1. 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.

1. 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 của nó thì 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 chương bị lây nhiễm khi thực thi sẽ bị nhiễm. Ví dụ 2 con virus lây nhiễm file nổi tiếng được biết đến là Jerusalen và Cascade.
  + Boot sector viruses: Loại này sẽ lây nhiễm vào khu vực hệ thống của đĩa. 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 là chương trình trình bày những quảng cáo cho mục đích lợi nhuận của chủ nhân nó. 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: Là 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 để theo dõi hoạt động của người dùng.
* Worms: Loại phần mềm độc hại này sẽ tự nhân bản và phá huỷ thông tin và toàn bộ file s được lưu trữ trên máy nạn nhân. Nó hoạt động để “ăn” hết tất cả files của HĐH và files trên đĩa.
* Trojan: Đây là loại malware được thiết kể để khiến người dùng tin rằng nó là chương trình an toàn àn thực thi chúng. Nó có thể được lập trình để đánh cắp thông tin cá nhận và thông tin tài chính của người dùng và 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: Đây 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.