El Comando Cibernético de Estados Unidos, El departamento de Seguridad Nacional y la Oficina Federal de Investigación, expusieron hoy una nueva operación de piratería por parte de Corea del Norte.

Las autoridades publicaron avisos de seguridad que detallan seis nuevas familias de malware que los hackers norcoreanos están utilizando en la actualidad.

Según la Fuerza de Misión Nacional Cibernética (CNMF), una unidad subordinada del Comando Cibernético de Estados Unidos, el malware se distribuye por medio de una campaña de phishing de Corea del Norte.

El Comando Cibernético de Estados Unidos cree que el malware se utiliza para proporcionar a los hackers de Corea del Norte acceso remoto a los sistemas infectados con el fin de robar fondos que luego se transfieren a Corea del Norte, como una forma de evitar sanciones económicas.

El gobierno de Corea del Norte tiene una larga historia de uso de piratas informáticos para robar fondos de bancos e intercambios de criptomonedas para evadir sanciones económicas y recaudar fondos para sus armas nucleares y programas de misiles.

En septiembre de 2019, el Departamento del Tesoro de Estados Unidos impuso sanciones al régimen de Pyongyang por el uso de esta táctica exacta.

Junto con la alerta de Twitter enviada por el Comando Cibernético de Estados Unidos, la Agencia de Infraestructura y Ciberseguridad (CISA) del DHS también publicó hoy informes detallados.

Los informes proporcionan un análisis en profundidad de las seis nuevas muestras de malware que las autoridades de Estados Unidos han estado rastreando recientemente.

- BISTROMATH – Se describe como un RAT con todas las funciones.
- SLICKSHOES – Un dropper de malware (cargador).

- CROWDEDFLOUNDER – *«Un ejecutable de Windows de 32 bits, que está diseñado para desempaquetar y ejecutar un binario de troyano de acceso remoto (RAT) en la memoria».*
- HOTCROISSANT – Un *«implante de balizamiento con todas las funciones»,* utilizado para realizar encuestas del sistema, cargar/descargar archivos, ejecutar procesos y ejecutar comandos.
- ARTFULPIE – Descrito como *«un implante que realiza la descarga y carga en memoria y la ejecución de una DLL desde una URL codificada».*
- BUFFETLINE – Se describe como *«un implante de balizamiento con todas las funciones»* que puede descarga, cargar, eliminar y ejecutar archivos, habilitar el acceso a la CLI de Windows, crear y finalizar procesos y realizar la enumeración del sistema de destino.

Un séptimo informe actualiza la información sobre HOPLIGHT, un troyano de puerta trasera basado en proxy que el DHS y el FBI expusieron en abril de 2019.

CISA atribuye el malware al grupo Lazarus

CISA atribuyó el malware a un grupo de hackers respaldado por el gobierno de Corea del Norte conocido como HIDDEN COBRA, también conocido como Lazarus Group.

Anteriormente, el Departamento de Justicia acusó a un miembro de este grupo por su participación en distintos incidentes de seguridad, incluido el hackeo de Sony en 2014, el ataque al banco de Bangladesh en 2016 y orquestar el brote del ransomware WannaCry en mayo de 2017.

En una captura de pantalla compartida con ZDNet, un miembro de Kaspersky GReAT, la unidad de élite de caza de hackers de Kaspersky, dijo que las muestras de malware también compartían código con otras cepas de malware de Corea del Norte, utilizadas en operaciones anteriores, confirmando efectivamente el Comando.

Las revelaciones de hoy son solo un paso más en el nuevo enfoque del gobierno de Estados

Unidos para manejar las operaciones de seguridad cibernética extranjeras realizadas contra objetivos estadounidenses.

Mientras que en años anteriores el gobierno de Estados Unidos ha evitado decir algo sobre los ataques contra entidades gubernamentales y el sector privado, recientemente adoptaron un enfoque de *«nombre y verguenza».*

Anteriormente, esto incluía alertas de seguridad en los sitios web de DHS/CISA y casos legales presentados por el Departamento de Justicia, pero esto recientemente se expandió al uso de sanciones del Departamento del Tesoro y comunicados de prensa de la Casa Blanca que llamaban ataque cibernéticos orquestados en el extranjero.

En noviembre de 2018, el enfoque de nombre y vergüenza también agregó una nueva táctica cuando el Comando Cibernético de Estados Unidos comenzó a cargar *«muestra de malware no clasificadas»* en VirusTotal y anunció las cargas por medio de una cuenta de Twitter.

Las muestras iniciales se vincularon con grupos de piratería rusos e iraníes. Posteriormente, el Comando Cibernético de Estados Unidos también comenzó a cargar muestras de malware relacionadas con la actividad de piratería de Corea del Norte, en agosto, septiembre y noviembre de 2019.

Sin embargo, en ninguno de los casos anteriores, el Comando Cibernético de Estados Unidos atribuyó alguna muestra de malware a un actor estatal, dejando la atribución a expertos de empresas privadas de seguridad cibernética.

Como Cyberscoop dijo hoy, esta es la primera vez que el Comando Cibernético de Estados Unidos ha vinculado públicamente una de estas muestras de malware a un actor del estado-nación, en lugar de depender del sector privado.

Pero el propósito de las advertencias de seguridad de hoy era crear conciencia sobre las campañas de piratería de Corea del Norte en curso.

Los avisos de seguridad de CISA incluyen indicadores de compromiso (COI) y reglas de YARA para ayudar a las empresas y organizaciones gubernamentales a buscar en las redes internas cualquier signo de malware de Corea del Norte.

Según Cyberscoop, los funcionarios estadounidenses también enviaron alertas de seguridad privada al sector privado estadounidense antes de la divulgación pública de hoy, instando a las compañías a investigar la amenaza actual.

Se desconoce la escalada de los ataques actuales de Corea del Norte contra objetivos estadounidenses, pero a juzgar por las tres exposiciones similares del año pasado, se cree que los ataques de Corea del Norte están en una ola constante.

Desde 2018, el DHS emitió 23 informes sobre malware de Corea del Norte. La agencia publicó previamente informes sobre WannaCry, DeltaCharlie, Volgmer, FALLCHILL, BANKSHOT, BADCALL, HARDRAIN, SHARPKNOT, un troyano/gusano de acceso remoto sin nombre, Joanap y Brambul, TYPEFRAME, KEYMARBLE, FASTCash y el informe anterior HOPLIGHT.

En enero de 2019, el Departamento de Justicia, el FBI y la Fuerza Aérea de Estados Unidos también intervinieron para derribar la botnet Joanap, que se cree que fue construida por hackers norcoreanos para ayudar en sus operaciones y servir como una red de representantes para disfrazar el origen de sus ataques.