Una nueva pieza de malware denominada dotRunpeX se está usando para distribuir numerosas familias de malware conocidas como Agent Tesla, Ave Maria, BitRAT, FormBook, LokiBot, NetWire, Raccoon Stealer, RedLine Stealer, Remcos, Rhadamanthys y Vidar.

> *«DotRunpeX es un nuevo inyector escrito en .NET que usa la técnica Process Hollowing y se utiliza para infectar sistemas con una variedad de familias de malware conocidas»,* dijo Check Point en un informe la semana pasada.

El malware parece estar en desarrollo activo y llega como un malware de segunda etapa en la cadena de infección, por lo general implementado por medio de un descargador (también conocido como cargador) que se transmite a través de correos electrónicos de phishing como archivos adjuntos maliciosos.

Alternativamente, se sabe que aprovecha los anuncios de Google maliciosos en las páginas de resultados de búsqueda para dirigir a los usuarios desprevenidos que buscan software popular como AnyDesk y LastPass a sitios de imitación que alojan instaladores troyanos.

Los últimos artefactos DotRunpeX, detectados por primera vez en octubre de 2022, agregan una capa de ofuscación adicional mediante el uso del protector de virtualización KoiVM.

Cabe mencionar que los hallazgos encajan con una campaña de publicidad maliciosa documentada por SentinelOne el mes pasado en la que los componentes del cargador y del inyector se denominaron colectivamente MalVirt.

El análisis de Check Point ha revelado además que *«cada muestra de DotRunpeX tiene una carga útil integrada de una determinada familia de malware para inyectar»,* y el inyector especifica una lista de procesos antimalware para finalizar.

Esto, a su vez, es posible al abusar de un controlador de explorador de procesos vulnerable (procexp.sys) que está incorporado en dotRunpeX para obtener la ejecución en modo kernel.

Hay indicios de que dotRunpeX podría estar afiliado a atacantes de habla rusa según las referencias de idioma en el código. Las familias de malware distribuidas con mayor frecuencia por la amenaza emergente incluyen RedLine, Raccoon, Vidar, Agent Tesla y FormBook.