CHÚNG TA THUA TRONG TRẬN CHIẾN BOTNET?

Máy bạn đã bị tấn công bởi botnet? Nó là cái gì vậy?

Botnet (hay còn gọi là mạng botnet) là tập hợp các máy PC cho phép sử dụng dải băng rộng (broadband), bị chiếm quyền điều khiển trong suốt thời gian tấn công của virus và worm (sâu). Khởi đầu với phần mềm kết nối ngược lại server để nhận thông tin liên lạc từ kẻ tấn công ở xa, giờ đây các botnet này xuất hiện khắp mọi nơi.

Theo số liệu thống kê của Symantec sáu tháng đầu năm 2006, trung bình một ngày có khoảng 57 000 bot hoạt động.

Cũng trong thời gian đó, hãng cung cấp phần mềm anti-virus này còn phát hiện ra con số khổng lồ 4,7 triệu máy tính được sử dụng tích cực trong các mạng botnet. Các máy này là nơi cho những kẻ quản lý botnet phát tán thư rác, khởi chạy các cuộc tấn công DoS (denial of service), cài đặt malware hay phần mềm dò tìm bàn phím log keystrokes nhằm mục đích ăn trộm thông tin.

Nguồn: cknow

Các máy trong botnet đều có các hệ điều hành bị phá hoại, nổi bật như là một hub khóa cho nhiều nhóm tội phạm có tổ chức chuyên nghiệp trên thế giới. Chúng sử dụng băng thông ăn cắp của máy tính bị chiếm quyền điều khiển để kiếm tiền từ các hoạt động Internet phi pháp.

Botnet sẽ cài đặt adware và spyware để phát tán thư rác và khởi chạy các cuộc tấn công phishing. CPU lặp vòng từ botnet được hướng tới hoạt động kinh doanh ngầm hàng tỷ đô la phát triển mạnh trên các máy tính bảo mật lỏng lẻo. Chúng còn dùng "máy kéo tiền" này kết nối các thiết bị vật lý lại với nhau thành hệ thống trên cả thế giới.

Hiện nay cảm giác chung của các chuyên gia bảo mật là sự thất vọng. Họ không thể tìm kiếm và vô hiệu hóa được các botnet. Nỗi thất vọng ảnh hưởng lên sản phẩm bảo mật và thái độ, quan điểm của nhân viên công nghệ, những người vốn tin cậy vào họ.

"Chúng ta đã biết về botnet một vài năm nay. Nhưng tất cả những điều chúng ta thu được mới chỉ ở mức minh họa cách thức hoạt động của chúng. Tôi sợ rằng sẽ phải mất từ 2 đến 3 năm nữa

chúng ta mới tạo ra được bộ máy đáp trả lại chúng", Marcus Sachs - người phát ngôn của giám đốc SRI International ở Arlington (Mỹ) nói.

SRI là viện nghiên cứu phi lợi nhuận hỗ trợ Trung tâm nghiên cứu và phát triển bảo mật Cyber của chính phủ Mỹ.

Trận chiến với botnet được tăng cường cùng sự tham gia tích cực của các tình nguyện viên. Họ xác định được cơ sở hạ tầng "command-and-control" của botnet, làm việc với các hãng cung cấp dịch vụ Internet (ISP), buộc họ phải thực hiện các luật thẩm định để vô hiệu hóa chúng. Nhưng cảm giác chung vẫn là sự thất vọng. Các tay săn lùng botnet khám phá ra rằng sau nhiều năm giảm được một số command-and-control của botnet, đến nay nỗ lực của họ đang trở nên lãng phí.

"Chúng tôi đã quản lý để cố gắng kìm lại xu thế này, nhưng dường như chỉ vô ích", Gadi Evron – chuyên gia nghiên cứu bảo mật của Beyond Security ở Netanya (Israel), đồng thời cũng là người đứng đầu nhóm săn tìm botnet nói. "Khi chúng ta vô hiệu hóa một dịch vụ command-and-control, botnet ngay lập tức tạo lại trên một host khác. Chúng tôi không thể tiêu diệt được chúng triệt để".

"Chúng ta đang phải đương đầu với cuộc chiến trí tuệ gay go. 'Bè lũ' botnet được cải tiến và phát triển với tốc độ nhanh chóng, chúng ta không thể bắt kịp chúng. Có quá nhiều chướng ngại vật trên con đường của chúng ta", Evron bổ sung.

Quá trình cài đặt tổng hợp hiện nay bao gồm cả việc sử dụng các máy tính bị chiếm quyền điều khiển để phân bổ server DNS (Domain Name System) cung cấp các dịch vụ giải pháp tên miền cho kẻ phá hoại.

Điều này cho phép các bot thay đổi địa chỉ IP động mà không cần thay đổi thông tin trên DNS hay trên host (và cả biện pháp cố định xoay vòng) của các website phishing trên máy tính bot.

Số liệu thống kê từ nhiều nguồn khác nhau cho thấy tình trạng bi quan của Evron đưa ra là thực tế trong tình hình hiện nay. Theo dữ liệu của MSRT (Malicious Software Removal Tool) thì Trojan back-door và bot là "mối đe dọa đáng kể và xác thực đối với người dùng Windows".

Con số lặp đi lặp lại của MSRT trong tháng giêng năm 2005 cho thấy, công cụ này đã loại bỏ ít nhất một Trojan trong khoảng 3,5 triệu máy tính duy nhất. Trong 5,7 triệu máy tính bị nhiễm độc khoảng 62% nguyên nhân là do Trojan hoặc bot.

Cuộc chạy đua 'mèo vờn chuột'

Trend Micro, công ty bảo mật có trụ sở ở Tokyo đã bán công nghệ giảm bớt botnet cho các hãng cung cấp dịch vụ Internet. Công ty này ước lượng khoảng hơn 5% tất cả các máy tính kết nối tới Internet bị sử dụng trong các mạng botnet. Chúng càng ngày càng tinh vi hơn qua từng năm.

"Những 'gã' này ngày càng được cải tiến vượt ra ngoài sức tưởng tượng của bạn", Jose Nazario - kỹ sư phần mềm và bảo mật của Arbor Networks tại Lexington (Mỹ) nói.

“Chúng ta thấy rằng, hiện nay các botnet đã được quản lý cẩn thận hơn. Kỹ thuật chúng sử dụng để phân vùng bot tinh vi và thú vị hơn. Các bot được phân vùng trên nhiều server khác nhau theo băng thông hoặc khu vực. Nếu đó là một máy dial-up (máy số), những kẻ quản lý botnet biết rằng bot sẽ không được dùng nhiều. Thế nên chúng chỉ đặt trên một kênh, kết nối với phần mềm gián điệp (spyware) và trả tiền cho phần cài đặt”, Nazario nói.

Joe Stewart, chuyên gia nghiên cứu bảo mật kinh nghiệm của SecureWork ở Atlanta đã bỏ thời gian ra cấu trúc ngược các bot và nghe lén hoạt động truyền thông trên botnet. Những thông tin tìm được xác nhận một điều đáng sợ là những kẻ tạo ra botnet đang giành chiến thắng trong cuộc chạy đuổi mèo vờn chuột với kỹ thuật cao cấp chống lại các chương trình bảo vệ 'đang cố rượt đuổi phía sau'.

Chẳng hạn Trojan back-door Sinit đã hoàn toàn sử dụng được một mô hình phân phối P2P, khẳng định mức độ tinh vi ngày càng cao của các botnet. “Với Sinit, không có dịch vụ trung tâm nào không thể bị ngắt. Mỗi máy bị nhiễm độc trở thành một phần của mạng P2P. Qua đó các Trojan được phát tán trên tất cả các host”, Stewart nói.

Evron, người bắt đầu dò tìm botnet từ năm 1996 cho hay những kẻ tạo ra bot đang dùng các dịch vụ tên miền miễn phí để chuyển dời nhanh chóng các máy khỏi phạm vi được bảo vệ. Các botnet hiện đang hoạt động như những tế bào khủng bố offline, nơi các điều khiển botnet nhóm lại trong một cấu trúc kiểu cây.

“Chúng nâng cấp các điểm khiến ta không phát hiện hay gỡ bỏ được bất kỳ câu lệnh hay điều khiển nào. Đôi khi, câu lệnh và điều khiển có thể là một link yếu nào đó. Ngày nay có đủ kênh điều khiển dư thừa và dễ dàng chọn lựa cho chúng tồn tại”, Evron tiếp tục nhận định.

Stewart của SecureWork đồng ý rằng việc săn đuổi nhằm giảm các lệnh và điều khiển giờ không còn hiệu quả nữa. “Chúng ta đang chống lại những gã chuyên nghiệp. Đây là cơ hội kinh doanh lớn của những kẻ hoạt động trong bóng tối. Chúng ta đang được chứng kiến tất cả các chước lẩn lút điên rồ nhằm dẫn đầu cuộc đua của chúng.”

Xu hướng lợi nhuận

Nguồn: perryballard

Cuộc tấn công của sâu Mocbot trong tháng 9 là bằng chứng xác thực nhất nhắm vào mục đích lợi nhuận từ những kẻ xây dựng botnet.

Cuộc tấn công khai thác lỗ hổng bảo mật trong Windows Server Service. Chuyên gia nghiên cứu bảo mật ở German Honey-net Project đã phát hiện ra rằng các máy bị chiếm quyền điều khiển để cài đặt phần mềm dịch vụ quảng cáo là của công ty DollarRevenue. Công ty này phải trả từ 1 penny đến 30 cent mỗi lần cài đặt.

Qua 24 giờ mạng botnet điều khiển IRC thâu tóm được quyền kiểm soát của hơn 7.700 máy. Trong suốt 4 ngày, các nhà nghiên cứu đếm được khoảng 9.700 cuộc phá hoại từ một trung tâm command-and-control đơn. Ước chừng những kẻ tấn công có thể kiếm được khoảng 430 đô la hoa hồng chỉ riêng từ DollarRevenue.

Theo Stewart, hoạt động chính của botnet được liên kết với việc phát tán spam và các cuộc tấn công phishing ăn trộm mã ID.

Một bot điển hình sẽ được cài đặt trong hàng nghìn máy và bắt đầu thâu tóm địa chỉ e-mail lưu trữ trên ổ cứng. Sau đó nó thiết lập và mở proxy SOCKS chuyên dụng để gửi đi lượng thư rác khổng lồ.

Trong hầu hết các trường hợp, những kẻ điều khiển bot thuê mạng botnet cho các spammer. Nhưng Stewart và nhiều người khác đưa ra bằng chứng thực tế là hiện nay nhiều nhóm tội phạm hoạt động trực tiếp trên botnet nhằm phục vụ cho mục đích lợi nhuận.

Chúng có thể được dùng để kích hoạt các hoạt động mờ ám (DDoS, DoS phân phối, các cuộc tấn công); thăm dò lưu lượng ăn trộm dữ liệu dạng text chuyển qua máy đã mất quyền kiểm soát; cài đặt phần mềm thăm dò keystroke để đăng nhập và trộm tài liệu ngân hàng; sử dụng các cú click gian lận trên mạng quảng cáo ngữ cảnh; và thậm chí sử dụng các hoạt động thăm dò hay cả trò chơi trực tuyến.

Randal Vaughn, chuyên gia các hệ thống thông tin máy tính ở trường đại học Baylor (Waco, Texas) lại thấy lạc quan mặc dù danh sách người sử dụng link yếu vẫn còn rất dài. Hầu hết trong số họ là những người không biết nhiều về kỹ thuật.

“Khi bạn gặp phải vấn đề mang tầm quốc tế, các tổ chức luật pháp không có khả năng giúp bạn. Đơn giản vì họ không có thể xử lý vấn đề nghiêm trọng của botnet. Họ nhiệt tình, nghiêm túc, nhưng thật khó để một ai đó ở Mỹ đòi hỏi nhân viên thi hành pháp luật ở Nga hay Trung Quốc thực hiện công việc cho mình. Tôi không nghĩ chúng ta đã từng có các hoạt động giảm nhẹ botnet tích cực ở bất kỳ khu vực nào trên thế giới”, Vaugh nói trong một cuộc phỏng vấn.

Một ý kiến khác là cách giải quyết của các hãng ISP nhỏ giúp người dùng xử lý vấn đề với các máy tính bị nhiễm độc. "Không có lợi nhuận kinh tế nào dành cho một ISP chỉ ngồi bên điện thoại hàng tiếng rưỡi đồng hồ để giúp khách hàng khôi phục máy tính bị tấn công. Giá cả cho dịch vụ này gấp nhiều lần so với giá thuê bao điện thoại". Một lượng lớn người dùng máy tính sử dụng

các phiên bản Windows khác nhau không cập nhật đầy đủ bản và lỗi tạo môt trường 'chín muồi' cho những kẻ phá hoại.

"Chúng ta cần cung cấp cho các hãng ISP công cụ xử lý vấn đề tốt hơn. Dàn xếp lại với các khách hàng một cách thủ công không hề khả thi về mặt kinh tế", Stewart nói. Ông có kế hoạch xây dựng nỗ lực truyền thông tạo ra công cụ miễn phí giúp tự động loại bỏ các bot trên mạng của hãng cung cấp dịch vụ Internet.

Một vài hãng bảo mật đã bắt đầu tung ra thị trường sản phẩm anti-botnet. Tháng 9, Trend Micro phát hành InterCloud Security Service, dịch vụ mới cung cấp công nghệ loại bỏ botnet cho các hãng ISP, trường đại học hay nhiều hãng cung cấp mạng lớn khác. InterCloud có khả năng xác định kẻ phá hoại trên mạng, cung cấp giải pháp tái sắp xếp tự động để ngăn chặn chúng ở môi trường thời gian thực.

Damballa, bắt đầu với các liên kết với khoa Tin học ở Viện công nghệ Georgia. Họ mạo hiểm tăng cường nguồn đầu tư để tạo ra công nghệ xác định chính xác lưu lượng Internet phát sinh bởi những kẻ phá hoại hay chiếm quyền điều khiển máy tính.

Nhưng, đến giờ thì những kẻ phá hoại vẫn đang giành chiến thắng.

T.Thu