|Cảnh báo virus máy tính Eurograbber|

Eurograbber là tập hợp các biến thể của Zeus bao gồm SpyEye, CarBerp và ZitMo. Virus này phá vỡ phương thức bảo mật xác thực 2 yếu tố là một trong những phương pháp đang được các ngân hàng sử dụng rộng rãi hiện nay vì có độ tin cậy cao.

Phương thức sử dụng Eurograbber để lấy cắp tiền của Ngân hàng diễn như sau:

(1). Các tin tặc sử dụng thủ đoạn lừa nạn nhân truy cập vào một liên kết độc hại có virus Eurograbber, virus xâm nhập vào máy tính nạn nhân, hiển thị giả mạo thông báo Ngân hàng để **lừa nạn nhân cung cấp số điện thoạ**i.

(2) Sau khi có số điện thoại của nạn nhân, tin tặc tiếp tục gỉa mạo các thông điệp của Ngân hàng để yêu cầu cài đặt phần mềm quản lý tài khoản. Thực chất đây là phần mềm độc hại giả mạo, dùng để lấy trộm tin nhắn xác thực từ Ngân hàng.

(3) Với việc lấy được các thông tin đăng nhập, số tài khoản và mật mã, tin tặc có thể thực hiện các giao dịch rút tiền tại Ngân hàng mà chủ tài khoản này không hề hay biết

Mặc dù chưa có ghi nhận về việc virus này xuất hiện tại Việt Nam, song để đề phòng nguy cơ lây nhiễm virus Eurograbber nói riêng và đảm bảo an toàn các giao dịch trực tuyến nói chung, Ngân hàng đề nghị Quý khách lưu ý những điểm sau:

- Kiểm tra rằng phần mềm chống virus của Quý khách đã được cập nhật.
- Đảm bảo rằng các tin nhắn SMS phản ánh yêu cầu giao dịch ngân hàng trực tuyến của bạn. Ví dụ, nếu bạn nhận được một tin nhắn yêu cầu bổ sung người thụ hưởng hoặc chuyển tiền cho một số tài khoản mà bạn không biết thì bạn KHÔNG ĐƯỢC nhập thông tin vào Ngân hàng trực tuyến và phải thông báo cho Ngân hàng ngay lập tức.
- Tin nhắn SMS được gửi từ Ngân hàng luôn luôn là: +8069; 1900545406; Stanchart.
- Kiểm tra nội dung SMS cẩn thận, nếu Quý khách cảm thấy nghi ngờ, vui lòng liên hệ Ngân hàng ngay lập tức.
- Để bảo mật, không bấm vào các liên kết từ các email, cài đặt bất kỳ những chương trình nào không rõ nguồn gốc hoặc thực hiện các giao dịch trực tuyến trên máy tính mà bạn nghi ngờ đang bị xâm hại.
- Luôn truy cập dịch vụ Ngân hàng trực tuyến của chúng tôi bằng cách gõ địa chỉ tham chiếu chính xác http://www.standardchartered.com.vn
- Đọc các mẹo bảo mật khác trên website của Ngân hàng

Lưu ý Quan trọng

Ngân hàng **không bao giờ yêu cầu** khách hàng cung cấp **số điện thoại** của Quí khách qua các kênh như: ngân hàng trực tuyến, điện thoại, email, SMS. Và Ngân hàng **không bao giờ yêu cầu** khách hàng cung cấp **mật khẩu** của Quí khách qua các kênh như điện thoại, email, SMS. Nếu Quý khách nghi ngờ rằng máy tính của Quý khách hoặc tài khoản ngân hàng của Quý khách đã bị xâm nhập trong khi giao dịch ngân hàng trực tuyến với chúng tôi, xin vui lòng liên hệ với chúng tôi ngay lập tức.

Thông tin liên hệ của Ngân hàng: 84-8-3911 0000 hoặc 84-4-3696 0000.

Địa chỉ:

- Lầu 1, TTTM Sài Gòn, 37 Tôn Đức Thắng, Quận 1, Tp HCM
- Tầng trệt – Tòa nhà CDC, 25 Lê Đại Hành, Quận Hai Bà Trưng, Hà Nội
- Tầng trệt- Tòa Tháp Hà Nội, 49 Hai Bà Trưng, Quận Hoàn Kiếm, Hà Nội