Diversas empresas dentro del ámbito de las criptomonedas están siendo blanco de una persistente campaña de malware que implica un recién descubierto backdoor para Apple macOS, denominado RustDoor.

La existencia de RustDoor fue inicialmente documentada por Bitdefender la semana pasada, caracterizándolo como un malware basado en Rust con la capacidad de recolectar y cargar archivos, además de recopilar información sobre las máquinas infectadas. Su método de distribución consiste en hacerse pasar por una actualización de Visual Studio.

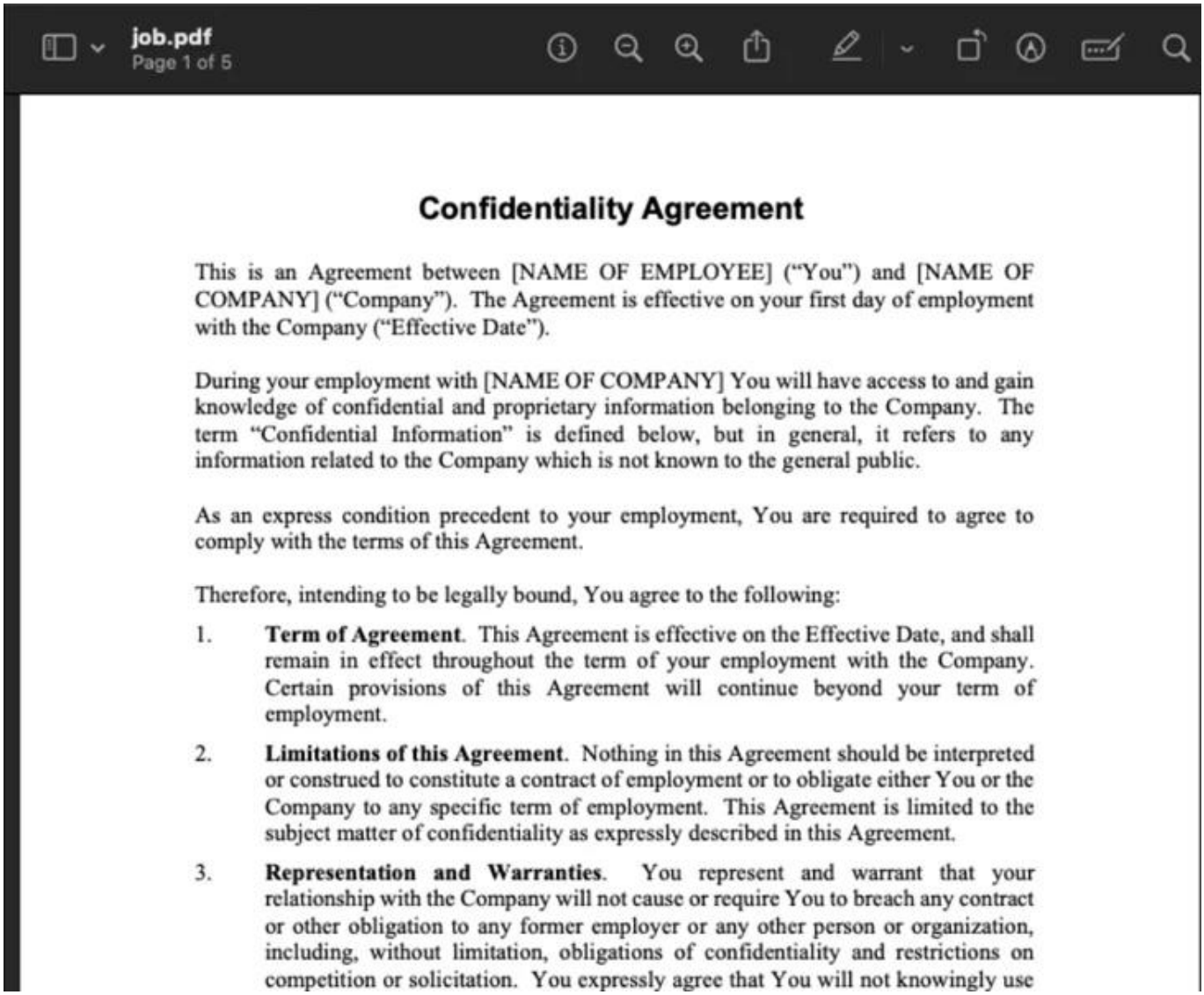
A pesar de que evidencias previas revelaron al menos tres variantes distintas de este backdoor, el mecanismo exacto de propagación inicial permanecía en la oscuridad.

No obstante, la firma de ciberseguridad rumana informó posteriormente que el malware se empleó como parte de un ataque dirigido en lugar de una campaña de distribución masiva. Señalaron que encontraron artefactos adicionales encargados de descargar y ejecutar RustDoor.

> *«Bajo la apariencia de archivos PDF con ofertas laborales, algunos de estos programas de descarga de la primera etapa son en realidad scripts que descargan y ejecutan el malware. Simultáneamente, descargan y abren un archivo PDF inofensivo que se presenta como un acuerdo de confidencialidad»,* indicó Bogdan Botezatu, director de investigación de amenazas y reportes en Bitdefender.

Desde entonces, han surgido tres muestras adicionales de software malicioso que actúan como cargas útiles de la primera etapa, cada una aparentando ser una oferta de trabajo. Estos archivos ZIP preceden a los binarios de RustDoor anteriores por casi un mes.

El nuevo eslabón en la cadena de ataque, es decir, los archivos de archivo («Jobinfo.app.zip» o «Jobinfo.zip»), contienen un sencillo script de shell responsable de adquirir el implante desde un sitio web denominado turkishfurniture[.]blog. También está diseñado para mostrar un inofensivo archivo PDF de distracción («job.pdf») alojado en el mismo sitio.



Bitdefender reportó el descubrimiento de cuatro binarios nuevos basados en Golang que establecen comunicación con un dominio controlado por un actor («sarkerrentacars[.]com»). La función de estos binarios es recopilar información sobre la máquina de la víctima y sus conexiones de red mediante el uso de las utilidades del sistema macOS, system_profiler y networksetup.

Estos binarios, además, tienen la capacidad de extraer detalles sobre el disco utilizando el

comando «diskutil list» y recuperar una extensa lista de parámetros y valores de configuración del kernel mediante el comando «sysctl -a».

Al profundizar en la infraestructura de comando y control (C2), se descubrió un punto final con fugas («/client/bots») que permite obtener información detallada sobre las víctimas actualmente infectadas, incluyendo las marcas de tiempo del registro del host infectado y la última actividad observada.

> Bogdan Botezatu, director de investigación de amenazas y reportes en Bitdefender, comentó: *«Sabemos que hasta ahora hay al menos tres empresas víctimas. Los atacantes parecen dirigirse al personal senior de ingeniería, lo que explica por qué el malware se camufla como una actualización de Visual Studio. Aún estamos investigando para determinar si hay otras empresas comprometidas en este momento».*
>
> *«Las víctimas parecen tener una conexión geográfica; dos de ellas se encuentran en Hong Kong, mientras que la tercera está en Lagos, Nigeria».*

Este desarrollo coincide con la revelación por parte del Servicio de Inteligencia Nacional de Corea del Sur (NIS) de que una organización de TI vinculada a la Oficina No. 39 del Partido de los Trabajadores de Corea del Norte está generando ingresos ilícitos al vender sitios web de apuestas con malware a otros ciberdelincuentes, con el objetivo de robar datos sensibles de apostadores desprevenidos.

La entidad responsable de este esquema de malware como servicio (MaaS) es Gyeongheung (también escrito como Gyonghung), un grupo de 15 miembros con sede en Dandong. Supuestamente, han recibido $5,000 de una organización criminal surcoreana no identificada a cambio de la creación de un sitio web y $3,000 mensuales por el mantenimiento del mismo, según informó la Agencia de Noticias Yonhap.