Se ha observado un nuevo troyano de acceso remoto (RAT) basado en JavaScript propagado a través de una campaña de ingeniería social, que emplea técnicas furtivas *«sin archivos»* como parte de sus métodos de detección y evasión para eludir el descubrimiento y el análisis.

Nombrado como DarkWatchman por investigadores del Equipo de Contrainteligencia Adversario (PACT) de Prevailion, el malware utiliza un algoritmo de generación de dominio resistente (DGA) para identificar su infraestructura de comando y control (C2), y utiliza el Registro de Windows para todas sus operaciones de almacenamiento, lo que permite evitar los motores antivirus.

> *«EL RAT utiliza métodos novedosos para la persistencia sin archivos, la actividad en el sistema y las capacidades dinámicas de tiempo de ejecución como la autoactualización y la recompilación. Representa una evolución en las técnicas de malware sin archivos, ya que utiliza el registro para casi todo el almacenamiento temporal y permanente, y por lo tanto, nunca escribe nada en el disco, lo que le permite operar por debajo o alrededor del umbral de detección de la mayoría de las herramientas de seguridad»*, dijeron los investigadores Matt Stafford y Sherman Smith.

Prevailion dijo que una organización de tamaño empresarial sin nombre en Rusia, fue una de las víctimas objetivo, con una serie de artefactos de malware identificados a partir del 12 de noviembre de 2021. Debido a sus características de puerta trasera y persistencia, el equipo de PACT evaluó que DarkWatchman podría ser un acceso inicial y herramienta de reconocimiento para su uso por grupos de ransomware.

Una consecuencia interesante de este novedoso desarrollo es que elimina completamente la necesidad de que los operadores de ransomware recluten afiliados, que normalmente se encargan de eliminar el malware de bloqueo de archivos y gestionar la exfiltración de archivos. El uso de DarkWatchman como preludio para las implementaciones de ransomware también equipa a los desarrolladores principales del ransomware con una mejor supervisión

de la operación más allá de la negociación de rescates.

Distribuido por medio de correos electrónicos de spear-phishing, que se hacen pasar por *«Notificación de caducidad de almacenamiento gratuito»* para un envío entregado por la compañía de envío rusa Pony Express, DarkWatchman proporciona una puerta de enlace sigilosa para futuras actividades maliciosas. Los correos electrónicos vienen adjuntos con una supuesta factura en forma de archivo ZIP que, a su vez, contiene la carga útil necesaria para infectar el sistema Windows.

El nuevo RAT es un RAT de JavaScript sin archivos y un registrador de teclas basado en C#, el último de los cuales se almacena en el registro para evitar la detección. Ambos componentes también son extremadamente ligeros. El código JavaScript malicioso solo ocupa unos 32 kb, mientras que el registrados de teclas apenas registra 8.5 kb.

> *«El almacenamiento del binario en el registro como texto codificado significa que DarkWatchman es persistente, pero su ejecutable nunca se escribe (permanentemente) en el disco; también significa que los operadores de DarkWatchman pueden actualizar (o reemplazar) el malware cada vez que se ejecuta»*, dijeron los investigadores.

Una vez instalado, DarkWatchman puede ejecutar binarios arbitrarios, cargar archivos DLL, ejecutar código JavaScript y comandos de PowerShell, cargar archivos a un servidor remoto, actualizar e incluso desinstalar el RAT y el registrador de teclas de la máquina comprometida. La rutina de JavaScript también es responsable de establecer la persistencia mediante la creación de una tarea programada que ejecuta el malware en cada inicio de sesión de usuario.

> *«El registrador de teclas en sí no se comunica con el C2 ni escribe en el disco. En su lugar, escribe su registro de teclas en una clave de registro que utiliza como búfer. Durante su funcionamiento, el RAT raspa y borra este búfer antes de transmitir las*

> *pulsaciones de teclado registradas al servidor C2»,* agregaron los investigadores.

DarkWatchman aún no se atribuye a un grupo de hackers, pero Prevailion caracterizó al equipo como un *«actor de amenazas capaz»,* además de señalar el objetivo exclusivo del malware de las víctimas ubicadas en Rusia y los errores tipográficos y faltas de ortografía que se identificaron en las muestras de código fuente, lo que plantea la posibilidad de que los operadores no sean hablantes nativos de inglés.

> *«Parece que los autores de DarkWatchman identificaron y aprovecharon la complejidad y opacidad del Registro de Windows para trabajar por debajo o alrededor del umbral de detección de herramientas de seguridad y analistas por igual. Los cambios en el registro son comunes y puede ser difícil identificar qué cambios son anómalos o están fuera del alcance de las funciones normales del sistema operativo y del software»,* finalizaron los investigadores.