La Agencia de Seguridad de Infraestructura y Ciberseguridad de Estados Unidos (CISA), publicó hoy una alerta de seguridad con detalles sobre una nueva cepa de malware que fue visto este año, desplegada por hackers del gobierno de Corea del Norte.

El nuevo malware fue detectado en ataques dirigidos a empresas estadounidenses y extranjeras activas en los sectores aeroespacial y de defensa militar, según los informes de McAfee (North Star Operation) y ClearSky (DreamJob Operation).

Los ataques siguieron el mismo patrón, con hackers norcoreanos haciéndose pasar por reclutadores de grandes corporaciones para acercarse a los empleados de las compañías deseadas.

Se pidió a los empleados seleccionados que pasaran por un proceso de entrevista, durante el cual generalmente recibían documentos maliciosos de Office o PDF que los hackers norcoreanos usarían para implementar malware en las computadoras de la víctima.

La carga útil final en los ataques es el punto focal de alerta de CISA, un troyano de acceso remoto (RAT) que CISA llama BLINDINGCAN (llamado DRATzarus en el informe de ClearSky).

Los expertos de CISA afirman que los hackers de Corea del Norte utilizaron el malware para obtener acceso a los sistemas de las víctimas, realizar reconocimientos y luego *«recopilar información sobre tecnología militares y energéticas».*

Esto fue posible gracias al gran conjunto de capacidades técnicas de BLINDINGCAN, que permitieron al RAT:

- Recuperar información sobre todos los discos instalados, incluido el tipo de disco y la cantidad de espacio libre en el disco
- Obtener información sobre la versión del sistema operativo
- Obtener información del procesador
- Obtener el nombre del sistema
- Obtener información de la dirección IP local

- Obtener la dirección de control de acceso a medios (MAC) de la víctima
- Crear, iniciar y finalizar un nuevo proceso y su hilo principal
- Buscar, leer, escribir, mover y ejecutar archivos
- Obtener y modificar marcas de tiempo de archivos o directorios
- Cambiar el directorio actual de un proceso o archivo
- Eliminar el malware y los artefactos asociados con el malware del sistema infectado

La alerta de CISA incluye indicadores de compromiso y otros detalles técnicos que pueden ayudar a los administradores de sistemas y profesionales de seguridad a establecer reglas para escanear sus redes en busca de signos de compromiso.

Con esta, ya son 35 alertas del gobierno de Estados Unidos sobre actividad maliciosa de Corea del Norte. Desde el 12 de mayo de 2017, CISA ha publicado informes sobre 31 familias de malware norcoreanas en su sitio web.

Los hackers del gobierno norcoreano han sido en conjunto, uno de los cuatro actores de amenazas más activos que se han dirigido a Estados Unidos en los últimos años, junto con grupos chinos, iraníes y rusos.