Amenazas informáticas

Grupo # 8

TIPO = RANSOMWARE “DARKSIDE”

El malware de rescate, o ransomware, es un tipo de malware que impide a los usuarios acceder a su sistema o a sus archivos personales y que exige el pago de un rescate para poder acceder de nuevo a ellos.

En el caso del DarkSide, de no querer negociar el pago del rescate, el grupo de hackers extorsiona a sus víctimas con filtrar la información en un sitio específicamente creado para ese fin.

Comienzo y propagación

DarkSide ransomware

El ransomware DarkSide fue el responsable del ataque a la compañía de oleoducto más importante de los Estados Unidos, Colonial Pipeline, que se ocupa de abastecer el 45% del combustible que se consume en la Costa Este del país y a más de 50 millones de habitantes

Habrían entrado a traves de las conexiones remotas como el RDP para acceder a los sistemas de las víctimas.

Otra amenaza implicada

Para llevar a cabo sus ataques, los hackers emplean infraestructuras de mando y control (C2) mediante las cuales ejecutan distintas Tácticas, Técnicas y Procedimientos (TTP) para finalmente llevar a cabo los objetivos de sus acciones, como viene a ser la distribución de Rasomware, entre otros.

En los distintos grupos ATP se pueden observar varios de ellos que presenten entre sus TTPs la penetración a sistemas a través de la explotación del servicio remoto (RDP), el uso de este medio para realizar movimientos laterales en la organización vulnerada, o la habilitación de RDP para crear persistencia en la máquina víctima, entre otros.

Soluciones posibles

Jornadas de capacitación a personal con acceso a la red sobre los riesgos de seguridad informática y cómo prevenir estas situaciones.