MALWARE "CẮN NGƯỢC" WEBSITE BẢO MẬT

Giới h

Giới hacker, tác giả malware và phisher đang dành khá nhiều thời gian và sức lực để tìm cách hạ gục các website bảo mật. Vì sao?

Ý đồ của chúng là: Nếu có thể hạ gục những website bảo mật trong vòng vài tuần, malware sẽ có thể cài đặt "vô tư" và dễ dàng vào trong một số lượng lớn máy tính, bởi người dùng không còn được ai cảnh báo, chỉ dẫn cách phát hiện cũng như xóa bỏ malware nữa.

Thêm vào đó, nếu như chúng có thể khiến cho các website bảo mật bị "out" khỏi mạng đủ lâu, ISP sẽ buộc phải đóng cửa những website này theo đúng quy định.

Theo phát hiện của PC World thì trong 2 tuần trở lại đây, trang web CastleCops.com, một địa chỉ chuyên trợ giúp những người dùng máy tính bị dính malware, đã phải hứng chịu một trận tấn công từ chối dịch vụ khá nặng.

Người đứng đầu CastleCops, chuyên gia Paul Laudanski cho biết website đã bị ngắt mạng tới vài tiếng trước khi các kỹ sư của hãng tìm ra cách khắc phục.

Đồng loạt bị bắn hạ

Nguồn: SecurityLabs

Vấn đề là CastleCops không phải mục tiêu duy nhất. "Nhiều website hữu ích khác cũng đang bị tấn công, bao gồm 419eater.com, fraudwatchers.org, Scam.com, scamfraudalert.com và scamwarners.com.

"Khi tôi kiểm tra, hầu hết những site này đều không thể truy cập được. Ý đồ của những kẻ tấn công đã quá rõ ràng", ông Laudanski bình luận.

Tệ hơn nữa, CastleCops đang buộc phải cho aa491.org mượn tạm "nhà" để trú chân, sau khi ISP của aa491 phát hoảng với tất cả các vụ tấn công DDoS nhằm vào site này.

Những site như CastleCops và scam.com đều do các tình nguyện viên lập ra, hầu hết chỉ có lòng nhiệt tình nhưng trình độ về bảo mật chỉ dừng lại ở mức amateur. Trong khi ấy, kẻ tấn công họ lại là các băng nhóm tội phạm có tổ chức và đang nóng lòng kiếm tiền.

Người ta cho rằng những website bảo mật nghiệp dư đang làm ảnh hưởng đến công việc kinh doanh bẩn thỉu của bọn tội phạm mạng, và mọi biện pháp cảnh cáo, dọa dẫm với họ đều vô dụng. Chính vì thế, lựa chọn tội nhất cho kẻ xấu là "bắt website câm miệng".

Điểm sáng duy nhất trong xu hướng này, theo ông Laudanski, là nó gián tiếp khẳng định vai trò của các website bảo mật nghiệp dư. "Nếu không có tác dụng thật thì bọn chúng tấn công chúng tôi làm gì?".

Trọng Cầm