Câu 1:

Theo thứ tự quan trọng nhất đến ít quan trọng nhất từ cao đến thấp, các biện pháp ngăn chặn Trojan được sắp xếp như sau:

1) Chạy phần mềm chống vi-rút, tường lửa và phát hiện xâm nhập dựa trên máy chủ giúp bảo vệ hệ thống của bạn khỏi Trojan.

2) Cài đặt các bản vá và bản cập nhật bảo mật cho hệ điều hành và ứng dụng bao gồm các bản sửa lỗi cho các lỗ hổng bảo mật mà Trojan có thể khai thác.

3) Hạn chế quyền trong môi trường máy tính để bàn để ngăn cài đặt ứng dụng độc hại.

4) Tránh mở tệp đính kèm email từ người gửi không xác định.

5) Tránh tải xuống và thực thi ứng dụng từ các nguồn không đáng tin cậy.

6) Củng cố các cài đặt cấu hình yếu, mặc định và tắt các chức năng không sử dụng.

7) Theo dõi lưu lượng mạng nội bộ để tìm các cổng hoặc lưu lượng truy cập hết hạn bất thường.

8) Trojan cũng có thể được gửi qua tin nhắn tức thời, tránh chấp nhận các chương trình được chuyển qua tin nhắn tức thời từ người gửi không xác định.

9) Trojan có thể được phân phối trên các đĩa CD và DVD, vì vậy ta nên quét các đĩa CD và DVD bằng phần mềm chống vi-rút trước khi sử dụng.

10) Tránh gõ các lệnh một cách mù quáng và triển khai các chương trình hoặc tập lệnh được làm sẵn.

11) Quản lý tính toàn vẹn của tệp máy trạm cục bộ thông qua kiểm tra tổng kiểm tra, kiểm tra và quét cổng thông qua các công cụ kiểm tra tính toàn vẹn của tệp để phát hiện các tệp bị nhiễm Trojan.

Câu 2: Tìm kiếm 3-5 loại Troạn mới xuất hiện trong thời gian gần đây. Lập bảng mô tả Troạn đó (Tên, nguồn gốc, đặc điểm, cổng xâm nhập, biện pháp phòng chống…).

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Tên | Nguồn gốc | Đặc điểm | Cổng xâm nhập | Biện pháp phòng chống |
| GoldDigger | Việt Nam | Ứng dụng độc hại này giả mạo một cổng thông tin chính phủ Việt Nam và một công ty năng lượng, lợi dụng dịch vụ Tiện ích Truy cập Android để trích xuất thông tin cá nhân, đánh cắp thông tin đăng nhập ứng dụng ngân hàng, chặn tin nhắn SMS và thực hiện các hành động của người dùng khác nhau. | Cổng mạng, email | - Luôn kiểm tra cập nhật trên thiết bị di động, tránh tải ứng dụng từ các nguồn bên ngoài Google Play Store và kiểm tra các quyền mà ứng dụng yêu cầu sau khi tải về. |
| Emotet/ Mealybug | Ukraine | Là một Trojan banking, thường được phân phối qua email mạo danh và có khả năng tự động lây lan trong mạng nội bộ. Emotet có thể đánh cắp thông tin ngân hàng và tài khoản đăng nhập. | Cổng mạng, email | - Giữ cho máy tính của bạn được cập nhật với các bản vá mới nhất cho Microsoft Windows.  - Không tải các tệp đính kèm đáng ngờ hoặc nhấp vào các liên kết có vẻ đáng ngờ.  - Sử dụng mật khẩu mạnh và sử dụng xác thực hai lớp. |
| Ryuk | Russian | Là một trong những ransomware đầu tiên có khả năng xác định và mã hóa các ổ đĩa và tài nguyên mạng, cũng như xóa bản sao đổ bóng trên điểm cuối. Các kẻ tấn công có thể vô hiệu hóa Windows System Restore cho người dùng, làm cho việc khôi phục sau một cuộc tấn công trở nên không thể nếu không có sao lưu ngoài hoặc công nghệ rollback. | Cổng mạng, email, lỗ hổng bảo mật | -Sử dụng phần mềm antivirus để bảo vệ bản thân  -Sao lưu dữ liệu của bạn một cách thường xuyên  -Cập nhật hệ thống thường xuyên |
| MMRat | Đông Nam Á | Là một Trojan banking, phần mềm độc hại có thể đọc dữ liệu nhập vào và nội dung màn hình, đồng thời có thể điều khiển từ xa các thiết bị của nạn nhân thông qua nhiều kỹ thuật khác nhau, cho phép kẻ tấn công thực hiện hành vi lừa đảo ngân hàng trên thiết bị của nạn nhân | Cổng mạng, email | - Luôn kiểm tra cập nhật trên thiết bị di động, tránh tải ứng dụng từ các nguồn bên ngoài Google Play Store và kiểm tra các quyền mà ứng dụng yêu cầu sau khi tải về. |
| Sharkbot | Không biết | Là một Trojan banking, nhắm đến việc đánh cắp các thông tin đăng nhập ngân hàng của người dùng tải xuống ứng dụng. Lần mới nhất mà Sharkbot quay trờ lại, nó đã núp bóng vào các ứng dụng dọn rác | Cổng mạng, email | - Luôn kiểm tra cập nhật trên thiết bị di động, tránh tải ứng dụng từ các nguồn bên ngoài Google Play Store và kiểm tra các quyền mà ứng dụng yêu cầu sau khi tải về. |

* GoldDigger(Source: <https://www.group-ib.com/media-center/press-releases/golddigger-trojan-vietnam/>)
* Emotet/ Mealybug (Source: <https://www.malwarebytes.com/emotet>, <https://en.wikipedia.org/wiki/Emotet>)
* Ryuk (Source: <https://www.malwarebytes.com/ryuk-ransomware>)
* MMRat( Source: <https://tinnhiemmang.vn/phat-hien-trojan-android-moi-mmrat-co-kha-nang-thuc-hien-gian-lan-tai-chinh-tren-thiet-bi-bi-nhiem>)