CẢNH GIÁC VỚI CÔNG CỤ TẠO TROJAN PHIÊN BẢN MỚI

Shark

Shark 2 là tên phiên bản mới của công cụ tạo "ngựa thành Troy" khá nguy hiểm mà hãng bảo mật PandaLabs vừa cảnh báo đến người dùng sau khi phân tích hàng loạt diễn đàn hacker trên Internet.

Shark 2 được phát triển và cập nhật liên tục, trên mỗi diễn đàn đều có những phiên bản khác nhau như 2.1, 2.2 hay 2.3.2. Điều nguy hiểm nhất mà Shark 2 có thể làm là hỗ trợ các script kiddies tạo ra những mã độc mà không cần am tường về kỹ thuật lập trình. Giao diện của Shark 2 cũng đơn giản, script kiddies chỉ cần chọn lựa loại mã độc hay trojan với chức năng tương ứng để xuất ra và sử dụng.

Các tùy chọn chức năng của Shark 2 khi tạo trojan cũng khá đa dạng. Loại trojan được tạo sẽ mở cửa hậu để dẫn lối cho các cuộc tấn công kế tiếp, cấu hình mã độc để tự động chạy mỗi khi hệ thống của nạn nhân khởi động, hiển thị các thông báo lỗi, thực thi các tập tin tùy ý, làm ngưng trệ các dịch vụ, tác vụ của hệ thống.

Tất nhiên là ngoài những tùy chọn kể trên thì không thể thiếu các khả năng mà hầu như trojan nào cũng có là: chụp màn hình hoạt động, âm thanh, thao tác phím gõ. Điều hướng nạn nhân truy cập vào các website giả mạo (phishing) hoặc tải về thêm các trojan khác, đánh cắp thông tin tài khoản ngân hàng, email..

Theo các chuyên gia phân tích bảo mật của PandaLabs, sở dĩ Shark 2 nguy hiểm là vì những "đứa con" của nó có thể được cấu hình để làm ngưng hoạt động chính bản thân chúng - khi phát hiện có công cụ sửa lỗi. Do đó, sẽ rất khó khăn khi cho việc dò tìm chúng trên hệ thống.

Người dùng Internet ngày càng trở thành miếng mồi ngon cho những hacker hoặc thậm chí là các script kiddies sử dụng những công cụ tạo trojan. Sau Pinch lại đến Shark 2, chắc chắn sẽ có những phiên bản kế tiếp hoặc những công cụ mới tạo ra các trojan nguy hiểm hơn. Chương trình chống virus liệu có đủ để đương đầu với các hiểm họa này? Tốt nhất cho một hệ thống vẫn là: chương trình chống virus, rootkit, tường lửa và sử dụng internet với mức độ cảnh giác cao.

Thanh Trực