**ÔN TẬP MÃ ĐỘC MẤY TÍNH**

**Câu 1:**

1. **Mã độc là gì?**

**Khái niệm:** là các chương trình máy tính được tạo ra với mục đích làm hại đến tính bí mật, tính toàn vẹn hoặc tính săn sàng của dữ liệu, ứng dụng và hệ điều hành của của hệ thống.

* Phát triển song hành cùng các thời kỳ của máy tính.
* Mã độc không tự sinh ra mà được tạo ra bởi con người và có thể mang các mục đích khác nhau như: phá hoại, thử nghiệm hay đơn giản chỉ là một trò đùa ác ý.

1. **Phân loại mã độc, liệt kê**

Phân loại dựa vào hình thức lây nhiễm, gồm 2 dạng chính:

* Dạng thứ nhất cần vật chủ để tồn tại và lây nhiễm, vật chủ ở đây có thế là các tệp dữ liệu, các tệp ứng dụng, hay các tệp chương trình thực thi. Mã độc thuộc dạng này chỉ là một đoạn mẵ đặc biệt cùa một chương trình máy tính không thể thực thi độc lập như một chương trình thông thường mà bắt buộc phải có bước kích hoạt của chương trình chủ thì mới có thể hoạt dộng được. Một số loại mã độc phổ biến thuộc dạng này là: Virus, Trojan, Trap Doors, Logic Bombs.
* Dạng thứ hai tồn tại độc lập như là các chương trinh độc hại có thể chạy trên hệ điều hành, một số loại mã độc thuộc dạng này là: Worms, Zombie.

1. **Trình bày hiểu biết về virus**

Virus là một loại mã độc có khả năng tự nhân bản và lây nhiễm chính nó vào các tệp, chương trình máy tính. Virus phải luôn bám vào vật chủ đế lây lan.

**Đặc điểm** của Virus là nó có thể tự đính kèm vào một chương trình khác và thực thi bí mật khi chương trình mang virus kích hoạt. Khi virus được thực thi nó có thể làm bất kỳ việc gì trên hệ thống như thay đổi, sao chép hoặc xó các tệp chương trinh. Vòng đời virus gồm 4 giai đoạn:

* Trú ẩn (Dormant): Giai đoạn này virus không làm gì cho đến khi được kích hoạt bởi một sự kiện nào đó.
* Lây lan (Propagation): Giai đoạn này virus thực hiện việc copy chính nó tới các chương trình, vị trí khác trong ổ đĩa.
* Kích hoạt (Triggering): Giai đoạn này virus được kích hoạt để thực thi chức năng của nó.
* Thực thi (Execution): Chức năng của virus được thực thi, chức năng có thể là vô hại như gửi một thông điệp nào đó tới màn hình, hoặc một chức năng có hại như phá hủy các chương trình, các tệp của hệ thống.

1. **Các loại virus chính**

* Virus thường trú (Memory - resident virus): Cư trú trong bộ nhớ chính như là một phần của chương trình hệ thống. Theo đó virus sẽ gây ảnh hưởng mỗi khi chương trình được thực thi.
* Virus tệp chương trình (Program fíle virus): Gây ảnh hưởng đến các tệp chương trình như exe/com/sys.
* Virus đa hình (Polymorphic yirus): Loại virus này tự thay đổi hình thức của nó, gây khó khăn cho các chương trinh Anti-virus. Virus “Tequilla” là loại virus đa hình đầu tiên xuất hiện năm 1991.
* Virus Boot (Boot Sector virus): Là loại virus đầu tiên trên thế giới được phổ biến rộng rãi và được viết vào năm 1986. Virus Boot lợi dụng tiến trình khôi động của máy tính để thực hiện việc kích hoạt mình. Khi máy tính được khởi động, nó luôn tìm đến master boot record để tấn công.
* Virus Stealth: Đây là loại virus có khả năng tự che giấu không để cho hệ điều hành và phần mềm Anti-virus biết. Nó nằm trong bộ nhớ để ngăn chặn sử dụng hệ điều hành và che giấu những thay đổi về kích thước các tập tin.
* Virus Macro: Là tập lệnh được thực thi bởi một ứng dụng văn phòng. Virus Macro phổ biến trong các ứng dụng Microsoft Office khi tận dụng khả năng kiểm soát việc tạo và mở tệp để thực thi và lây nhiễm.
* Virus Email: Là những virus được phát tán qua thư điện tử. Ví dụ virus Melissa được đính kèm trong thư điện tử. Nếu người dùng mở tệp đính kèm Macro được kích hoạt sau đó virus tự động gửi chính nó tới tất cả những hòm thư có trong danh sách thư của người đó.

1. **Trojan hourse**

**Khái niệm:** là loại mã độc được đặt theo sự tích “Con ngựa thành Troy”, không có khả năng tự nhân bản, ẩn chứa các đoạn mã với mục đích gây hại.

**Các hoạt động?**

Không tấn công trực tiếp bằng cửa trước dễ bị phần mềm quét virus và tường lửa máy tính phát hiện. Tin tặc đã chèn mã độc, virus trong các phần mềm khác. Một khi virus hoạt động, nó sẽ lây lan rất nhanh và để lại hậu quả khó lường nếu người dùng không có phản ứng ngăn chặn sự cố kịp thời.

**Bắt nguồn?**

* Đường dẫn hoặc tệp tin đính kèm trong email
* Khai thác ứng dụng: Ví dụ các lỗ hổng trong trình duyệt web, phần mềm hoặc ứng dụng nhắn tin. Lỗ hổng này chủ yếu xuất phát từ việc người dùng không thường xuyên cập nhật bản vá lỗi của nhà sản xuất.
* Phần mềm tải về: Việc tải phần mềm từ những trang lưu trữ tài nguyên hoặc các mạng chia sẻ tệp tin có thể chứa nhiều loại phần mềm độc hại, bao gồm cả Trojan.

**Chú ý:** Những phương pháp tấn công này có thể được thực hiện trực tiếp hoặc gián tiếp dựa vào điểm yếu của thiết bị.

**Hậu quả?**

Trojan có thể gây hại theo ba cách sau:

* Thực hiện các chức năng của chương trình chủ một cách bình thường, đồng thời thực thi các hoạt động gây hại một cách riêng biệt (ví dụ: như gửi một trò chơi dụ cho người dùng sử dụng)
* Thực thi các chức năng của chương trình chủ, nhưng sửa đổi một số chức năng để gây hại (ví dụ như một Trojan giả lập một cửa sổ login để lấy password)
* Che giấu các hành động phá hoại khác (ví dụ: như Trojan che giấu cho các tiến trình độc hại khác bằng cách tắt các hiển thị của hệ thống).

**Giải pháp**?

Thông qua nguồn gốc lây nhiễm của Trojan, chúng ta có thể thực hiện các phương pháp phòng tránh như:

* + Không click vào các tệp tin, đường dẫn trong email được gửi từ người lạ.
  + Không tải về các phần mềm khi chưa biết rõ nguồn gốc do ai viết, có virus hay không, phần mềm có yêu cầu truy cập quyền riêng tư người dùng không.
  + Không bấm trực tiếp vào các đường link rút gọn đuôi adf.ly hoặc các link rút gọn khác được chia sẻ trên forum, mạng xã hội. Thay vì đó, bạn có thể copy đường dẫn và paste vào trang virustotal để kiểm tra. Nếu an toàn thì bạn tải về hoặc xem tiếp nội dung đó.
  + Cập nhật bản vá lỗ hổng thường xuyên cho Windows và các phần mềm khác.
  + Bật tường lửa và sử dụng trình diệt virus.

1. **Botnet**

**Khái niệm:**  là mạng lưới các máy bị xâm nhập bởi phần mềm client nào đó.Một bot trong đó đang được điều khiển tập trung bởi một ứng dụng server như Botmaster.

**Vòng đời:** Vòng đời hoặc thời gian của một botnet phụ thuộc vào cách tạo ra botnet. Nó có thể xác định trong giai đoạn như sau:  
1. Kẻ tấn công(bot-herder) quyết định các thông số bot ban đầu như hướng lây nhiễm, tần suất, C&C chi tiết.  
2. Đăng ký DDNS (Dynamic DNS). Để điều khiển botnet có thể thay đổi địa chỉ IP và tạo ra bộ điều khiển bot mới hoặc nội dung bất cứ khi nào cần thiết.  
3. Đăng ký một IP tĩnh.  
4. Bot-herder hoạt động hoặc tìm kiếm những bot mới.  
5. Bots lây lan.  
6. Tấn công nạn nhân bằng DDoS hoặc thư rác hoặc lừa đảo.v.v  
7. Bị mất các bot

**Mục đích?**

Có thể là:

* Gửi mail spam: cách thức kiếm tiền phổ biến của các Spammer. Hơn nữa các Botnet cũng tạo ra các web gian lận chèn bổ sung quảng cáo chạy trên nền web, người sử dụng tương tác click vào link quảng cáo sẽ tạo ra tiền cho các Hacker.
* Các cuộc tấn công DdoS dùng Botnet xảy ra liên tục. Bot Herder sẽ lập trình ra một link website bất kỳ nào đó và điều khiển tất cả các máy tính là nạn nhân của Bot truy cập vào website đó, tạo ra tình trạng nghẽn mạng, dẫn đến không truy cập được nữa. Gửi hăm dọa, làm gian lận và tống tiền người dùng.
* Botnet đào tiền ảo từ một máy tính lớn, giúp chúng thu về tiền ảo như Bitcoin và các chi phí khác sẽ bị chịu bởi người dùng.

**Quy trình hoạt động của Botnet:**

Đánh vào những lỗ hổng an ninh, những mảng vá cũ hay những server lỗi thời hết hạn, các Bot nằm ẩn mình trong các máy khách – kết nối sẵn với Botmaster, chỉ đợi lệnh và điều khiển từ Botmaster để tiến hành hoạt động của mình. Sau khi nhận lệnh từ Hacker, mỗi Bot có một hoạt động riêng tùy theo sự điều khiển từ phía ngoài. Nó có thể tấn công theo nhiều cách như là: Tạo Spam, tấn công DdoS, chiếm giữ hệ thống, lừa đảo ăn cắp Bitcoin. Mục đích cuối cùng là điều khiển hoạt động của máy tính bị nhiễm, buộc người dùng phải làm theo mệnh lệnh của nó.

**Phân loại Botnet:**

Botnet có 2 loại cơ bản là DNS và IRC. Mỗi loại có một chức năng riêng và ưu điểm riêng.

**DNS Bot**: dễ thực hiện và điều khiển đơn giản không quá cầu kỳ, được dùng để chạy Bot trên nền Web. Nhưng vẫn bị hạn chế trong việc trao đổi thông tin giữa Bot master và các Bot.

**IRC Bot:** Giúp trao đổi thông tin giữa Bot Master và các Bot, điều khiển qua mạng chat IRC. Nhưng lại bị phụ thuộc vào các IRC và người quản trị Server.

**Giải pháp phòng vệ Botnet :**

* Phần mềm chống Virut mới nhất
* Nâng cấp tường lửa
* Cập nhật phần mềm mới và cài đặt các mảng vá lỗi liên tục
* Làm theo hướng dẫn về bảo mật cho máy tính bạn

1. **Zombie**

Zombie là chương trình độc hại bí mật liên kết với một máy tính khác ngoài internet để nghe lệnh từ các máy tính đó. Các Zombie thường sử dụng trong các cuộc tấn công từ chối dịch vụ DDoS để tấn công vào một website nào đó. Kiểu thông dụng nhất của Zoombie là các agent dùng để tổ chức một cuộctấn công DDoS. Kẻ tấn công có thể cài Zoombie vào một số lượng lớn các máy tính rồi ra lênh tấn công cùng một lúc.  
**Ví dụ** Trinoo và Tribe Flood Network là hai Zoombie nổi tiếng được sử  
dụng như các công cụ để thực hiện tấn công DDoS.

1. **Ransomware**

**Khái niệm:** Đây là cách gọi tên của dạng mã độc mới nhất và có tính nguy hiểm cao độ đối với nhân viên văn phòng, bởi nó sẽ mã hóa toàn bộ các file word, excel và các tập tin khác trên máy tính bị nhiễm làm cho nạn nhân không thể mở được file

**Phòng ngừa:**

* Không mở các file đính kèm từ email không rõ
* Đảm bảo hệ điều hành, phần mềm, các ứng dụng và phần mềm diệt virus được cập nhật thường xuyên và không tắt chương trình Kaspersky
* Đảm bảo tính năng giám sát hệ thống của Kaspersky đã được bật.
* Luôn sao lưu và bảo vệ dữ liệu bằng các thiết bị rời và chỉ có thể truy cập trong quá trình sao lưu.
* Cấu hình hạn chế truy cập đến các thư mục chia sẻ trong mạng.
* Bật tính năng System Protection (System Restore) cho tất cả các ổ đĩa

1. **Trình bày hệ lây nhiễm file của virus**

* **Cơ chế hoạt động**
* Thực thi các tệp (.exe, .com….) OS cung cấp vùng nhớ cho các chương trình; tải tệp cùng các thư viện; trao quyền điều khiển cho chương trình;
* Virus lợi dụng, chèn đoạn mã vào tệp đúng vị trí mà OS trao quyền điều khiển cho tệp trên vùng nhớ;
* Sau khi tiến hành xong thì mới trả lại quyền điều khiển cho chương trình; người sử dụng không hề hay biết;
* Virus có thể lây nhiễm vào tệp hoặc nhiều kiểu tệp khác nhau để thực thi
* Để tiến hành lây nhiễm thì Virus tệp phải tiến hành một số bước như sau:
* Tìm kiếm các tệp thực thi để lây nhiễm.
* Tìm kiếm trong thư mục hiện hành;
* Tìm kiếm trog các thư mục đặc biệt của hệ thống (Windows, system32, user)
* Thực hiện lây nhiễm vào các tệp tìm được.
* Chiếm quyền điều khiển, thực hiện mục đích trước khi trả lại quyền cho chương trình.
* Khi trả lại quyền thì tất cả dữ liệu của tệp phải được đảm bảo an toàn.
* Một số kỹ thuật để thực hiện việc lây nhiễm như: thêm, ghi đè, chèn, định hướng lại và đồng dạng.

***/\* các ví dụ sau có thể có có thể k có thể bỏ đi nếu thấy dài \*/***

VD: thêm

VD: ghi đè

* Đảm bảo kích thước của tập tin
* Đảm bảo cấu trúc tập tin, không hỏng chương trình ban đầu.

*Có hai phương pháp ghi đè:*

* Ghi đè lên 1 phần và chuyển một nội dung ở chương trình gốc sang một nơi khác.
* Nén một nội dung mã ban đầu, sau đó sử dụng bộ nhớ thực thi công việc rồi sau đó trả lại cho chương trình ban đầu.
* VD: **Kỹ thuật chèn**
* Virus chèn mã của nó trực tiếp lên vùng chứa các đoạn dữ liệu của không sử dụng của chương trình thực thi.
* Giống với kỹ thuật thêm, khác là mã virus không chèn ở đầu hoặc cuối chương trình mà nằm ngay trong đoạn mã tệp chương trình.

VD: định hướng lại

* Các đoạn mã được giấu trong một vài vùng nhớ vật lý trên đĩa, như boot sector hay tệp ẩn.
* Sử dụng các kỹ thuật thêm hoặc chèn để cấy virus trong các tệp chương trình.
* Virus thành phần được kích hoạt khi đoạn mã điều khiển chạy
* Đoạn mã Virus điều khiển quá trình tìm kiếm lây nhiễm sau đó trả điều khiển cho chương trình chủ. Loại virus này dễ bị tiêu diệt khi bị phát hiện, chỉ cần xóa các virus điều khiển tại các vị trí ẩn náu của chúng sẽ vô hiệu hóa các virus thành phần.

VD: đồng dạng

* Biến đổi bản thân nó có các đặc tính giống tệp mục tiêu để giành được sự ưu tiên thực thi trước khi thực thi chương trình gốc.
* *Một số phương pháp đồng dạng:*
* Virus đồng dạng đặt chính nó trước con đường tìm kiếm các tệp thực thi của hệ điều hành (tạo nên tên trùng với tên của tệp thực thi).
* Ví dụ: hệ điều hành MS-DOS tìm kiếm một tệp thực thi có tên là fo bằng cách tìm kiếm theo thứ tự ưu tiên fo.com, fo.exe và fo.bat. Nếu các tệp mục tiêu là một tệp EXE, khi đó virus đồng dạng có thể là một tệp COM có cùng tên.
* Thực hiện kỹ thuật đảm bảo tính tồn tại duy nhất
* Yêu cầu đặt ra với các virus là tính tồn tại duy nhất của mình trong bộ nhớ cũng như trên mỗi tệp.
* Trong vùng nhớ, virus sử dụng 2 kỹ thuật chính:
* Tạo thêm chức năng kiểm tra, gọi chức năng này, giá trị trả lại trong thanh ghi sẽ quyết định sự tồn tại trong bộ nhớ hay chưa.
* So sánh một đoạn mã trong vùng nhớ ấn định với đoạn mã của virus, nếu có sự chênh lệch thì có nghĩa là chưa có mặt trong vùng nhớ
* Trong các tệp chương trình
* Kiểm tra logic đối với các thông tin của Entry trong thư mục của tệp.
* Kiểm tra dò một đoạn mã đặc trưng tại một vị trí ấn định nào đó trên tệp, như như byte cuối cùng của tệp.

**Câu 2: Mô tả các bước 3- 4 dòng**

Có 2 phương pháp phân tích mã độc chính đó là:

* Phân tích tĩnh: phân tích mã nguồn và Gỡ rối (Debug)
* Phân tích động: phân tích và Điều tra hành vi của mã độc

Cả 2 cùng giải thích cách hoạt động của mã độc, công cụ, tuy nhiên thời gian làm việc và kỹ năng cần có thì lại rất khác nhau. Phân tích tĩnh thường đòi hỏi người phân tích xem xét kỹ mã của virus (đã được chuyển sang dạng có thể hiểu được, như assembly, hay C), hiểu được luồng thực thi và các hành vi của nó thông qua mã đã dịch ngược. Phân tích động là phân tích cách hoạt động của virus khi nó được thực thi, nó kết nối đến đâu, lây lan như thế nào, cài đặt những gì vào hệ thống, thay đổi thành phần nào, hoạt động ra sao. Mỗi phương pháp đều có điểm mạnh, yếu riêng.

**So sánh 2 phương pháp phân tích mã độc**

**Tĩnh:** với những loại virus phức tạp, thì để đọc hiểu được hết mã thực thi của nó là một việc rất khó; nhưng cung cấp cho người phân tích cái nhìn hết sức chính xác về những gì mà nó làm.

**Động:** quá trình phân tích diễn ra nhanh hơn, dễ dàng hơn; nhưng không phải hành vi nào cũng phân tích được, VD những loại virus phát hiện ra công cụ phân tích thì nó sẽ không hoạt động nữa, hoặc virus chờ đến một lúc nào đó mới hoạt động.

* cần phải kết hợp cả 2 phương pháp trên để đạt được hiệu quả tốt nhất.

**Công cụ sử dụng trong 2 phương pháp phân tích mã độc**

Về công cụ, cả 2 phương pháp này cũng tương đổi khác nhau:

* Phân tích tĩnh được thực hiện dưới sự hỗ trợ của các công cụ debugger, disassembler, decompiler (như OllyDbg, IDA, WinDbg…).
* Trong khi phân tích động dựa vào các công cụ monitor hệ thống, mạng (như ProcessMon, network monitor, TcpView, Autoruns…).

1. **Nguyên lý phân tích mã độc (đặc trưng, bất thường)**

**Dựa vào dấu hiệu đặc trưng**

**Ưu thế:**

* Phát hiện chính xác các mã độc nếu **signature** trùng khớp với các mẫu trong tập mẫu **nhận dạng**

**Hạn chế:**

* Xây dựng tập các signature là vô cùng **khó khăn**.
* **Không phát hiện được** các **mã độc mới**,

các zero-days.

* Việc lưu trữ và đối chiếu signature gặp khó khăn

|  |  |
| --- | --- |
| Kỹ thuật | Nội dung |
| Tĩnh | Dịch ngược chương trình, đối chiếu các đoạn mã để xác định có chứa mã độc hay có phải mã độc k. Xác suất nhận dạng gần như tuyệt đối chính xác nhg mất time |
| Động | Xác định chính xác mã độc bằng việc sử dụng các thông tin thu thập đc từ chương trình có quyền kiểm tra và đối chiếu vs các tập mẫu |
| Kết hợp | Sử dụng cả 2 |

**Dựa vào đặc điểm bất thường**

**Ưu thế:**

* Là chìa khóa để có thể phát hiện ra các khai thác **zero-day** hay **zero-attack**.

**Hạn chế:**

* **Sai số** giữa trạng thái bình thường và bất thường
* Sự **phức tạp**, rắc rối khi xác định những trạng thái

|  |  |
| --- | --- |
| Kỹ thuật | Nội dung |
| Tĩnh | Các đặc trưng về cấu trúc tệp tin của chương trình sẽ đc dùng để kiểm tra và xác định có pải mã độc k? Đặc điểm nổi bật của cách này là có thể phát hiện mã độc nhg k cho chương trình mã độc thực thi |
| Động | các thông tin thu được từ việc thực thi chương trình sẽ đc sử dụng để phát hiện mã độc. Ở giai đoạn phát hiện, ng thực hiện sẽ liên tục việc đối chiếu giữa các trạng thái mới và các trạng thái đã học đc. Và giai đoạn phát hiện đc triển khai trong suốt quá trình chương trình đc thực thi |
| Kết hợp | Sử dụng môi trg ảo có cấu trúc giống máy thật (máy ảo) để sử dụng cả 2 kỹ thuật trên |

1. **Kỹ thuật phát hiện mã độc (check..., fuzry hashsing)**

**Checksummers**

**Khái niệm:** là kỹ thuật phát hiện đối tượng mã độc trên cơ sở tính toàn vẹn của chương trình.

**Ưu điểm:**

* Độ chính xác gần như tuyệt đối.

**Nhược điểm:**

* Nhận dạng thiếu. Quá trình nhận dạng lâu nếu cơ sở dữ liệu mẫu lớn.
* Quá trình xây dựng cơ sở dữ liệu mẫu khó khăn, phức tạp. Mã độc có thể dễ dàng vượt qua nếu nhận dạng bằng mã hash.

**Fuzzy hashing**

**Khái niệm:** vẫn là nhận dạng mã độc qua mã hash nhưng đã được bổ sung thêm các phân tích và tính toán để từ một mã hash của mã độc, có thể nhận ra các mã hash “họ hàng”, nâng cao khả năng phát hiện.

**Ưu điểm:**

* **Cải thiện hơn** kỹ thuật Checksummers.
* Nâng cao khả năng phát hiện mã độc với **cơ sở dữ liệu mẫu bị hạn chế**.

**Nhược điểm:**

* Việc **xây dựng** **thuật toán** và **lựa chọn độ dài ký tự phù hợp** là **khó khăn.**
* Có thể xảy ra cảnh bảo giả (**cảnh báo sai**).

**Scan string**

**Khái niệm:** kỹ thuật sử dụng một chuỗi trích ngang (chuỗi bytes) là đặc trưng của tập tin mã độc và không tồn tại trong các tập tin sạch để làm cơ sở dữ liệu mẫu dùng để nhận dạng mã độc.

**Ưu điểm:**

* Nhận dạng **chính xác.**
* **Tốc độ** nhận dạng **nhanh** hơn so với kỹ thuật Checksummers.

**Nhược điểm:**

* Quá trình xây dựng và cập nhật cơ sở dữ liệu **phức tạp.**
* Nhận dạng **bị động**, không phát hiện được khi mã chương trình bị thay đổi.

1. **Quy trình phân tích mã độc**

Gồm 6 bước:

1. **Nhận diện hệ thống bị nhiễm**
2. Phát hiện sự cố mã độc

Dựa vào dấu hiệu:

* Hệ thống tự động tắt hoặc đăng xuất dột ngột
* Hệ thống hoạt dộng với bộ nhớ nhiều hơn bình thường
* Tên 1 ổ đĩa thay dổi hoặc không thể truy cập
* Các chương trình hoặc file đột ngột k truy cập đc nữa

1. Xác định nguồn lây nhiễm

• Khoanh vùng xử lý hay cách ly các máy có dấu hiệu nghi ngờ nhiễm mã độc.

• Ghi lại ngày giờ phát hiện mã độc hại và các thông tin liên quan.

• Để nguyên tình trạng của phần cứng, phần mềm liên quan đến hệ thống bị nhiễm.

Xác định hệ thống bị nhiễm mã độc hại :

• Thông tin về hệ điều hành đang sử dụng.

• Trình duyệt Web sử dụng.

• Tường lửa sử dụng.

• Các chương trình đang cài đặt trên máy tính.

• Các tiến trình đang chạy thông thường, chạy ngầm.

• Các chương trình bảo vệ máy hiện thời đã có.

Từ đó xác định được các modules, các tiến trình, các dịch vụ, các drivers, các add-on - plugin của trình duyệt, phiên bản hệ điều hành của hệ thống có liên quan đến hoạt động của mã độc. Mục đích để có thể xác định nguồn gốc lây lan và tìm ra nguyên nhân tại sao máy tính lại bị lây nhiễm ? Đồng thời thực hiện rà soát lại xem hệ thống có bị lỗi bảo mật nào không ?

1. **Thu thập mã độc và phân loại**
2. Thu thập

Để đảm bảo các máy tính này nguyên vẹn để điều tra rõ hơn sự cố sau này thì người phân tích thường sẽ sao lưu ổ cứng bị nhiễm ra một nơi và phân tích trên bản sao ổ cứng đó. Tiếp tục, quan sát và tìm kiếm các tệp thực thi lạ trên hệ thống, sau đó thực hiện phân tích, hoặc sử dụng một số công cụ giám sát hệ thống như xem xét các tiến trình, kiểm tra xem có tiến trình lạ không để xác định nguyên nhân tạo ra tiến trình lạ, xác định tiến trình đó được tạo từ ở đâu, thực hiện nén mẫu và mang đi phân tích.

1. Phân loại

Tự phân tích và xử lý mẫu mã độc hoặc gửi mẫu mã độc đó cho các hãng Anti-virus (ví dụ: Hãng Symatec, McAffee) để giúp các hãng có thể cập nhật được mẫu mới qua cổng thông tin (Website) hoặc gửi mẫu mã độc thông qua email.

1. **Phân tích thông tin sơ lược**

Bước 1: Phân tích đặc trưng kiểm tra đặc điểm tệp tin, giá trị băm, các chuỗi ký tự.

Bước 2: Phân tích file nén, bước này kiểm tra xem tệp tin có bị nén không ? Nếu có bị nén thì có thể sử dụng các công cụ giải nén sau đó quay trở lại bước 1, hoặc nếu không giải nén được thì sang bước 3.

Bước 3: Tương quan kết quả, tại đây thu nhận các kết quả, người phân tích lấy giá trị băm của tệp tin phân tích, gửi lên trang Virustotal để xem mẫu này đã được phân tích hay chưa ? Nếu có kết quả phân tích rồi lưu lại làm tài liệu để so sánh kết quả phân tích sau này.

1. **Phân tích động hành vi**

Xây dựng môi trường phân tích cách ly với hệ thống thật (để mô phỏng các dịch vụ Internet và xây dựng các môi trường phù hợp để mã độc có thể chạy được) Cho phép người phân tích quan sát xem một tệp mẫu nghi ngờ khi thực thi sẽ làm những gì?, chạy như thế nào ?, thực hiện những hành động gì trên máy tính, hoặc tương tác với các dịch vụ mạng thông qua các công cụ theo dõi.

1. **Phân tích mã thực thi**

Đọc mã thực thi của mã độc sử dụng một bộ phân tích (Disassembler) để dịch ngược các đoạn mã bên trong một chương trình mã độc thành dạng hợp ngữ, từ đó tìm hiểu các chỉ lệnh nhằm biết chính xác chương trình mã độc có thể làm những việc gì.

Những chỉ lệnh được thực thi bởi CPU, do vậy những chỉ lệnh này sẽ cho người phân tích biết chính xác những gì chương trình mã độc thực hiện. Tuy nhiên để có thể thực hiện được việc phân tích tĩnh, đòi hỏi người phân tích phải am hiểu sâu về hợp ngữ, về các mã chỉ dẫn lệnh và các khái niệm và các hàm API trong hệ điều hành.

1. **Viết cáo cáo**

Sau khi phân tích xong mẫu mã độc, người phân tích cần tổng hợp thành một báo cáo hành vi hoạt động của mã độc.

Dưới đây là một ví dụ về báo cáo tổng hợp lại kết quả sau khi phân tích một mẫu mã độc của hãng McAfee.

Báo cáo kết quả phân tích mẫu W32/Espace.worm

**Câu 3: Phương án xử lý**

**Áp dụng cho tất cả các phiên bản Windows.**

Người dùng thực hiện những bước như sau để xử lý mã độc

1. Tắt hệ thống System Restore
2. Cập nhật chương trình Mcafee kèm mẫu nhận dạng .dat 3.Quét toàn bộ hệ thống
3. Phục hồi hệ thống sau khi quét:
4. Vào chế độ Microsoft Recovery Console và khởi tạo lại MRB sạch

**- Trên Vào Windows Xp** đưa đĩa CD vào và khởi động lại máy tính. Khi màn hình hiện chữ Welcome to setup, nhấn R để vào màn hình Recovery Console. Lựa chọn Windows installation cung cấp mật khẩu Administrator, sau đó gõ lệnh fixmbr để lấy lại Master Boot Record. Sau đó lấy đĩa CD và khởi động lại máy.

**- Trên Windows Vista, Windows 7** đưa đĩa CD vào và khởi động lại máy tính. Nhấp chọn Repair your Computer. Khi của sổ hiển thị System Recovery Options, chọn phần Command Prompt. Sử dụng câu lệnh “bootec /fixmbr” để khởi tạo lại Master Boot Record. Sau đó khởi động và bỏ đĩa CD khỏi máy tính.

**/\* cái này t tự ghi ra tham khảo \*/**

**CÁCH PHÒNG TRÁNH MALWARE**

Trong thuật ngữ chuyên ngành, người ta sử dụng từ malware để chỉ các

loại phần mềm gây hại như virus, worm, trojan horse, spyware và adware. Dưới

đây là những cách phòng trừ malware hiệu quả.

 **Thói quen Online thông minh**

Nhân tố quan trọng nhất trong cuộc chiến phòng ngừa malware chính là

bạn. Bạn không cần phải là chuyên gia, mà chỉ cần không tải và cài đặt bất cứ

thứ gì bạn không hiểu hoặc không tin tưởng.

**+ Đối với website**

Một website yêu cầu bạn cài đặt một chương trình. Nếu không chắc chắn,

bạn hãy rời website và điều tra về phần mềm mà bạn đang được đề nghị cài đặt.

Nếu kết quả tốt, bạn có thể quay lại và cài đặt sau.

**+ Đối với email**

Đừng tin tưởng bất cứ thứ gì chứa đựng trong một email rác. Kể cả khi

nhận được email từ người bạn biết có kèm theo link hay file đính kèm, cũng nên

cảnh giác. Nếu nghi ngờ về cái bạn được đề nghị xem hay cài đặt, thì đừng làm

điều đó.

**+ Đối với thiết bị di động**

Bạn bè, gia đình và đồng nghiệp có thể vô tình đưa cho bạn đĩa hoặc USB

nhiễm virus. Đừng vội dùng những dữ liệu này, cần phải quét bằng các chương

trình diệt virus trước.

**+ Đối với cửa sổ pop-up**

Khi lướt web bạn có thể thấy nhiều cửa sổ bung ra yêu cầu bạn tải về

hoặc đồng ý dùng một chương trình quét hệ thống nào đó. Bạn cần tắt các cửa

sổ này đi và nhớ là không bấm vào bất kỳ nội dung gì bên trong nó. Có thể tắt

bằng Windows Task Manager (bấm Ctrl-Alt-Delete)

**+ Đối với một phần mềm**

Một số chương trình cố gắng cài malware trong quá trình cài đặt của

chúng. Vì vậy khi cài đặt bạn cần để ý tới các lựa chọn trước khi bấm Next, OK

hay I Agree. Nếu không chắc chắn thì tắt đi, kiểm tra độ tin tưởng của chương

trình và cài lại nếu mọi việc bình thường.

**+ Đối với các dịch vụ chia sẻ file trực tuyến**

Đây là một môi trường nguy hiểm và bạn phải biết rõ mình đang làm gì

khi quyết định dùng những dịch vụ này. Bởi có rất ít sự kiểm soát hiệu quả, nên

các hacker có thể dễ dàng tạo một malware có tên giống như một bộ phim,

album hay chương trình nổi tiếng để thu hút bạn tải về.

* + - **Loại bỏ malware**

Cần chấp nhận thực tế rằng dù bạn có phòng ngừa kỹ càng cỡ nào thì

cũng có ngày bạn sẽ bị nhiễm một trong các loại malware. Đấy là bởi malware

càng ngày càng tinh vi và có thể đột nhập vào máy bạn mà bạn không thể lường

hết được. Khi đó cần tiêu diệt chúng bằng cách dùng những chương trình phù

hợp:

**+ Một hệ điều hành thường xuyên cập nhật: Hãy sử dụng Windows Update.**

**+ Một trình duyệt đều nên cập nhật**

Bản mới nhất

**+ Trình diệt virus**

Cập nhật thường xuyên

**+ Trình diệt spyware**

Cập nhật thường xuyên.

**+ Firewall**

Nên dùng của bên thứ 3 hoặc dùng luôn của window

**+ Bộ lọc thư rác**

Nên bật chức năng lọc thư rác lên