DarkSide Ransomware
(CSB21-07)
June 22, 2021

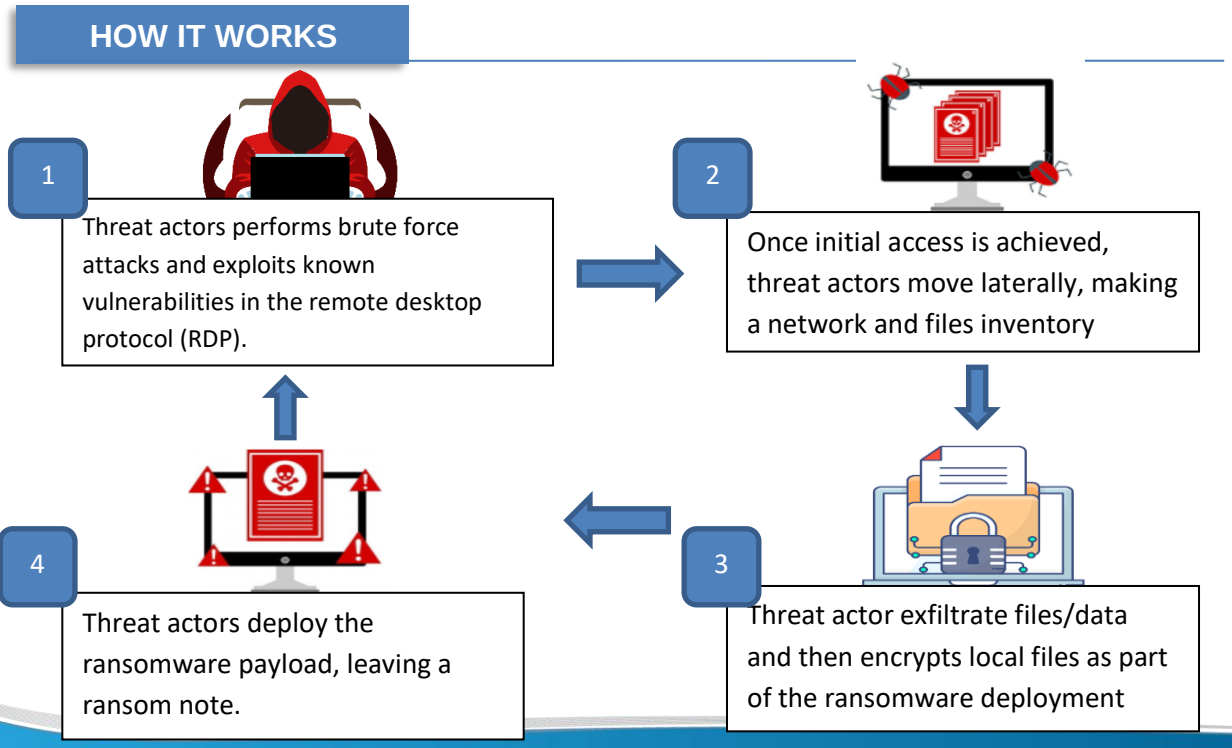
DarkSide ransomware is a ransomware-as-a-service (RaaS) which primarily targets Windows systems but was also reported to have the ability to target Linux OS variants. Discovered on August 2020, DarkSide ransomware has begun attacking organizations worldwide and has been performing targeted attacks against numerous companies.

Like other ransomware attacks, threat actors breach a network and will spread laterally throughout the network until they gain access to an administrator account and will harvest unencrypted data from their victim's servers and upload it to their servers simultaneously.

Based on the "press release" issued by the threat actors behind DarkSide ransomware, they claim to be former affiliates of other well-known cryptolockers. Moreover, said threat actors also stated that they will not target medicine (hospital, hospices), education (schools, universities), non-profit organizations, and government sector.

The Darkside ransomware uses Salsa20 and RSA-1024 to encrypt their victim's files. According to research, the malware then stops services that contain the following terms in their names: vss, sql, svc, memtas, mepocs, sophos, veeam or backup. It then proceeds to enumerate running processes and terminates them so it can unlock the files they were accessing to encrypt them. It also uses a PowerShell command to delete all volume shadow copies already created and which could be used to restore files.

HOW IT WORKS



IMPACT

- Temporary or permanent loss of data.
- Potential harm to the organization's reputation.
- Interfere with the normal functioning of the computer system or prevent its utilization.

MITIGATIONS

- Do not pay the ransom.
- Remove infected computer within the network.
- Ensure that backup data is offline and secure.
- Coordinate with IT Project Officer assigned in your office/unit.
- Perform a full system scan in safe mode to remove any infections.

PREVENTION

- Navigate directly to websites by typing the legitimate URL into the browser instead of clicking on links in messages/emails.
- Avoid auto-saving password, payment card numbers, or contact information.
- Use unique, complex passwords for all devices/accounts.
- Update software, including operating systems, applications and firmware.
- Implement scheduled backups of data and conduct testing of backups regularly. Consider maintaining multiple backups in different locations for redundancy.
- Ignore all emails from unknown sender. Avoid opening or downloading files attached to spam emails.
- Do not use cracked or untrusted program.
- Regularly run a complete scan to check the computer for present of malware.

REFERENCE

- https://us-cert.cisa.gov/ncas/alerts/aa21-131a
- https://www.trendmicro.com/en_ph/research/21/e/what-we-know-about-darkside-ransomware-and-the-us-pipeline-attac.html