Thanos Builder

Tiered Ransomware

June 13, 2020

ATLAS CYBERSECURITY

www.atlas-cybersecurity.com

Functionality

- Depending on the service, the Thanos ransomware offers various configuration options, features, and classes
  - Researchers have observed more than 80 Thanos 'clients' with different configuration options
- One such options is the ability to change the encryption process utilized by Thanos to use the RIPlace technique
  - This technique involves replacing a victim's files with encrypted data, by writing the newly encrypted data from memory to a new file, and then using the "rename" call to replace the original file.
  - After the sensitive file is replaced (thus the inspiration for the name "RIPlace") it enables the threat actors to bypass ransomware protections
    - In the builder, a user can simply select an option to enable the RIPlace functionality
- More features of the Thanos ransomware include
  - The ability to exfiltrate all files with a specified set of extensions
  - An anti-analysis tool allowing the client to perform several checks to determine whether it is being loaded in a virtual environment
  - Two obfuscation methods
- The encryption process for Thanos utilizes a random, 32-byte string generated at runtime as a password for the AES file encryption
  - The string is then encrypted with the Thanos operator's public key
    - Without the corresponding private key, recovering the encrypted files is impossible
  - It's important to note that the builder includes the option to use a static password for the AES file encryption
    - If this option is selected, the clients generated by Thanos will contain the AES password used to encrypt file
    - This means that if a Thanos client is recovered after encryption has occurred, there is a chance that the victims may be able to recover their files without having to pay the ransom