Ransomware

Joshua Reynolds
NMSU Reverse Engineering
Spring 2024

Ransomware

Malware that encrypts important files (including data and/or configuration settings) and demands payment for its restoration.

Very common attack, and some attackers use weak attacks that a reverse engineer can undo.

Attackers do follow through with decrypting when companies pay up, to promote future business. When companies don’t pay, attackers also follow through on promises to release sensitive data publicly.

Cryptography - Encryption

Encryption schemes come in pairs – a 1:1 encryption function and a 1:1 decryption function. Encryption and decryption are inverses.

How do you know if encryption is good? If it can win this game:

1. Alice encrypts a message.
2. Alice privately flips a fair coin. If heads, Alice reveals the encrypted message. If tails, Alice generates random bytes of the same length.
3. For a good encryption scheme, nobody can tell if Alice is showing an encrypted message or just random bytes.

Broken Encryption Schemes

The simplest encryption schemes include character swapping.

For example, you could add 0xA4 to every byte to encrypt, and subtract 0xA4 from every byte to decrypt.

Programmatic encryption can be undone by a determined reverse engineer who learns how to undo the encryption.

Symmetric Encryption

When attackers use state-of-the-art cryptography, there is danger.

Advanced Encryption Standard (AES) uses an encryption key to encrypt and decrypt. Ransomware that uses AES cannot be decrypted without that key.

RC4 should be deprecated, it may be broken

ChaCha20 is another alternative

Weakness of Symmetric Encryption in Ransomware

But the key must be sent in some form to the ransomware to use for encrypting. When this key can be extracted, reverse engineers can write a decryptor without paying the ransom.

Asymmetric Encryption

Asymmetric Encryption has enabled us to do business over the Internet

Unlike symmetric key encryption, two different keys are used for decryption and encryption.

The key needed to encrypt things can be shared publicly, and the decryption key kept private. (HTTPS relies on this property, among other things)

We call these keys the **public key** and the **private key**

Asymmetric Encryption Limitations

Asymmetric Encryption is slow, and can only encrypt relatively small chunks of data at a time. Symmetric encryption is much faster.

Ransomware’s combination of symmetric and asymmetric encryption

What state of the art ransomware does is to generate a random AES key for every file it encrypts.

Then, only this key is encrypted with asymmetric cryptography.

If victims buy the private key for decryption, they can decrypt the AES keys that each of their files have been encrypted with.

Cryptographically Strong Ransomware

Attacker generates and stores a **unique public/private asymmetric key pair** for each victim.

The public key is packaged in the payload of their attack

For each file that is encrypted, a random AES key is generated, used, encrypted, and stored with the file.

If attackers don’t use unique keys for each attack, they cannot sell a decryptor without it working for everyone

Backups and Defeating Backups

Encrypting everything on a server takes time, particularly if that server has a large amount of storage.

Encrypting some files will start to cause errors that may give away the attack.

Some anti-malware systems will also monitor how many files are opened.

Ransomware can hide by working “low and slow” and choosing to start with files that haven’t been opened in many days.

If ransomware isn’t detected for a long time, the encrypted version of files can be even copied into backups automatically.

Detecting Ransomware

Windows Ransomware Protection:

Windows Defender can be directed to protect certain folders from access

Only a list of programs specified by the user can access each folder

Filesystem Entropy Watch:

Programs write to files all the time, so detecting ransomware is tricky.

One technique to detect whether a file is being encrypted is to compare the **entropy** of the file before and after a file write.

If a program increases entropy drastically, it is likely encrypting files.

Activity: Attacking Ransomware 1 from the assignment