

HACKER TRUNG QUỐC "PHẤT" LÊN NHỜ MALWARE

Các ch

Các chuyên gia bảo mật vừa ghi nhận một sự gia tăng đột biến về số lượng các phần mềm phá hoại có gốc gác từ Trung Quốc. Nguyên do chỉ có một: nhiều hacker tại nước này đã "ngủi thấy mùi tiền" và cơ hội làm giàu từ malware.

"Mới 3 - 4 tháng trước, số lượng malware xuất xứ từ Trung Quốc tăng không đáng kể. Nhưng giờ thì con số thay đổi từng ngày", ông Chris Boyd, giám đốc nghiên cứu malware của hãng bảo mật Facetime Communications cho biết.

Trước đây, khu vực Đông Nam Á thường là điểm nóng của nạn đánh cắp mật khẩu, nhất là với những game online ăn khách như World of Warcraft. Bọn tội phạm thường theo đuổi tiền tệ và tài sản ảo, để rồi sau đó bán lại trên những website đấu giá.

Tuy nhiên, điều mà ông Boyd muốn nhấn mạnh chính là tín hiệu dự báo cho một xu hướng lớn hơn: Hacker Trung Quốc đang tự phát triển các rootkit và malware của riêng mình. Nếu như trước đây, chúng chỉ mạnh về sao chép và cải biên malware, thì giờ đây, các sản phẩm "cây nhà lá vườn" ồ ạt ra đời.

Cũng như tất cả các nơi khác trên thế giới, tiền chính là động cơ lớn nhất đứng đằng sau xu hướng này. "Chúng bắt đầu nhận ra mình có thể kiếm bộn tiền từ việc cài đặt malware".

Nguồn: AP

Roger Thompson, giám đốc công nghệ của Exploit Prevention Labs cũng chia sẻ quan điểm này với Boyd. Thompson cho biết hoạt động phát tán malware từ Trung Quốc gia tăng đột biến kể từ tháng 1 năm ngoái - thời điểm mà người ta tin là chính một nhóm hacker Trung Quốc đã tấn công

website của Superbowl.

Ngoài ra, hầu hết những lỗ hổng Zero-day trong Word và Excel thời gian gần đây đều có mối liên hệ với hacker Trung Quốc. "Tôi luôn nghĩ rằng bộ mặt của hacker thế hệ mới sẽ là người Trung Quốc. Thứ nhất là vì số lượng đông đảo, và thứ hai là ở sức mạnh công nghệ", Thompson dự đoán.

Boyd cho biết những malware Trung Quốc trong vài tháng trở lại đây có mức độ tinh vi "đáng lo ngại". Đầu tháng này, ông phát hiện được một Trojan có tên Symfly. Không chỉ download nhiều ứng dụng adware về máy, Trojan này còn cài đặt tự động thanh công cụ Alexa.

Alexa là một ứng dụng hợp pháp của Amazon nhằm đo lường mức độ phổ biến của một website. Và Symfly lợi dụng chính công cụ này để dụ người dùng truy cập một loạt website nhằm tăng thứ hạng cho những website đó.

Trọng Cẩm