HIỂM HỌA BẢO MẬT THẾ HỆ MỚI

Tháng Một năm nay, một thiếu niên 20 tuổi đã bị buộc tội xâm nhập vào máy tính của chính phủ Mỹ và điều khiển chúng vào các phi vụ... lừa đảo.

Nguồn: Techcentral

Jeanson James Anc

Tháng Một năm nay, một thiếu niên 20 tuổi đã bị buộc tội xâm nhập vào máy tính của chính phủ Mỹ và điều khiển chúng vào các phi vụ... lừa đảo.

Nguồn: Techcentral

Jeanson James Ancheta đã cấy phần mềm Trojan vào hệ thống máy tính của Trung tâm Hải quân China Lake tại Sa mạc Mojave ở California, từ đó, giành được quyền điều khiển máy tính trong toàn mạng. Jeanson đã sử dụng "botnet VIP" này để tạo ra lượng hit cho các quảng cáo trên website và thảnh thơi thu tiền trả công từ các nhà quảng cáo. Nghe có vẻ vô hại và tiểu tiết quá chăng? Bạn sẽ không nói như vậy, nếu biết vố làm ăn này đã giúp Ancheta bỏ túi tới 60.000 USD trước khi bị phát hiện. Chưa hết, các nhân viên điều tra còn khám phá ra rằng Ancheta đang kiểm soát khoảng hơn 400.000 máy tính trên toàn thế giới. Số máy tính Zombie này hoàn toàn cúi đầu trước mọi chỉ thị từ xa của hắn, từ tạo ra lượng hit cho các banner quảng cáo , phát tán thư rác cho đến gửi malware tới các máy tính hớ hênh khác. Có thể nói, Ancheta là ví dụ điển hình cho một loại hình tội phạm mới trên mạng Internet, có động cơ mãnh liệt về tiền bạc và vật chất. Những chương trình Spyware hoặc Trojan mà chúng cấy vào máy tính người dùng, một khi được cài đặt, sẽ hoạt động miệt mài và cần mẫn như những nô lệ trung thành, phục dịch ông chủ của chúng từ xa. Hiếm khi người dùng vô tư nhận biết được rằng máy tính của họ đã bị tấn công. Hệ

thống vẫn làm việc bình thường, ngoại trừ có lúc hơi chậm chạm một chút. Và tất nhiên, họ chẳng hay biết gì tới những nhiệm vụ bí mật mà máy tính của mình đang tiến hành. Ung nhọt mới Các botnet đang trở thành một khối ung nhọt mới, nhức nhối trong địa hạt bảo mật Internet. Theo thống kê của hãng bảo mật CipherTrust, có tới hơn 180.000 máy tính bị biến thành zombie mỗi ngày, và con số này không hề muốn dừng lại ở đó.

Nguồn: Infotech

Hacker có thể sử dụng botnet để đánh lừa các nhà quảng cáo trực tuyến (như trong trường hợp Ancheta), hoặc có thể cho thuê theo giờ để phát tán thư rác với số lượng lớn. Nhiều kẻ thậm chí còn thuê botnet để tiến hành các vụ tấn công từ chối dịch vụ nhằm vào website đối thủ. Dễ dàng nhận thấy những hoạt động này diễn ra rất chuyên nghiệp, theo một quy trình khép kín "ăn cháo trả tiền". Nó đang dần thay thế phong cách hành xử của các hacker nghiệp dư trước đây, vốn coi tấn công chỉ là sở thích. "Những đợt bùng phát virus lớn như Sasser và Blaster càng ngày càng ít. Nhiều người tưởng rằng tình hình đang được cải thiện, trong khi thực tế nó càng ngày càng tệ hơn", Mikko Hypponen, giám đốc nghiên cứu của F-Secure cho biết. "Những vụ tấn công diễn ra tập trung hơn, có mục tiêu cụ thể hơn nên người dùng ít biết. Nhưng thiệt hại thì khổng lồ". Trong mắt Hypponen, botnet là một cơn đau đầu không dễ chữa, bởi máy tính Zombie hầu hết là PC gia đình có nối mạng. "Phải mất rất nhiều thời gian và công sức để giải thích với một người dùng bình thường về những khái niệm kiểu này, cũng như cách "giải phóng" cho máy tính của họ. Vì thế, đại bộ phận các ISP đều khoanh tay làm ngơ".
Mặt trận mới của phishing Hầu hết giới phân tích đều dự đoán các vụ tấn công phishing sẽ tăng tiến với tốc độ tên lửa, cả về số lượng lẫn độ tinh vi.

Nguồn: Techcentral

David Sancho, một chuyên gia diệt virus tại Trend Micro đã minh chứng bằng một vụ tấn công mới đây tại Đức. Kẻ tấn công giả dạng một công ty điện lực, gửi email tới cho các nạn nhân và yêu cầu họ kiểm tra hóa đơn bằng cách click vào file PDF đính kèm. Trong trường hợp này, file đính kèm có đuôi .pdf.exe và nó đã cấy Trojan vào máy tính người nhận. "Một khi được kích hoạt, nó sẽ âm thầm theo dõi mọi kết nối Internet, mọi lần truy cập trang web, mật khẩu và username của bạn rồi báo cáo lại cho "Ông chủ". Phương án này rất thông minh, vì hacker không cần phải lập ra một máy chủ giả". Hypponen cũng dự đoán rằng giới phisher sẽ sớm tìm ra cách bẻ gãy mật khẩu dùng-một-lần mà nhiều ngân hàng đang sử dụng làm hàng rào bảo mật. "Người nhận bị lừa đăng nhập vào một ngân hàng giả, và tại đây, chúng đòi họ khai báo mã xác thực. Ngân hàng giả sẽ truy cập vào ngân hàng thật bằng mật khẩu này rồi rút sạch tiền. Sau đó, nó sẽ quay trở lại với người dùng, thông báo là có lỗi xảy ra và yêu cầu cung cấp tiếp mã xác thực khác". Tìm "gà" để "chăn"

Nguồn: Infotech

Thách thức lớn nhất đối với dân phisher là tìm "gà" để "chăn", do ngày càng nhiều người dùng biết tới hình thức tấn công này. Giải pháp của chúng là nhắm đến những mục tiêu nhỏ hơn và sử dụng các ngôn ngữ khác ngoài tiếng Anh, chẳng hạn như Hy Lạp, Séc và Phần Lan. Mặc dù máy tính Windows vẫn là mục tiêu ngắm bắn chính, song hãy chuẩn bị tinh thần đón nhận các cuộc tấn công phisher nhắm vào ĐTDĐ. F-Secure cho biết họ đã phát hiện được 179 con virus di động và ước tính có khoảng hàng chục ngàn điện thoại đã bị "dính chưởng". Nokia đã đối phó với cảnh báo này bằng việc tung ra những mẫu điện thoại có phần mềm diệt virus tích hợp, đồng thời siết chặt hàng rào bảo mật cho các model chạy hệ điều hành Symbian phiên bản 9. Tuy nhiên, F-Secure cũng đã ghi nhận được phần mềm Java hiểm độc đầu tiên viết riêng cho ĐTDĐ, đồng nghĩa với việc mọi mẫu dế, không riêng gì dòng cao cấp, đều nằm trong vùng nguy cơ. Tháng 3 vừa qua, Hypponen đã phát hiện thấy một Trojan di động chuyên gọi về một số điện thoại tại Nga. Cứ mỗi lần như thế, nó lại mang về 5 euro cho kẻ phát tán.
Thiên Ý