**Họ và tên: Tăng Dũng Cẩm**

**MSSV: 22520141**

1. **Mô tả các ký thuật cơ bản của virus máy tính**
2. **Kỹ thuật lây nhiễm**

Là kỹ thuật cơ bản cần phải có của mỗi virus. Có thể đơn giản hoặc phức tạp tuỳ loại virus.

❖ Kỹ thuật lây nhiễm Boot Record / Master Boot của đĩa: thay thế BR hoặc MB trên phân vùng hoạt động với chương trình virus.

❖ Kỹ thuật lây nhiễm file thi hành: chương trình virus sẽ được ghép vào file chủ bằng cách nối thêm, chèn giữa, điền vào khoảng trống, ghi đè…

Thuật toán thường dùng:

* Mở file

▪ Ghi lại thời gian/ngày tháng/thuộc tính

▪ Lưu trữ các byte đầu tiên (thường là 3 byte)

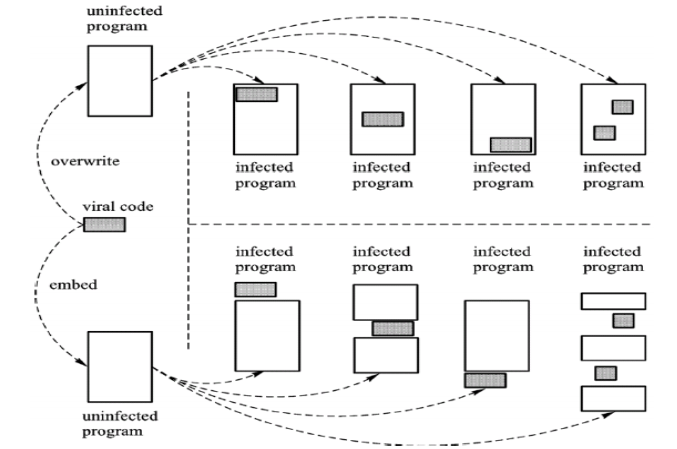
▪ Tính toán lệnh nhảy mới

▪ Đặt lệnh nhảy

▪ Chèn thân virus chính vào

▪ Khôi phục thời gian/ngày tháng/thuộc tính

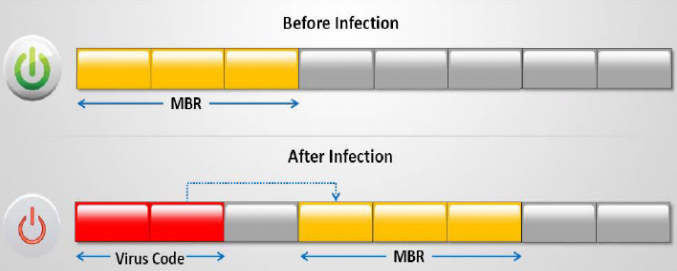
▪ Đóng file.



1. **Kỹ thuật định vị trên vùng nhớ**

❖ Phân phối một vùng nhớ để thường trú, chuyển toàn bộ chương trình virus tới vùng nhớ này, sau đó chuyển quyền điều khiển cho đoạn mã tại vùng nhớ mới với địa chỉ segment: offset mới.

❖ Là một kỹ thuật quan trọng đối với các chương trình virus dạng mã máy (virus Boot, virus file). Virus macro và virus Script thực chất là các lệnh của chương trình ứng dụng nên không cần tiến hành kỹ thuật này.



1. **Kỹ thuật kiểm tra sự tồn tại**

❖ Mỗi virus chỉ nên lây nhiễm/kiểm soát một lần để đảm bảo không làm ảnh hưởng đến tốc độ làm việc của máy tính.

❖ Virus phải kiểm tra sự tồn tại của chính mình trước khi lây nhiễm hoặc thường trú.

▪ Kiểm tra trên đối tượng bị lây nhiễm

▪ Kiểm tra trên bộ nhớ

❖ Kỹ thuật kiểm tra thường là:

▪ Dò tìm đoạn mã nhận diện trên file hoặc bộ nhớ.

▪ Kiểm tra theo kích thước hoặc nhãn thời gian của file.

1. **Kỹ thuật thường trú**

❖ Các virus boot phải phân phối một vùng nhớ riêng để lưu giữ chương trình virus bao gồm mã lệnh, biến, vùng đệm.

❖ Các virus file cần phải kiểm tra xem chương trình đã thường trú chưa, nếu chưa sẽ định rõ vùng nhớ muốn sử dụng, copy phần virus vào bộ nhớ, sau đó khôi phục file chủ và trả quyền điều khiển về cho file chủ.

1. **Kỹ thuật mã hoá**

❖ Nhằm che giấu mã lệnh thực sự của chương trình virus. Thủ tục mã hoá cũng chính là thủ tục giải mã.

1. **Kỹ thuật nguỵ trang**

❖ Nhằm giấu giếm, nguỵ trang sự tồn tại của virus trên đối tượng chủ.

❖ Những virus sử dụng kỹ thuật này thường chậm bị phát hiện nên có khả năng lây lan mạnh.

❖ Sơ đồ nén file chủ để nguỵ trang sự tồn tại của Virus:

▪ Kiểm tra kích thước file chủ định lây nhiễm

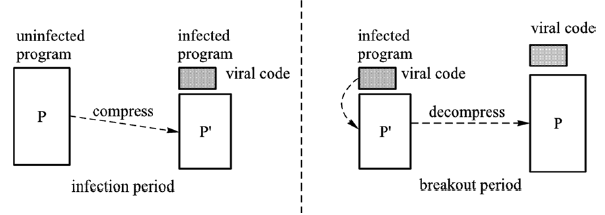
▪ Nén file chủ

▪ Gắn đoạn mã cần lây nhiễm vào file chủ

▪ Có thể chèn thêm những đoạn ký tự vô nghĩa khi kích thước

file chủ + virus vẫn nhỏ hơn kích thước file chủ nguyên thuỷ.

▪ Giải nén file chủ trước khi file này thực thi.



1. **Kỹ thuật phá hoại**

❖ Đa dạng

❖ Phá hoại dữ liệu trên máy tính

❖ Phá hỏng một phần máy tính

1. **Kỹ thuật chống bẫy**

❖ Chọn lọc file trước khi lây nhiễm theo một số tiêu chí nào đó nhằm tránh những file bẫy của chương trình Antivirus.

▪ Không lây nhiễm các file có số trong tên file

▪ Không lây nhiễm những chương trình sử dụng nhiều mã lệnh đặc biệt.

▪ Không lây nhiễm các file có tên liên tục (ví dụ aaaaa.com…).

▪ Không lây nhiễm các file liên tục có cùng kích thước.

▪ Không lây nhiễm các file ở thư mục gốc.

▪ Không lây nhiễm các file có lệnh nhảy và lệnh gọi zero.

1. **Kỹ thuật tối ưu**

❖ Gồm các kỹ thuật viết mã và thiết kế nhằm tối ưu chương trình về tốc độ và kích thước.

1. **Kỹ thuật tạo vỏ bọc**

❖ Là kỹ thuật chống gỡ rối / dịch ngược mã lệnh virus nhằm chống lại phần mềm antivirus.

❖ Thường mã hoá hoặc sử dụng các lệnh JMP và CALL để chương trình lộn xộn, phức tạp.

❖ Sử dụng các thủ tục giả để phân tích viên gặp khó khăn khi phân biệt các tác vụ…

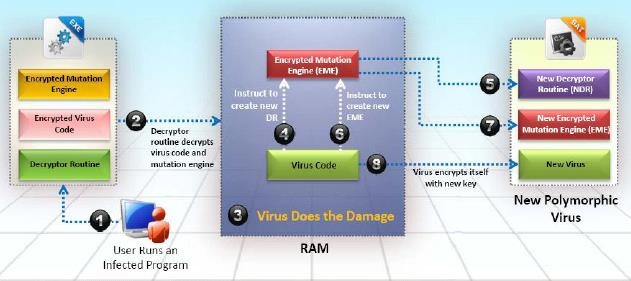
1. **Kỹ thuật đa hình**

❖ Là kỹ thuật chống lại phương pháp dò tìm đoạn mã mà các chương trình antivirus thường sử dụng để nhận dạng một virus đã biết bằng cách tạo ra các bộ giải mã khác biệt.

1. **Kỹ thuật biến hình**

❖ Cũng là một kỹ thuật chống lại các kỹ thuật nhận dạng của chương trình antivirus bằng cách sinh ra cả đoạn mã mới hoàn toàn.

❖ Là một kỹ thuật khó, phức tạp.



1. **Kỹ thuật chống mô phỏng và theo dõi**

❖ Một số chương trình antivirus hiện đại sử dụng phương pháp heuristic để phát hiện virus dựa trên hành vi của chương trình. Kỹ thuật này nhằm chống lại sự phát hiện của chương trình antivirus như vậy.

❖ Thông thường là chèn thêm những đoạn mã lệnh “rác” không ảnh hưởng đến logic của chương trình xen kẻ giữa những mã lệnh thực sự.

1. **Tìm và nêu đặc điểm của 2 - 3 loại mã độc (virus, worm...) xuất hiện trong thời gian gần đây (tên, nguồn gốc, đặc điểm, phương thức phá hoại, biện pháp phòng chống, nguồn tham khảo).**

* **Tên: Medusa Malware**

**Nguồn gốc:**

* Medusa xuất hiện như một dịch vụ mã độc tống tiền (Ransomware-as-a-Service - RaaS), cho phép các hacker thuê và tùy chỉnh mã độc để thực hiện các cuộc tấn công

**Đặc điểm**

* Đa dạng mục tiêu: Medusa chủ yếu nhắm vào các hệ thống Windows, khai thác các lỗ hổng trong các dịch vụ từ xa (RDP), các chiến dịch phishing tinh vi và các tài khoản đã bị xâm nhập.
* Mã hóa dữ liệu: Sau khi xâm nhập, Medusa sẽ tiến hành mã hóa tất cả các loại tệp tin quan trọng của nạn nhân, khiến dữ liệu trở nên vô dụng.
* Đòi tiền chuộc: Để lấy lại dữ liệu, nạn nhân sẽ bị buộc phải trả một khoản tiền chuộc bằng tiền điện tử.
* Rò rỉ dữ liệu: Ngoài việc mã hóa dữ liệu, Medusa còn có khả năng đánh cắp và rò rỉ dữ liệu của nạn nhân ra công khai, tạo thêm áp lực buộc nạn nhân phải trả tiền chuộc.
* Tránh phát hiện: Medusa sử dụng nhiều thủ thuật để tránh bị phát hiện, chẳng hạn như tắt các dịch vụ bảo mật, xóa nhật ký hệ thống và mã hóa các tệp cấu hình.

**Phương thức phá hoại**

* Khai thác lỗ hổng: Medusa thường khai thác các lỗ hổng chưa được vá trong các phần mềm và hệ điều hành để xâm nhập vào hệ thống.
* Phishing: Các email lừa đảo, các trang web giả mạo được sử dụng để lừa người dùng click vào các liên kết độc hại hoặc tải xuống các tập tin bị nhiễm mã độc.
* Truyền nhiễm qua mạng: Medusa có thể tự động lan truyền qua các máy tính trong cùng một mạng, gây ra thiệt hại lớn hơn.

**Biện pháp phòng chống**

* Cập nhật phần mềm: Luôn cập nhật hệ điều hành, các ứng dụng và phần mềm diệt virus lên phiên bản mới nhất để vá các lỗ hổng bảo mật.
* Sử dụng phần mềm diệt virus: Cài đặt và thường xuyên quét máy tính bằng phần mềm diệt virus uy tín.
* Sao lưu dữ liệu: Thường xuyên sao lưu dữ liệu quan trọng vào các thiết bị lưu trữ ngoại vi hoặc dịch vụ đám mây.
* Đào tạo nhận thức: Tăng cường nhận thức về các mối nguy hiểm của mã độc cho người dùng, giúp họ nhận biết và tránh các cuộc tấn công.
* Hạn chế truy cập từ xa: Hạn chế việc truy cập từ xa vào hệ thống nếu không cần thiết.
* Xác thực hai yếu tố: Sử dụng xác thực hai yếu tố để bảo vệ tài khoản.

**Nguồn tham khảo**

* **Bitdefender:** [**Medusa Ransomware: A Growing Threat with a Bold Online Presence**](https://www.bitdefender.com/en-us/blog/businessinsights/medusa-ransomware-a-growing-threat-with-a-bold-online-presence/)
* **ProvenData:** [**Medusa Ransomware: What You Need to Know - Proven Data**](https://www.provendata.com/blog/medusa-ransomware/)
* **Tên: Akira ransomware**

**Nguồn gốc:**

* Akira Ransomware được phát hiện và báo cáo vào năm 2023.

**Đặc điểm**

* Mã hóa dữ liệu: Giống như các loại ransomware khác, Akira mã hóa các tệp quan trọng của nạn nhân, khiến chúng trở nên không thể truy cập.
* Double extortion: Akira thường kết hợp phương thức mã hóa dữ liệu với việc đánh cắp dữ liệu. Tức là, ngoài việc mã hóa, kẻ tấn công còn sao chép dữ liệu của nạn nhân và đe dọa sẽ công khai nếu không nhận được tiền chuộc. Điều này tăng áp lực lên nạn nhân và làm tăng khả năng họ sẽ trả tiền.
* Khai thác lỗ hổng: Akira thường khai thác các lỗ hổng trong các hệ thống, phần mềm để xâm nhập vào mạng của nạn nhân. Ví dụ, nó có thể khai thác các lỗ hổng trong các thiết bị mạng như VPN, firewall.
* Phát triển liên tục: Giống như các loại malware khác, Akira không ngừng được phát triển và cải tiến để tránh bị phát hiện và loại bỏ.

**Phương thức phá hoại**

* **Phishing:** Kẻ tấn công thường sử dụng các email lừa đảo, các trang web giả mạo để lừa người dùng click vào các liên kết độc hại hoặc tải xuống các tệp bị nhiễm mã độc.
* **Khai thác lỗ hổng:** Akira lợi dụng các lỗ hổng chưa được vá trong các phần mềm, hệ điều hành để xâm nhập vào hệ thống.
* **Truyền nhiễm qua mạng:** Sau khi xâm nhập vào một máy tính, Akira có thể tự động lan truyền sang các máy tính khác trong cùng một mạng.

**Biện pháp phòng chống**

* Đảm bảo các bản sao lưu này được cập nhật thường xuyên và kiểm tra định kỳ để đảm bảo tính toàn vẹn.
* Luôn cập nhật phần mềm, ứng dụng và hệ điều hành để khắc phục các lỗ hổng bảo mật. Các ransomware thường khai thác các lỗ hổng đã biết để tấn công vào hệ thống.
* Sử dụng phần mềm chống mã độc và chống ransomware từ các nhà cung cấp uy tín và cập nhật định kỳ. Chọn phần mềm có khả năng phát hiện ransomware và các hành vi đáng ngờ, từ đó có thể ngăn chặn mã độc trước khi nó thực thi.
* Sử dụng tài khoản không có quyền admin để giảm thiểu rủi ro từ ransomware.
* Tắt tính năng truy cập từ xa không cần thiết
* Cảnh giác khi mở email và tải xuống tệp. Hạn chế tải xuống các tệp hoặc phần mềm từ các trang web không đáng tin cậy.
* Sử dụng giải pháp mạng an toàn như thiết lập firewall và IDS/IPS để giám sát lưu lượng mạng, phát hiện và ngăn chặn lưu lượng đáng ngờ có thể là dấu hiệu của ransomware.
* Áp dụng xác thực đa yếu tố (MFA) đối với các tài khoản quan trọng để tăng cường bảo mật và ngăn chặn truy cập trái phép ngay cả khi tên người dùng và mật khẩu bị đánh cắp.
* Theo dõi và phát hiện các mối đe dọa bảo mật. Triển khai giải pháp giám sát bảo mật (SIEM) để phát hiện các hoạt động đáng ngờ hoặc dấu hiệu của mã độc. Tạo cảnh báo ngay khi phát hiện hoạt động bất thường có liên quan đến ransomware.

**Nguồn tham khảo**

* **Bleepingcomputer:**

[**Akira and Fog ransomware now exploit critical Veeam RCE flaw**](https://www.bleepingcomputer.com/news/security/akira-and-fog-ransomware-now-exploiting-critical-veeam-rce-flaw/)

[**FBI: Akira ransomware raked in $42 million from 250+ victims**](https://www.bleepingcomputer.com/news/security/fbi-akira-ransomware-raked-in-42-million-from-250-plus-victims/)

* **Trendmicro:** [**Ransomware Spotlight: Akira | Trend Micro (US)**](https://www.trendmicro.com/vinfo/us/security/news/ransomware-spotlight/ransomware-spotlight-akira)