Kỹ thuật lây nhiễm virus

1. Overwriting Viruses

Một vài virus đơn giản là copy chính nó vào những file khác. Dĩ nhiên, kỹ thuật này cực kỳ nguyên thuỷ nhưng lại là cách dễ nhất. Những virus kiểu này có thể phá huỷ hoàn toàn khi chúng lây trên tất cả các file trên đĩa.

Overwriting viruses không thể bị khử khỏi hệ thống. Những file bị nhiễm bắt buộc phải bị xoá đi và restore lại từ backup.

Hình dưới đây cho thấy nội dung của file chủ sẽ thay đổi như thế nào khi bị Overwriting virus tấn công.





Loại virus này thì thật sự không thành công bởi vì nó có thể dễ dàng bị phát hiện bởi người dùng.

1. Appending Viruses

Loại virus này sẽ chèn đoạn code độc hại vào cuối file chủ, sau đó sẽ thay đổi nội dung phần đầu của file chủ bằng cách sử dụng lên JMP để di chuyển xuống thực thi mã của virus trước, sau đó virus sử dụng lệnh JMP để di chuyển lên vị trí đầu của file chủ.

Hình ảnh minh hoạ



1. Prepending Viruses

Trái ngược với appending virus, prepending virus chèn đoạn mã virus vào phần đâu của file chủ,



1. Cavity Viruses

Loại virus này sẽ tìm một khoảng trống vừa đủ trong file chủ để chèn đoạn mã độc của nó vào, sau đó thay đổi Entry Point của file chủ trỏ đến thực thi mã độc này trước, sau khi thực thi xong virus sẽ dùng lênh JMP để trỏ về vị trí Entry Point cũ của file chủ.



\*Rất khó để tạo ra những con virus này.

1. Fractionated Cavity Viruses

Loại virus này thường là khi không tìm được một khoảng trống đủ để chứa mã độc, nó sẽ tìm nhiều khoảng trống nhỏ hơn và cách mã độc chèn vào những khoảng trống đó, sau đó dùng nhiều lệnh khác nhau để kết hợp những đoạn này



1. Compressing Viruses

Loại virus này thường sẽ nén nội dung của file chủ nhằm mục đích tránh việc dung lượng file chủ bị tăng lênh.



Áp dụng kỹ thuật này nên một số PE Packer ra đời ví dụ như PKLITE, LZEXE, UPX và ASPACK, những công cụ này được hacker sử dụng để giảm dung lượng của virus, trojan hay worm cũng như mã hoá chúng để qua mặt AntiVirus.

1. Embedded Decryptor Technique

Những virus này sẽ mã hoa đoạn mã của chúng và chèn đoạn mã giải mã vào file chủ. Khi file chủ được thực thi, các hàm trong đoạn giải mã sẽ giải mã mẫ đọc của virus và thực thi chúng.



1. API-Hooking Technique Win32

Phần này dài vc, tìm hiểu sau.