1. **Mã độc Mức yêu cầu 01 - RQ01**: Mã độc này thực hiện chèn mã độc vào quá trình bình thường bằng cách sử dụng section .reloc, tạo và nối mới section trong tập tin thực thi để tiêm payload của virus. [Đây có thể được coi là một kỹ thuật process hollowing](https://harrisonwl.github.io/assets/courses/malware/spring2017/slides/week04/FileViruses.pdf)[1](https://harrisonwl.github.io/assets/courses/malware/spring2017/slides/week04/FileViruses.pdf).
2. [**Mã độc Mức yêu cầu 02 - RQ02**: Mã độc này đạt được RQ01 và có khả năng lây nhiễm qua các file thực thi khác cùng thư mục khi người dùng kích hoạt tập tin chủ1](https://harrisonwl.github.io/assets/courses/malware/spring2017/slides/week04/FileViruses.pdf).
3. [**Mã độc Mức yêu cầu 03 - RQ03**: Thay vì thay đổi Entry-point của chương trình, mã độc này áp dụng lần lượt 02 chiến lược lây nhiễm trong nhóm kỹ thuật Entry-Point Obscuring (EPO) virus2](https://www.virusbulletin.com/virusbulletin/2014/07/api-epo). Một số dạng EPO-virus có thể xem xét để thực hiện yêu cầu này bao gồm:
   * [**Call hijacking EPO virus**: Mã độc này sử dụng kỹ thuật che giấu điểm đầu vào thực thi của mã virus1](https://harrisonwl.github.io/assets/courses/malware/spring2017/slides/week04/FileViruses.pdf).
   * [**Import Address Table-replacing EPO virus**: Mã độc này thay thế tất cả các lệnh gọi API liên quan đến thư viện đầu tiên của bảng nhập khẩu với một lệnh gọi đến routine ban đầu của mã độc2](https://www.virusbulletin.com/virusbulletin/2014/07/api-epo).
   * [**TLS-based EPO virus**: Mã độc này sử dụng giao thức TLS để mã hóa và đóng gói nội dung của nó, bảo vệ chúng khỏi việc bị quan sát hoặc sửa đổi trong quá trình truyền3](https://news.sophos.com/en-us/2021/04/21/nearly-half-of-malware-now-use-tls-to-conceal-communications/).