Hồ sơ điều tra

Mã điều tra: B1.10-26.05

Ngày 26.05.2020

Mô tả:

Như thường lệ vào buổi sáng, cô Mai nhấm nháp tách cà phê của mình trong khi vội lướt qua những email được gửi đến hộp thư điện tử của mình vào tối qua. Một trong những lá thư được cô chú ý, cho dù nó khá giống như một thư rác nhưng mà một cách nào đó đã qua mặt được bộ lọc thư điện tử. Thông điệp của bức thư dường như gợi mở người đọc về những ưu điểm khi mua dược phẩm qua hình thức trực tuyến trên web, kèm một đường dẫn đến trang web bán dược phẩm trên mạng. "Người ta có thật sự yêu thích phong cách này không?" – Cô Mai nghĩ như vậy. Sau đó, cô rất tò mò muốn biết bằng cách nào mà trang web này thuyết phục được những khách vào trang web để mua hàng, nên cô nhấn vào liên kết trong email.

Trang web tải rất chậm, dường như là bị hỏng bởi lí do là không có nội dung gì trên trang web. Thất vọng, cô Mai đóng cửa sổ trình duyệt và tiếp tục uống hết ly cà phê buổi sáng và tới công ty.

Cô không nhận ra rằng máy tính hệ điều hành Windows XP của mình đã bị nhiễm mã độc nào đó.

Bây giờ, bạn đóng vai trò là một nhân viên điều tra Khang. Đồng thời, Khang được cung cấp tập tin chụp lại các gói tin mạng (tập tin pcap) khi cô Mai tương tác với trang web nói trên. Nhiệm vụ của Khang là tìm hiểu xem chuyện gì đã xảy ra đối với máy tính của cô Mai sau khi cô nhấp vào đường dẫn nhà thuốc trực tuyến trong email đã đề cập. Công việc phân tích này sẽ được tiến hành trên file PCAP và cố gắng tìm xem có một tập tin phần mềm độc hại nào đó hay không.

Câu hỏi:

1. Trong quá trình lây nhiễm, trình duyệt web của cô Mai đã tải về các tập tin Java applet. Xác định số tập tin này. Tìm tên các tập tin .jar tương ứng trong các tập tin Java Applet.
2. Tên người dùng trên máy tính bị nhiễm của cô Mai là gì?
3. Liên kết nào đã được cô Mai nhấp vào để vụ lây nhiễm được kích hoạt?
4. Như là một phần của sự cố lây nhiễm, một tập tin độc hại được tải về trên máy tính của cô Mai. Xác định mã băm MD5 của tập tin.
5. Xác định tên gọi của Packer (bộ đóng gói) để che giấu bảo vệ tập tin độc hại. Biết rằng Packer là một kỹ thuật sử dụng trong việc phát triển các mã độc, virus máy tính.
6. Xác định mã băm MD5 của phiên bản không bị đóng gói (Unpack) của tập tin thực thi độc hại trên Windows.
7. Mã thực thi độc hại này cố gắng kết nối tới một địa chỉ IP bên ngoài Internet. Xác định địa chỉ IP này.