ROCK PHISH - NGUỒN GỐC HIỂM HOẠ CỦA INTERNET

Lừa đả

Lừa đảo trực tuyến (phishing) giờ đã trở thành một khái niệm khá quen thuộc trong cộng đồng người dùng Internet. Nhưng có lẽ khái niệm Rock Phish thì chưa được phổ biến như vậy.

Tuy nhiên, các chuyên gia bảo mật khẳng định Rock Phish mới thực sự là mối lo ngại còn hơn cả các vụ tấn công phishing. Bởi nó chính là gốc rễ của phần lớn các vụ tấn công phishing, cũng như là tác giả của hãng loạt các thủ đoạn lừa đảo tinh vi.

Rock Phish là...

Điều đầu tiên mà bạn cần biết về Rock Phish là "hiện chưa có một ai biết chính xác nó là cái gì, hay ai đứng đằng sau tổ chức và vận hành nó".

Wikipedia định nghĩa Rock Phish Kit như sau: "Một công cụ khá phổ biến được thiết kế với mục tiêu giúp cho cả những người không phải dân kỹ thuật cũng có thể thực hiện các vụ tấn công phishing".

Các chuyên gia bảo mật lại cho rằng định nghĩa đó là hoàn toàn sai. Họ cho rằng Rock Phish là một cá nhân hoặc một nhóm người có tổ chức phải chịu trách nhiệm cho hơn một nửa số lượng các vụ tấn công phishing đã và đang diễn ra trên toàn cầu.

Thủ đoạn chủ yếu của bọn lừa đảo trực tuyến (phisher) là lừa nạn nhân cung cấp cho chúng các thông tin cá nhân nhạy cảm bằng cách sử dụng những trang web giả mạo giống hệt trang web của một ngân hàng hoặc một cửa hàng trực tuyến. Đây là một hình thức tấn công rất hấp dẫn đối với bọn tội phạm mạng, bởi nguồn lợi nhuận mà nó mang về là rất lớn.

Hãng nghiên cứu Gartner ước tính trong năm qua, thiệt hại mà lừa đảo trực tuyến đã gây ra cho người tiêu dùng và doanh nghiệp Mỹ đã lên tới con số 2,8 tỉ USD. Tính trung bình mỗi nạn nhân phải chịu mức thiệt hại tương đương 1.244 USD.

Nhưng cho đến nay, vẫn chưa có một ai biết Rock Phish là gì, nó tồn tại ở đâu và liệu nó chỉ hoạt động trên một quốc gia hay liên quốc gia.

"Chúng là những Keyser Söze của thế giới phishing," Zulfikar Ramzan - chuyên gia nghiên cứu

cao cấp của Symantec Security Response - nhận định. (Keyser Söze là một nhân vật trụ cột của thế giới tội phạm ngầm trong bộ phim The Usual Suspects phát hành năm 1995).

"Bọn chúng đang tiến hành những hành động làm kinh hoàng cho người dùng Internet trên toàn cầu".

Lịch sử của Rock Phish

Cái tên Rock Phish xuất hiện vào cuối năm 2004. Lúc đó cái tên này được đặt cho một nhóm tội phạm có tổ chức cực kỳ nguy hiểm.

Sở dĩ chúng được đặt cái tên đó là bởi vì để qua mặt các công cụ lọc phishing, nhóm tội phạm này thường tạo ra một thư mục có tên "rock" lưu trữ trực tiếp cùng với các website giả mạo của chúng.

Kể từ đó, nhóm tội phạm này đã phát triển ngày càng mạnh mẽ và trở thành một trong những băng nhóm tội phạm lừa đảo trực tuyến "thành công nhất" trên thế giới. Chúng liên tục "phát minh" ra nhiều kỹ thuật tấn công mới khiến các chuyên gia bảo mật chuyên nghiệp cũng phải "ngưỡng mộ" tài năng của chúng.

Ước tính đến nay các thủ đoạn tấn công phishing của nhóm tội phạm này đã mang về cho chúng một nguồn lợi nhuận lên tới 100 triệu USD.

Phương thức hoạt động

Rock Phish không phải nổi tiếng vì việc chuyên tấn công vào hai mục tiêu được ưa chuộng nhất là eBay và PayPal, mà thay vào đó chúng chuyên tấn công vào các tổ chức tài chính của Mỹ và Châu Âu.

Con số thống kê mới nhất cho thấy Rock Phish đã giả mạo 44 thương hiệu của các doanh nghiệp tại 9 quốc gia khác nhau và gửi đi vô số email mạo danh, nhằm lừa nạn nhân truy cập vào một trong những website giả mạo và cung cấp cho chúng những thông tin bí mật như số thẻ tín dụng, tài khoản ngân hàng trực tuyến ... Rock Phish chưa từng "tha" cho "một con mồi" nào, từ Barclays, Citibank, Deutsche Bank, E-Trade đến hàng trăm doanh nghiệp thanh toán trực tuyến khác.

Các chuyên gia bảo mật ước tính Roch Phish có dính dáng đến gần 1/2 số lượng email lừa đảo được gửi đi trên mạng Internet. "Chúng là nhóm tội phạm lừa đảo trực tuyến "năng động" nhất trên thế giới," Dan Hubbard - Giám đốc nghiên cứu công nghệ và bảo mật của Websense - nhận định.

Điều khiến các chuyên gia bảo mật như Dan Hubbard phải lo ngại nhất về Rock Phish là nhóm tội phạm này luôn đi trước một bước so với các sản phẩm bảo mật và luật pháp.

Lấy ví dụ, các chuyên gia bảo mật cho biết Rock Phish chính là kẻ đi đầu trong việc gửi spam bằng hình ảnh nhằm qua mặt các công cụ lọc thư rác. Rồi trong khi các hãng phần mềm tích hợp công

cụ lọc phishing vào trong trình duyệt thì nhóm tội phạm này đã "sáng tạo" ra những kiểu đường dẫn URL đặc biệt giúp chúng không bị "điểm danh" trong "danh sách đen" các URL phishing.

Chuyên gia Ramzan của Symantec lắc đầu ngao ngán cho biết kiểu địa chỉ website "dùng một lần" như kiểu của Rock Phish khiến chúng thật sự rất khó bị phát hiện. Nhiều khi các chuyên gia bảo mật cũng phải bó tay trong việc ngăn chặn những trang web kiểu này.

Với kiểu sử dụng cơ sở dữ liệu danh sách các địa chỉ phishing như trình duyệt Firefox thì việc bị Rock Phish qua mặt là chuyện như cơm bữa. "Nói rộng hơn là những công nghệ chống phishing dựa trên danh sách đen là hoàn toàn vô dụng," Ramzan nhấn mạnh.

Anti-Phishing Working Group cho biết trong thời gian gần đây Rock Phish vẫn tiếp tục góp phần làm gia tăng mạnh mẽ số lượng các trang web phishing trên toàn cầu. Tháng 8, nhóm tội phạm này đã phát tán hơn 19.000 địa chỉ website phishing. Con số này lại tăng gấp đôi trong tháng 10 vừa qua với hơn 35.000 địa chỉ.

Các chuyên gia bảo mật cho rằng Rock Phish được điều hành bởi một nhóm nhỏ những tên tội phạm mạng có trình độ kỹ thuật cao. Ước tính số lượng của chúng chỉ vào khoảng một chục người. Nhưng đây mới chính là những kẻ đầu não bởi trách nhiệm của chúng là tạo ra các trang web phishing, quản lý tên miền và bảo đảm các thông tin tài chính ăn cắp được đều được gửi về một máy chủ trung tâm. Các chuyên gia bảo mật gọi cái máy chủ đó là "Mother Ship" (tàu mẹ).

Những thông tin mà chúng ăn cắp được sau đó sẽ được rao bán trên các chatroom. Đối tượng tiêu thụ "hàng" của bọn chúng chủ yếu là những kẻ rửa tiền giúp biến những đồng tiền ăn cắp thành tiền sạch.

"Minh tinh" của thế giới phishing

Rock Phish sử dụng một hệ thống mạng các PC bị "bắt cóc" để chuyển hướng khách truy cập đến trang của chúng về "Mother Ship".

Một yếu tố đặc biệt nguy hiểm khác trong phương thức hoạt động của Rock Phish là nhóm tội phạm này đã áp dụng phương thức hoạt động phi tập trung hoá trong các hoạt động phạm pháp.

Thủ đoạn được xem là thành công nhất của bọn chúng là Rock Phish thường xuyên sử dụng tên miền của các quốc gia ít được biết đến như tên miền ".md" của Moldovia bởi những quốc gia như thế này hầu như chưa có luật chống lại phishing. Chính lỗ hổng này đã tạo điều kiện cho sự phát triển mạnh mẽ của Rock Phish.

"Rock Phish là những nhà hoạt động vì đổi mới trong thế giới phishing," chuyên gia Ramzan của Symantec thừa nhận. "Bất cứ khi nào chúng ta thấy xuất hiện một kỹ thuật tấn công phishing mới thì chắc chắn đó là tác phẩm của Rock Phish".

Trang Dung