# **Phân loại malware**

## **Malicious Software (malware) là gì?**

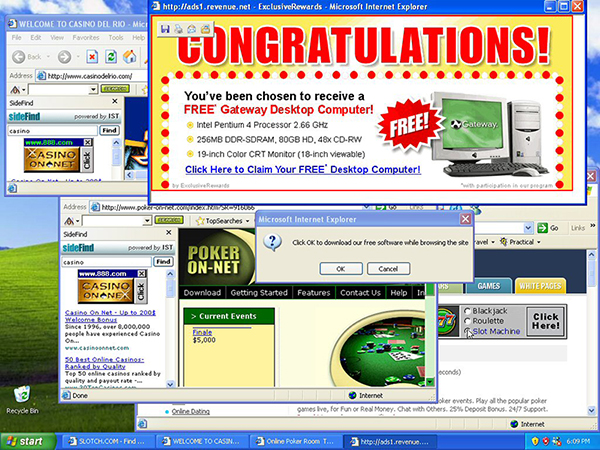
**Malware** là chương trình được viết với mục đích gây hại và lây nhiễm vào hệ thống. Malware bao gồm viruses, trojan horses, worms, spyware, adware và một loại cực kỳ nguy hiểm xuất hiện vài năm gần đây là Ransomware.

## **Những loại malware hiện nay.**

* **Virus**:

Virus là 1 loại đặc biệt của malware. Nó có một đoạn code có thể nhiễm vào chương trình khác và gây hại khi được chạy. Nó được biết đến là sẽ gây hại khi chương trình được chia sẻ giữa các máy tính. Hành vi này thường được xem như ký sinh trùng.

* + **File infector viruses**: Loại virus này thì thường lây nhiễm vào file những đoạn mã thực thi vào file thực thi khác ví dụ như .com và .exe files. Ngoài ra nhiều virus của loại này còn lây nhiễm vào Memory. Sau khi Memory bị lây nhiễm, bất kỳ một chương trình chưa bị lây nhiễm nào khác, khi được thực thi sẽ bị nhiễm. Ví dụ 2 con virus lây nhiễm file nổi tiếng được biết đến là Jerusalem và Cascade.
  + **Boot sector viruses**: Loại này sẽ lây nhiễm vào khu vực hệ thống của đĩa(hiện nay rất hiếm thấy xuất hiện). Tất cả các đĩa cứng đều chứa 1 chương trình nhỏ trong boot record mà sẽ được thực thi khi máy tính khởi động. Boot sector virus sẽ gắn chúng vào phần này của đĩa và sẽ được thực thi khi người dùng khởi động máy tính. Một số loại nổi tiếng như Form, Disk Killer, Stoned…
  + **Multipartite viruses**: Là loại virus được kết hợp từ 2 loại File infector virus và Boot sector virus. Ví dụ như virus One\_Half, Emperor, Anthrax, Tequilla.
  + **Macro viruses**: Loại này lợi dụng macro (sử dụng Visual Basic for Application) trên các chương trình của Microsoft Office để phán tán và lây nhiễm. Ví dụ như virus W97M.Melissa, WM.NiceDay và W97M.Groov.
* **Adware**:



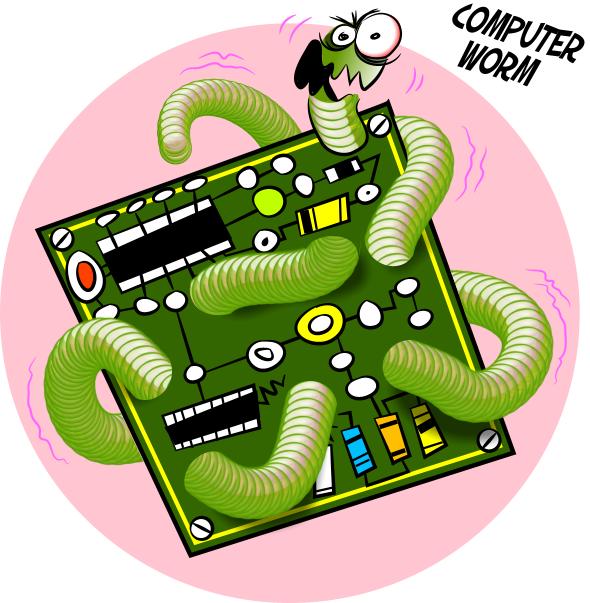
Adware được biết đến là một chương trình hỗ trợ cho việc quảng cáo. Nó hiện những quảng cáo cho mục đích lợi nhuận. Những quảng cáo đó được xuất hiện vào thời điểm người dùng cài đặt phần mềm. Không phải tất cả adware đều độc hại, nhưng nó trở thành một vấn đề bởi nó ảnh hưởng xấu đến hiệu suất của máy tính và có thể gây phiền phức.

* **Spyware**:



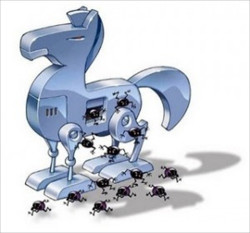
Spywarelà loại chương trình gián điệp trên hệ thống của bạn, nó sẽ theo dõi và thu thập những hành động trên Internet của bạn. Nó giúp những hacker trong việc thu thập thông tin về hệ thống của nạn nhân mà không được sự cho phép. Spyware thì thường ẩn bên trong chương trình chủ và rẩt khó để phát hiện. Một số spywrae như keylogger có thể được cài đặt bên trong thiết bị phần cứng để theo dõi hoạt động của người dùng.

* **Worms**:



Worms là loại phần mềm độc hại này sẽ tự nhân bản và phá huỷ thông tin và toàn bộ files được lưu trữ trên máy nạn nhân. Nó hoạt động để “ăn” hết tất cả files của HĐH và files trên đĩa. Cơ lây nhiễm của nó hoàn toàn “active” bằng việc khai thác lỗ hổng của HĐH.

* **Trojan**:



Trojan là loại malware được thiết kể để khiến người dùng tin rằng nó là chương trình an toàn và thực thi chúng. Nó có thể được lập trình để đánh cắp thông tin cá nhận và thông tin tài chính của người dùng, sau đó là chiếm hữu toàn bộ tài nguyên của các tệp tin hệ thống máy chủ. Trong những hệ thống lớn, nó có thể cố gắng khiến cho hệ thống máy chủ hoặc tài nguyên mạng trở nên không khả dụng để phát hiện nó. Ví dụ: mạng doanh nghiệp của bạn sẽ trở nên vộ dụng.

* **Ransomware**:



Ransomware là loại malware khi lây nhiễm sẽ vô hiệu hoàn toàn máy tính của nạn nhân hoặc thậm chí sẽ mã hoá các file quan trọng của nạn nhân. Sau đó, những tên hacker sẽ để lại một thông báo trên màn hình yêu cầu nạn nhân phải trả tiền cho chúng để nhận được chìa khoá giải mã. Ransomware có mức độ lây lan mạnh hiện nay là WannaCry, malware này có cơ chế phát tán giống như worm.

# **Các dấu hiệu nhận biết máy tính bị nhiễm malware**

## **Máy tính hoạt động chậm chạp**

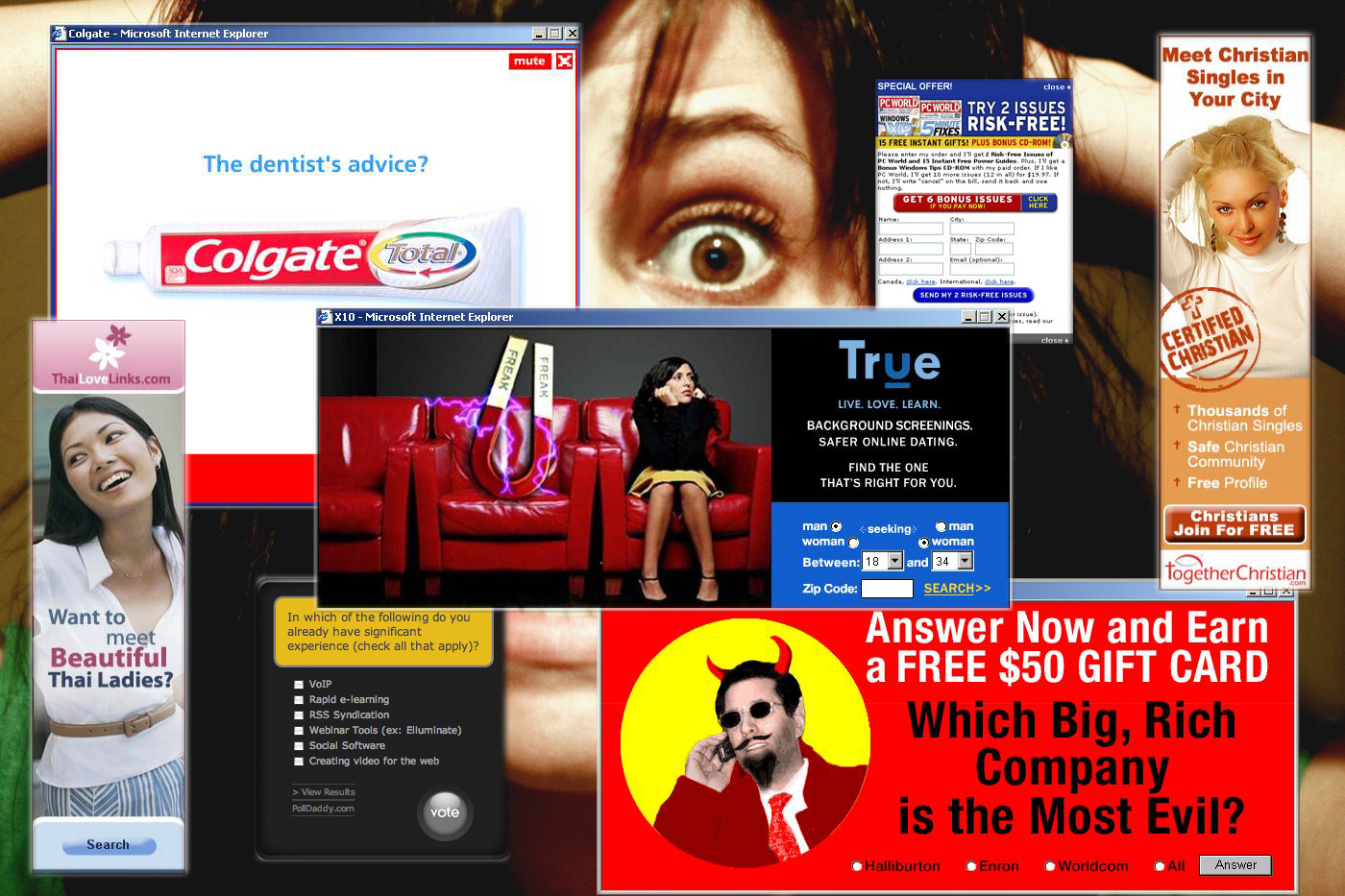


- Bạn phải mất rất nhiều thời gian để khởi động máy tính.

- Bạn phải đợi rất lâu để khởi đồn một chương trình.

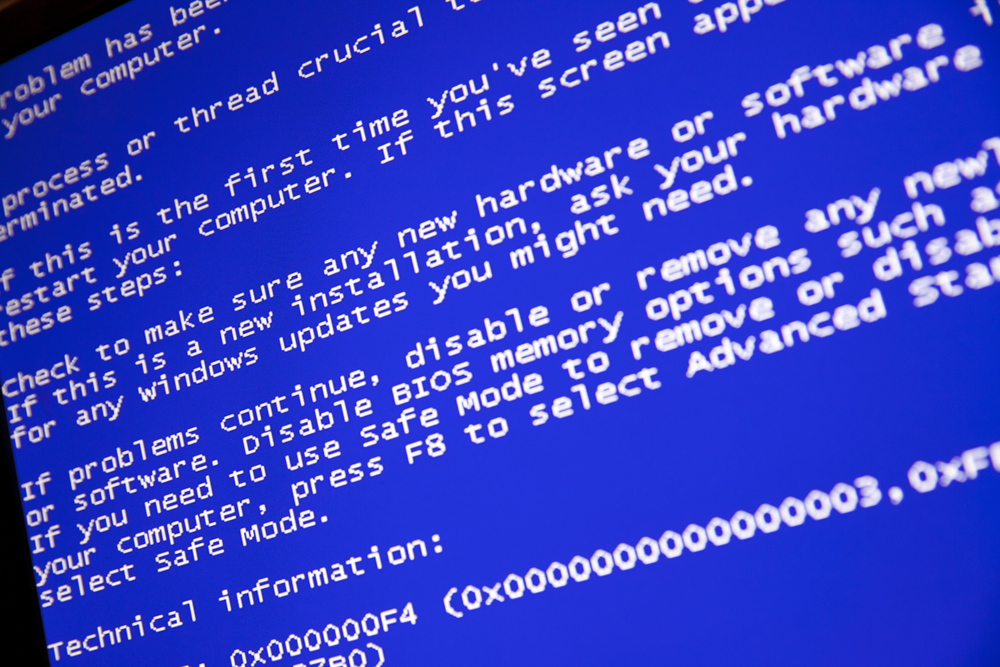
Các malware thường có khuynh hướng làm chậm hệ thống máy tính, tốc độ truy cập Internet hoặc tốc độ của những chương trình khác.

## **Xuất hiện những hộp quảng cáo**



Trường hợp này xảy ra khi máy tính bị lây nhiễm Adware.

## **Đột ngột bị crashed nhiều lần liên tục**

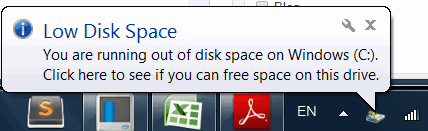


Nếu máy tính của bạn xuất hiện màn hình xanh (Blue Screen of Death) liên tục thì khả năng cao máy tính của bạn đã bị nhiễm malware hoặc có xung đột giữa phần mềm và phần cứng.

## **Xuất hiện những hoạt động đáng ngờ tại các ổ đĩa**

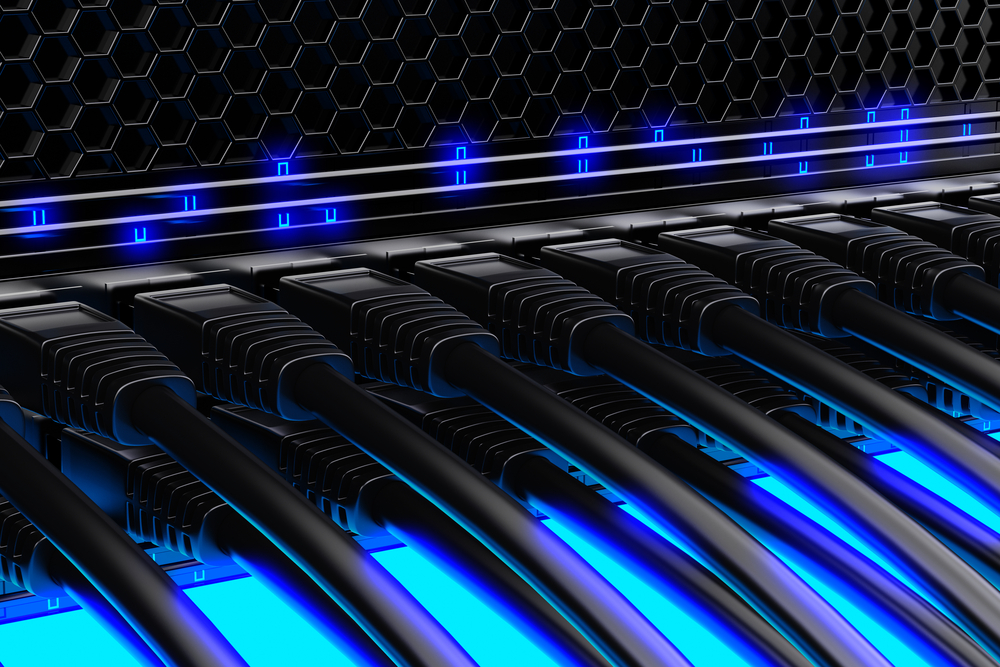
Nếu ổ đĩa liên tục thể hiện những hoạt động kỳ lạ ngay cả khi bạn không sử dụng hay là không có chương trình hoặc các tác vụ download đang chạy, thì có thể máy tính đã bị nhiễm malware. Ngoài ra cũng có một khả năng khác là do ổ đĩa của bạn bị hỏng.

## **Đột ngột hết dung lượng các ổ đĩa**



Khi ổ đĩa đột ngột hết dung lượng thì chắc chắn máy bạn đã bị nhiễm malware.

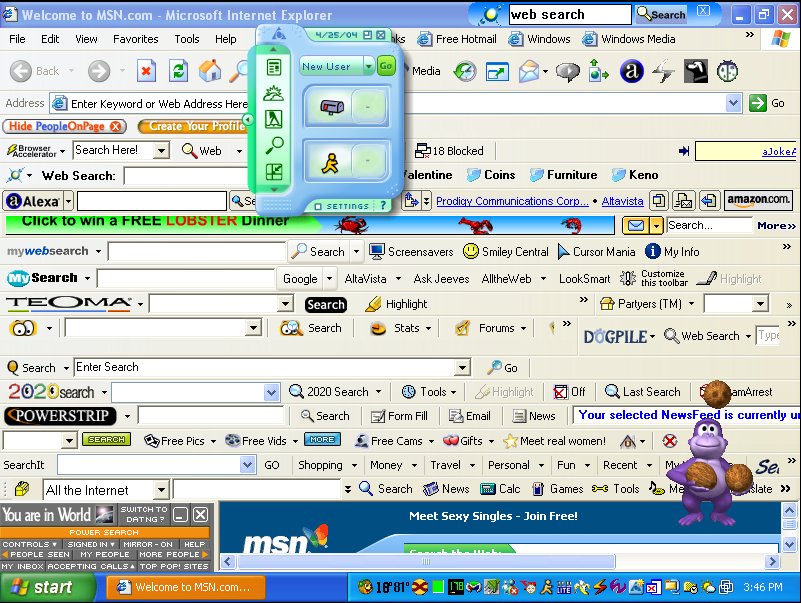
## **Hoạt động kết nối mạng của máy tính gia tăng bất thường**



Nếu như bạn không truy cập Internet hoặc không có tác vụ download nào đang diễn ra nhưng hoạt động mạng của máy tính vẫn ở mức cao thì có khả năng cao máy tính đang bị nhiễm malware và đặt biệt là botnet.

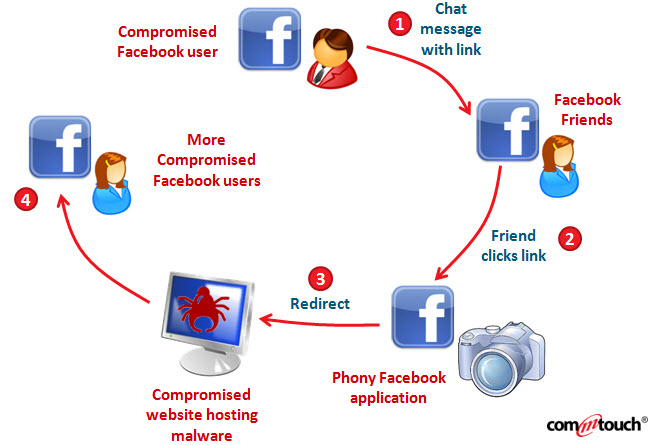
Tuy nhiên bạn cũng nên kiểm tra là có phải do hoạt động Update của Windows đang diễn ra hay không.

## **Browser bị thay đổi homepage, bị cài đặt nhiều plugin lạ**



Những hiện tượng này thường đi kèm sau khi máy tính bị nhiễm adware.

## **Bạn bè thông báo rằng nhận được các tin nhắn lại từ bạn**



Lúc này chắc chắn một điều rằng quyền riêng tư của bạn đã bị xâm phạm. Có 2 trường hợp, một là bạn bị nhiễm virus Spammer, hai là tài khoản mạng xã hội hoặc mạng trò chuyện của bạn đã bị hacker đánh cắp.

# **Phòng ngừa và khắc phục hậu quả do malware gây ra**

## **Phòng ngừa**

* Tạo bản sao hệ điều hành (hay còn gọi là “Ghost HĐH”) bằng chương trình như Norton Ghost.
* Thường xuyên tạo các Point trong System Restore.
* Sử dụng AntiVirus chất lượng như Kaspersky, Nortron, Panda, …
* Không truy cập vào các trang web đen.
* Luôn luôn quét các thiết bị gắn ngoài khi kết nối vào máy tính.
* Sử dụng HĐH có bản quyền và thường xuyên cập nhật các bản vá lỗi.

## **Khắc phục**

* Nếu hệ thống máy tính bị nhiễm các loại malware như worm hay ransomware thì cách duy nhất là “ghost” lại hệ điều hành hoặc sử dụng System Restore.
* Ngoài ra, sau khi AntriVirus diệt được virus có thể sẽ gây ra các lỗi hệ thống, lúc này nên sử dụng các công cụ sử lỗi như Fix Auto, VnFix (dành cho Windows) để khắc phục.
* Cách cuối cùng là nhờ các kỹ thuật viên của AntiVirus bạn đang sử dụng (nếu có bản quyền) hoặc đem ra cửa hàng tin học để được tư vấn khắc phục.

# **Kỹ thuật lây nhiễm virus**

## **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.

## **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 lệnh 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.



## **Prepending Viruses**

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



## **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.

## **Fractionated Cavity Viruses (biến thể của Cavity virus)**

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



## **Compressing Viruses**

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



## **Embedded Decryptor Technique**

Những virus này sẽ mã hoá 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 mã độc của virus và thực thi chúng.



# **AntiVirus**