Los miembros del ya desaparecido grupo de ransomware Conti, pusieron en práctica una nueva variedad de malware desarrollada por hackers probablemente afiliados al grupo de ciberdelincuencia FIN7, lo que indica la colaboración entre los equipos.

El malware, denominado Domino, está diseñado principalmente para facilitar la explotación de seguimiento en sistemas comprometidos, incluyendo la entrega de un ladrón de información menos conocido que se ha anunciado para la venta en la web oscura desde diciembres de 2021.

> *«Los ex miembros del sindicado TrickBot/Conti [...] han estado usando Domino desde al menos finales de febrero de 2023 para entregar el ladrón de información Project Nemesis o backdoors más capaces como Cobal Strike»,* dijo Charlotte Hammond, investigadora de segurida de IBM Security X-Force.

FIN7, también llamado Carbanak e ITG14, es un sindicado cibercriminal prolífico de habla rusa, que se sabe que emplea una variedad de malware personalizado para implementar malware adicional y ampliar sus métodos de monetización.

Los análisis recientes de Mandiant, SentinelOne y PRODAFT, propiedad de Google, revelaron el papel del grupo como precursor de los ataques de ransomware Maze y Ryuk, sin mencionar la exposición de sus conexiones con las familias Black Basta, DarkSide, REvil y LockBit.

La última ola de intrusiones, detectada por IBM Security X-Force hace dos meses, involucra el uso de Dave Loader, un encriptador previamente atribuido al grupo Conti (también conocido como Gold Blackburn, ITG23 o Wizard Spider), para implementar la backdoor de Domino.

Las conexiones potenciales de Domino con FIN7 provienen de la superposición del código

fuente con DICELOADER (también conocido como Lizar o Tirion), una familia de malware probada en el tiempo atribuida al grupo. El malware, por su parte, está diseñado para recopilar información confidencial básica y recuperar cargas útiles cifradas desde un servidor remoto.

Este artefacto de la siguiente etapa es un segundo cargador con nombre en código Domino Loader, que alberga un ladrón de información .NET encriptado denominado Project Nemesis, que es capaz de acumular datos confidenciales del portapapeles, Discord, navegadores web, billeteras criptográficas, servicios VPN y otras aplicaciones.

> *«Domino ha estado activo en la naturaleza desde al menos octubre de 2022, que es notablemente cuando las observaciones de Lizazr comenzaron a disminuir»,* dijo Hammond, señalando que los hackers pueden estar eliminando gradualmente este último.

Otro enlace crucial que une a Domino con FIN7 proviene de diciembre de 2022, que aprovechó otro cargador llamado NewWorldOrder Loader, para entregar las backdoors de Domino y Carbanak.

Se dice que la puerta trasera y el cargador de Domino, ambos DLL de 64 bits escritos en Visual C++, se han usado para instalar Projec Nemesis desde al menos octubre de 2022, antes de que los ex miembros de Conti lo usaran a inicios de 2023.

El uso de malware ladrón por parte de los distribuidores de ransomware no tiene precedentes. En noviembre de 2022, Microsoft reveló intrusiones montadas por un atacante conocido como DEV-0569 que aprovechó el malware BATLOADER para entregar Vidar y Cobalt Strike, el último de los cuales finalmente facilitó los ataques de ransomware operados por humanos que distribuyeron el ransomware Royal.

Esto ha planteado la posibilidad de que los ladrones de información se implementen durante infecciones de menor prioridad, mientras que aquellos que pertenecen a un dominio de

Active Directory reciben Cobalt Strike.

> *«El uso de malware vinculado a múltiples grupos en una sola campaña, como Dave Loader, Domino Backdoor y Project Nemesis Infostealer, destaca la complejidad que implica el seguimiento de los atacantes, pero también proporcionan información sobre cómo y con quién operan»,* concluyó Hammond.