DỰ BÁO MỘT HÌNH THỨC TẤN CÔNG PHISHING THẾ HỆ MỚI

Các nh

Các nhà nghiên cứu của Goolge và Viện công nghệ Georgia (Mỹ) đang nghiên cứu một phương pháp tấn công ảo không thể phát hiện được, theo đó có thể "lặng lẽ" kiểm soát nạn nhân cho dù họ ở bất cứ đâu trên Internet.

Nghiên cứu trên dự kiến sẽ được công bố vào tháng 2 năm tới, với những phân tích chi tiết về máy chủ DNS "đệ quy mở" - được sử dụng để chỉ định cách thức máy tính tìm kiếm lẫn nhau trên Internet bằng cách dịch tên miền, chẳng hạn như Google.com, thành địa chỉ IP dạng số. Giới tội phạm đang liên kết những dạng máy chủ này với các kỹ thuật tấn công mới nhằm phát triển một thể thức phishing thế hệ mới.

Các nhà nghiên cứu ước tính rằng hiện đang có khoảng 17 triệu máy chủ DNS đệ quy mở trên Internet, phần lớn là đưa ra thông tin chính xác. Tuy nhiên, không giống máy chủ DNS, các hệ thống đệ quy mở sẽ đáp lại tất cả những truy vấn tìm kiếm DNS từ bất cứ máy tính nào trên Internet, một tính năng cực kỳ hữu ích cho tin tặc.

Viện Công nghệ Georgia và Google cũng ước tính rằng có khoảng 0,4% (khoảng 68.000) máy chủ DNS đệ quy mở đang bị lợi dụng và đáp trả sai các truy vấn DNS. Khoảng 2% trong số các máy chủ này đưa ra câu trả lời khó hiểu. Đây thực sự là một mối đe doạ bởi DNS từng được coi là nền tảng và sự tin cậy của Internet.

"Đây là một hình thức tội phạm bởi những máy chủ dạng này có thể hướng dẫn người dùng truy cập vào những website nguy hiểm hoặc một máy chủ Web chuyên spam", phát biểu của David Dagon, nhà nghiên cứu thuộc Viện công nghệ Georgia.

Việc tấn công vào hệ thống DNS không phải là mới, và các nhóm tội phạm mạng đã và đang thay đổi cấu hình DNS trên máy tính nạn nhân từ nhiều năm nay. Tuy nhiên, chỉ một phần nhỏ hacker "mũ đen" lợi dụng và nhân rộng phương pháp tấn công này. Thay vào đó chúng sử dụng virus để tiến hành thay đổi cấu hình DNS, rồi sau đó chỉ việc sử dụng các phần mềm độc hại (malware) điều khiển.

Google đã đưa ra ngữ cảnh của cuộc tấn công như sau:

Nạn nhân ghé thăm một trang web hoặc mở một file đính kèm độc hại có thể khai thác lỗ hổng

phần mềm máy tính. Những kẻ tấn công sau đó sẽ chỉ cần thay đổi một file trong Registry để điều khiển PC kết nối tới máy chủ hacker đối với tất cả thông tin DNS. Nếu mã khai thác ban đầu không bị chương trình diệt virus chặn lại thì cuộc tấn công sẽ cho phép tin tặc điều khiển máy tính theo cách không thể phát hiện được.

Khi đã thay đổi cấu hình Windows, bọn tội phạm có thể chiếm quyền điều khiển máy tính và chuyển tiếp tới site độc hại bất cứ khi nào chúng muốn. Do phương thức tấn công này chỉ diễn ra ở cấp độ DNS nên những phần mềm chống phishing không thể phát hiện được site phishing mà người dùng truy cập vào.

Theo Chris Rouland, giám đốc kỹ thuật bộ phận hệ thống bảo mật Internet của IBM cho rằng những kiểu tấn công DNS như trên sẽ nhằm vào các site Web 2.0 trong vài tháng tới, bởi những trang kiểu này thường cho phép người dùng kết nối với nhiều trang web mà trong số chúng có thể không đáng tin cậy và an toàn.

Văn Hân