Câu hỏi:

- ***Nhóm 3:***

1. Làm thế nào để phân biệt mã độc mới với các loại mã độc truyền thống?
2. Phương pháp tấn công phổ biến mà các hacker sử dụng để triển khai mã độc là gì?

- ***Nhóm 4:***

3. Trong những mã độc nhóm đã trình bày (CoinMinner, NanoCore, ViperSoftX, Agent Tesla, Ratejay, Gh0st, Dark Vision, Amadey, Lalap), các bạn có thể cho tôi biết mã độc nào là nguy hiểm và phổ biến nhất không? Và tệp người dùng nào sẽ thường bị dính mã độc đó? Tại sao?
4. Nếu trong trường hợp tôi bị dính mã độc nguy hiểm mà bạn trả lời ở câu 3, thì bước "sơ cứu" ban đầu tôi nên xử lý là gì để có thể giảm thiểu tối đa thiệt hại?

Trả lời:

1. Phân biệt mã độc mới với mã độc truyền thống thường dựa vào phân tích hành vi, cấu trúc và chữ ký số, cũng như sử dụng các công cụ phát hiện dựa trên machine learning để nhận diện các hành vi độc hại không rõ ràng.

2. Phương pháp tấn công phổ biến để triển khai mã độc bao gồm phishing (email spam), lỗ hổng bảo mật không được vá (exploits), và các kỹ thuật tấn công "drive-by download" qua các trang web bị nhiễm (chiếm bởi hacker).

3. Agent Tesla là một trong những mối đe dọa phổ biến và nguy hiểm hiện nay. Agent Tesla là một loại malware phức tạp với chức năng là một Advanced Persistent Threat (APT) có khả năng thu thập thông tin và thực hiện các hành động trên máy nạn nhân từ xa.

Tệp người dùng thường bị nhiễm Agent Tesla bao gồm cá nhân và tổ chức không có biện pháp bảo mật mạnh mẽ hoặc không thực hiện các cập nhật bảo mật định kỳ, đặc biệt là những người sử dụng email và mở các đính kèm hoặc liên kết đáng ngờ. Người dùng cũng có thể nhiễm mã độc này thông qua việc tải phần mềm từ nguồn không đáng tin cậy.

Agent Tesla thường được phát tán qua chiến dịch phishing, sử dụng các email mạo danh chứa các đính kèm độc hại hoặc liên kết đến các trang web nhiễm malware. Khi người dùng vô tình mở đính kèm hoặc nhấp vào liên kết, Agent Tesla sẽ được cài đặt và bắt đầu hoạt động. Phần mềm gián điệp này có thể ghi lại các phím gõ, chụp ảnh màn hình, đánh cắp thông tin đăng nhập và thông tin khác, gây ra rủi ro lớn với dữ liệu cá nhân và doanh nghiệp.

4. Nếu nghi ngờ bị nhiễm mã độc nguy hiểm như Agent Tesla, các bước bạn nên làm bao gồm:

- Ngắt kết nối từ internet để ngăn chặn việc dữ liệu bị chuyển đi.
- Không đăng nhập vào bất kỳ tài khoản nào hoặc thực hiện các giao dịch tài chính.
- Chạy phần mềm chống mã độc uy tín để quét và loại bỏ mối đe dọa.
- Thay đổi mật khẩu từ một máy tính khác không bị nhiễm.
- Thông báo cho các tổ chức tài chính nếu cần thiết.
- Tìm kiếm sự giúp đỡ từ chuyên gia bảo mật.