CẶP ĐÔI TROJAN LÀM TỶ LỆ PHÁT TÁN SPAM GIA TĂNG

Tổng lượng e-mail spam phát tán trong ba quý đầu năm tăng mạnh. Nguyên nhân là do hai Trojan download nguy hiểm, sử dụng hình thức tấn công máy PC rồi dùng chúng để phát tán lượng e-mail khổng lồ.

Hôm thứ sáu tuần qua, hãng nghiên cứu MessageLabs đưa ra thông báo rằng có một cặp Trojan nguy hiểm khiến tỷ lệ phát tán spam gia tăng. Chúng sử dụng kỹ thuật tinh vi hiện nay các hãng bảo mật chưa thể bắt kịp.

Theo một hãng cung cấp bảo mật ở Anh thì tỷ lệ gia tăng của spam tăng đột biến lên tới 72,9% trong tháng 10 so với 64,4% của tháng trước đó. Nguyên nhân chủ yếu là do hai Trojan nguy hiểm đã tấn công các máy PC và dùng chúng để phát tán lượng mail khổng lồ.

"Warezov Trojan là Trojan nguy hiểm nhất chúng tôi thấy trong thời gian gần đây. Mỗi lần thực hiện tấn công, nó download chương trình hoạt động hay thành phần tiếp theo, thay đổi một vài byte mã nguồn và đưa ra thành một bản mới. Điều này khiến hệ thống chống virus rất khó dò tìm và xác định", Paul Wood - chuyên gia phân tích ở MessageLabs nói.

Mặc dù không tìm ra chứng cớ thuyết phục cuối cùng, nhưng các nhà nghiên cứu của MessageLabs cho rằng bằng cách tự động thay đổi mã nguồn riêng, Warezov (với nhân "Stration") đã mở rộng cửa sổ tấn công. "Nếu các công ty anti-virus phải mất từ 5 đến 6 giờ để tạo ra một ký hiệu thì Trojan mở rộng hơn nhiều với những bản thể mới".

Một "con sâu làm rầu nồi canh" khác trong tháng mười là SpamThru, mã nguồn độc hại gây hậu quả nặng nề cho các máy tính. SpamThru còn có tên gọi khác do các công ty bảo mật đặt ra là "spam cannon" (khẩu đại bác spam). Nó dùng các mẫu mail kiểu hợp nhất khác nhau để phát tán thư rác ra ngoài mạng. Điều đó cho phép mỗi lần hoạt động, spam chiếm quyền điều khiển để đưa ra ngoài hàng triệu thư mà vẫn lưu lại được các danh sách đen.

Mô hình hoạt động kiểu "command-and-control" (lệnh và điều khiển) mềm dẻo của SpamThru cũng khiến cho các hãng cung cấp dịch vụ Internet (ISP), các nhà nghiên cứu và cơ quan thẩm định khó kiểm soát hay khoá hoạt động của chúng. SpamThru dựa trên kiểu truyền thông P2P (peer-to-peer) giữa các bot và bộ não điều khiển hacker của chúng. "Mỗi một bot đều biết về các bot khác trong cùng một mạng. Nếu một bot mất kênh lệnh và điều khiển, nó có thể truy vấn kênh luân phiên từ các bot khác. Điều này thực sự làm tăng tính đàn hồi cho các botnet".

Cùng với nhau, hai Trojan này kết hợp tạo ra con số khổng lồ thư rác trong tháng mười. Hãng nghiên cứu MessageLabs đã tiến hành thử nghiệm và thu được gần một triệu bản copy các biến thể của Warezov chỉ trong một khoảng thời gian 24 giờ hồi cuối tháng.

"Chắc chắn là tỷ lệ phát tán thư rác sẽ còn tiếp tục tăng cho đến cuối năm nay". Thậm chí chuyên

gia nghiên cứu Wood của MessageLabs còn cảnh báo rằng quý tư là khoảng thời gian lịch sử của các spammer. "Đây là tỷ lệ gia tăng cao nhất từ trước đến giờ. Tôi nghĩ rằng sẽ chỉ còn một chút xíu nữa con số này sẽ là 100%".

Trong bản báo cáo cuối tháng, MessageLabs cũng chú ý rằng trong khi tổng lượng e-mail phishing đang giảm dần thì tỷ lệ phần trăm thư độc hại liên quan đến lừa đảo vẫn gia tăng.

Ấn Độ là đất nước bị tấn công bằng e-mail có chứa virus nhiều nhất. Theo nghiên cứu, trong tháng mười, ở Ấn Độ, cứ trong 16 mail thì có 1 mail chứa phần mềm độc hại. Có nhiều bằng chứng cho thấy rằng hầu như một lượng gấp đôi tỷ lệ phần trăm các mail chứa phần mềm độc hại đó là spam. Lượng spam trong tháng mười tăng hơn 20,5% so với con số 49,3% của tháng trước.

Bạn có thể download bản báo cáo tháng mười của MessageLabs (kiểu file PDF) ở đây.

T.Thu