17/11/22

DTrack evoluciona para amenazar a Europa y América Latina

DTrack es un **troyano de acceso remoto** usado por el grupo Lazarus. Este **APT norcoreano** tiene cómo objetivos típicos los sectores de la **educación, fabricación química, investigación gubernamental, proveedores de telecomunicaciones y de infraestructuras tecnológicas**.

Trazas de la **actividad de DTrack** se han observado en Alemania, Brasil, India, Italia, México, Suiza, Arabia Saudí, Turquía y Estados Unidos. Esto demuestra las **intenciones del grupo de expandir su operación hacia Europa y América Latina**.

El troyano analizado por el equipo de Kaspersky permite a los atacantes subir, bajar, ejecutar y borrar archivos en el equipo de la víctima. Un kit de herramientas **diseñado para efectuar movimientos laterales, pivotando en la red del objetivo**.

DTrack, funcionamiento y novedades

Este troyano sigue varias fases hasta cargar el *malware* final en el sistema víctima. **DTrack se esconde en un ejecutable que a primera vista parece inofensivo**. En una **primera fase localiza el código** necesario para continuar con el proceso mediante un *offset* con referencia en el ejecutable inicial **o recursos del mismo**.

Una vez obtenida la localización y clave necesaria, se descifra el contenido de la siguiente fase. **Los algoritmos de encriptado para esta fase varían entre versiones modificadas de RC4, RC5 y RC6**. El *payload* que se obtiene tras descifrar esta fase es una *shellcode* **muy ofuscada**.

Cómo **novedad**, en las últimas muestras detectadas **el** *payload* **de la tercera fase no es el definitivo**, existiendo otra capa más de empaquetado. La *shellcode* tiene **curiosidades que dificultan su análisis**, cómo la búsqueda dentro del código del ejecutable de una *key* a partir de la que obtiene un **bloque de configuración** con el tamaño final del *payload* y el *offset* para el punto de entrada del ejecutable.

En la **última fase un archivo DLL** se descifra y carga en el proceso **explorer.exe**. En muestras anteriores de DTrack las librerías cargadas eran **cadenas ofuscadas**, en las **nuevas muestras se usa API hashing para esta función**. Otro pequeño cambio es la inclusión de tres servidores de comando y control en vez de los seis habituales.

Indicadores de Compromiso

Dominios:

pinkgoat[.]com
purewatertokyo[.]com
purplebear[.]com
salmonrabbit[.]com

Hashes:

ba8f9e7afe5f78494c111971c39a89111ef9262bf23e8a764c6f65c818837a44
3fe624c33790b409421f4fa2bb8abfd701df2231a959493c33187ed34bec0ae7

Más información:

Lazarus Backdoor DTrack Evolves to Target Europe and Latin America - Infosecurity Magazine (infosecurity-magazine.com)

Dtrack expands its operations to Europe and Latin America | Securelist