DoppelPaymer Ransomware (CSB21-09)

July 23, 2021

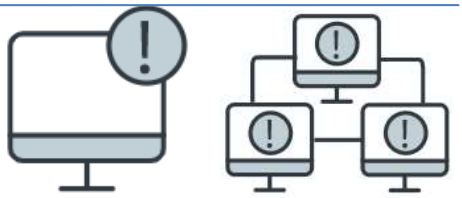
DoppelPaymer Ransomware, successor of BitPaymer ransomware, was first reported on June 2019. DoppelPaymer threat actors targets critical industries worldwide such as healthcare, emergency services, and education. Like many other ransomware threat actor groups, DoppelPaymer operators maintain a public site and social media presence typically include lists of their victims and their leaked data.

DoppelPaymer ransomware encrypt the files of their victims, locking them out of their systems, and exfiltrate their data and use it as collateral. DoppelPaymer is one of the first ransomware variants where threat actors have called their victims, pressuring them to pay the ransom through intimidation or threatening them to release exfiltrated data.

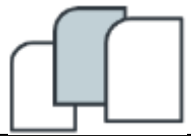
DoppelPaymer operators gains access through certain admin credentials and utilizing them in order to spread throughout the whole network. Once the said ransomware is able to penetrate and gain access towards a main Windows domain controller, they then deploy the ransomware payloads towards all of the devices linked to the network.

HOW IT WORKS

1. Threat actor sends spam or phishing email with attached documents embedded with malicious codes – either JavaScript or VBScript



2. On execution, this code downloads DoppelPaymer's first-stage loader on the victim's machine. Once user credentials are compromised, the ransomware can be distributed across the network.



3. Once the ransomware has been installed, threat actors will exfiltrate credentials and data

4. DoppelPaymer encrypt files, change the passwords, and forces the system to restart into safe mode to prevent user entry from the system, leaving a ransom note that appears before the login screen

IMPACT

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

MITIGATIONS

- Do not pay the ransom.
- Remove infected computer within the network.
- Ensure 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

- Refrain from opening emails from unknown senders.
- Beware of phishing emails, spams and clicking malicious attachment.
- Keep systems and applications updated, including anti-virus and anti-malware software.
- Perform regular online and offline back up of important data/files.
- Monitor inbound and outbound network traffic; set alert for data exfiltration.
- Implement two-factor authentication (2FA) for user login credentials.
- Block websites that are known for being malware breeding grounds (illegal download sites, etc.)
- Do not use cracked or untrusted program.
- Regularly run a complete anti-virus or anti-malware scan.

REFERENCE

- https://www.trendmicro.com/en_ph/research/21/a/an-overview-of-the-doppelpaymer-ransomware.html