Arete
Incident Response

Variant - Wasted

Characteristics

- Arete first saw WASTED on June 04, 2020
- We have had a total 4 engagements
- They do not negotiate down the ransom at all (to date)
- They threaten to increase the ransom every 24 hours
- Demands have ranged from 40 BTC to 1,000 BTC
- Hours of operation: contact me UTC 5am-8am and 5pm-8pm.
- Decryptor is faster than most other variants.
- We've seen them enter through VPN with compromised credentials (hint: enable MFA on VPNs)
- They will look for and prevent access to backups by deletion or encryption
- They use a variety of means to remain persistent with Command and Control frameworks.
- They can be on the network for a few days or several weeks. Their reconnaissance is thorough to include multiple compromised accounts, full listing of server names and potential functions.
- Ransomware payload is customized to the victim's environment. The file extension will have 3 characters that represent the client name somehow prepended to wasted ex. *.abcwasted
- Ransomware note has the company's full name at the top. It is located in the corresponding *.abcwasted_info
- The _info file has a public key which is required to decrypt the file. When sending the files to the TA, both the encrypted file and the _info need to be sent.
- They have been very slow to respond, 12+ hours in some cases, and even during their apparent working hours, could be 2-3 hours before reply, even if we were replying immediately to them
- In one case it took them 3 times to accomplish POL