Exhibit 17

3. The ransomware enumerates all the files it needs to encrypt using a hardcoded list of data file extensions.
4. It then generates locally a set of private symmetric keys to be used for encrypting the files. Symmetric keys are used for both encryption and decryption. In some cases one key per file is generated, in other cases it could be one key per file extension or just one key for the entire set. It all depends on how paranoid the malware author is.
5. The ransomware uses the private key algorithm and the symmetric private keys generated in the previous step to encrypt the files.
6. Then the private encryption keys themselves are encrypted using the public key from step two. The result is stored in the victim's computer's key store.
7. The ransom note is displayed, sometimes with an incentive to pay quickly.

Decryption

1. Once the malware operator receives payment, the private key from the C&C server is sent to the ransomware decryptor code.
2. This private key is then used to decrypt the symmetric private keys used earlier to encrypt the files and which were stored in the local key store.
3. The symmetric private keys obtained are used to decrypt and recover the original data files.

Earlier versions of ransomware like CryptoWall 2.0 were not as sophisticated and used the public key directly to encrypt data files. Cryptowall 3.0 evolved to the process above combining public/private keys and symmetric keys. Cerber uses a combination of RSA public/private keys and RC4 keys. Typically, a combination of AES and RC4 encryption algorithms are used with varying ciphers.

Cyphort's Ability to Detect Ransomware

Detecting ransomware can be doe using network-based detection or endpoint-based detection. We will focus on network-based detection and more specifically how Cyphort detects these advanced threats.

Cyphort's advanced detection fabric includes multiple detection and analytics capabilities, which work together to quickly identify advanced targeted attacks like ransomware. These capabilities are summarized below.

Object Analysis Pipeline

All files analyzed by Cyphort go through a multi-stage detection pipeline within the SmartCore analytics angine, which is comprised of the following components:

- **Static AV Engine** - leverages top-tier Anti-Virus technology with very frequent signature updates to detect known viruses.
- **Reputation Engine** - provides reputation-based detection, where file hashes, signers and other meta-data about the file and the context around its source are compared to our threat intelligence knowledge base.

- **Behavioral Engine** - performs dynamic analysis of the object's behavior in a sandbox environment and applies machine learning models to the observed behavior.
- **Emulation Engine** - emulates files containing scripts as an alternative to full behavioral analysis.
- **Yara Engine** - allows application of Yara rules to files as well as memory dumps obtained during behavioral analysis.

Network Analysis Pipeline

Traffic visible to Cyphort also goes through a couple of steps before files are extracted for analysis:

- **Snort rules** - all traffic is subjected to snort rules from Cyphort Labs as well as third party sources.
- **Chain Heuristics** - flags suspicious traffic and submits it to a browserp-based dynamic analysis environment where heuristics rules are applied to identify malicious traffic like exploit kits redirects.

Use Cases

The detection methods for ransomware are usually tailored to the delivery mechanism. Let's review each delivery mechanism above and discuss what methods of detection Cyphort uses in each case.

Email Attachments

Cyphort can monitor email traffic using either a journaled account or Bcc mailbox. In both cases, Cyphort extracts all email attachments and submits them to SmartCore's Object Analysis Pipeline, where it extracts all links (including links inside attachments) and submits them to SmartCore's reputation engine. Cyphort integrates with Office365 and Gmail to provide seamless remediation capability by blocking or quarantining malicious emails.

If ransomware is being delivered via a PDF, Office document, malicious Javascript or executable file attached to an email, Cyphort uses all elements of the Object Analysis Pipeline to identify the threat.

Locky was a prominent example of ransomware downloaded by an email attachment. The attachment itself is either a Javascript file inside a zip file or a Word document with a VBA macro claiming to be an invoice or a shipment notification.

Cyphort detects the Javscript zipped attachments as Exploit.Script.