amenazas semiautónomos»*, dijo el investigador.

En todo caso, los hallazgos son otro indicador más de que los grupos de ransomware como PYSA y Conti operan y están estructuradas como compañías de software legítimas, e incluso incluyen un departamento de recursos humanos para reclutar nuevos empleados y un premio al *«empleado del mes»* por abordar problemas desafiantes.