Lazarous Group, el famoso grupo de hackers con vínculos con el régimen norcoreano, está detrás de un nuevo marco de malware multiplataforma, con el objetivo de infiltrarse en entidades corporativas de todo el mundo, robar bases de datos de clientes y distribuir ransomware.

El marco de malware MATA, llamado así por la referencia de los autores a la infraestructura como «*MataNet*», capaz de apuntar a los sistemas operativos Windows, Linux y MacOS, cuenta con una amplia gama de características diseñadas para llevar a cabo una variedad de actividades maliciosas en las máquinas infectadas.

La campaña MATA comenzó a inicios de abril de 2018, con la victimología rastreada a compañías no identificadas en el desarrollo de software, comercio electrónico y sectores de proveedores de servicios de Internet ubicados en Polonia, Alemania, Turquía, Corea, Japón e India, según dijo Kaspersky este miércoles.

El informe ofrece una versión digital del marco MATA, al mismo tiempo que se basa en evidencia previa recopilada por investigadores de Netlab 360, Jamf y Malwarebytes en los últimos ocho meses.

En diciembre pasado, Netlab360 reveló un troyano de administración remota (RAT), completamente funcional llamado Dacls, dirigido a plataformas Linux y Windows, que compartían infraestructura clave operada por Lazarous Group.

Después, en mayo, Jamf y Malwarebytes descubrieron una variante para macOS de Dacls, que se distribuyó por medio de una aplicación de autenticación de dos factores troyanizada.

En el último desarrollo, la versión para Windows de MATA, consiste en un cargador utilizado para activar una carga útil cifrada de la siguiente etapa: un módulo orquestador (lsass.exe), capaz de cargar 15 complementos adicionales al mismo tiempo y ejecutarlos en la memoria.

Los complementos en sí mismos son ricos en funciones, con características que permiten que el malware manipule archivos y procesos del sistema, inyecte archivos DLL y cree un servidor

proxy HTTP.

Los complementos MATA también permiten a los piratas informáticos apuntar a dispositivos de red sin disco basados en Linux, como enrutadores, firewalls o dispositivos IoT, y sistemas macOS al enmascararse como una aplicación 2FA llamada TinkaOTP, que se basa en una aplicación de autenticación de dos factores de código abierto llamada MinaOTP.

Una vez que se implementaron los complementos, los hackers intentaron localizar las bases de datos de la empresa comprometida y ejecutar varias consultas de la base de datos para obtener los detalles del cliente.

Aún no está muy claro si tuvieron éxito en sus intento. Además, los investigadores de Kaspersky dijeron que se utilizó MATA para distribuir el ransomware VHD a una víctima anónima.

Kaspersky informó que vinculó MATA con el Grupo Lazarus basándose en el formato de nombre de archivo único que se encuentra en el orquestador («c_2910.cls» y «k_3872.csl»), que se ha visto anteriormente en algunas variantes del malware Manuscrypt.

Lazarus Group, patrocinado por el estado, también conocido como Hidden Cobra o APT38, se ha relacionado con muchas ofensivas cibernéticas importantes, como el ataque a Sony Pictures en 2014, el hackeo bancario SWIFT en 2016 y la infección del ransomware WannaCry en 2017.

Recientemente, el grupo agregó el skimming web a su repertorio, apuntando a sitios web de comercio electrónico de Estados Unidos y Europa para plantar skimmers de pago basados en JavaScript.