Vius máy tính - Nguy cơ thường trực của an ninh mạng máy tính tại Việt Nam

Trường Sơn - Thanh Hải

58,6 triệu lượt máy tính tại Việt Nam bị nhiễm virus; có 57.835 dòng virus xuất hiện mới, virus lây lan nhiều nhất là W32.Conficker.Worm, nó đã tấn công 6,5 triệu lượt máy tính; các virus siêu đa hình (Metamorphic virus) là nỗi ám ảnh với người sử dụng máy tính tại Việt Nam, với khả năng thay hình đổi dạng để lẩn trốn, 2 dòng virus Vetor và Sality đã lan truyền trên 5,9 triệu lượt máy tính, và trung bình một ngày đã có hơn 160 nghìn máy tính bị nhiễm virus đó những thông tin mà Hệ thống giám sát virus của Bkav đã nghi nhận được được trong năm 2010, cho thấy báo động đỏ về tình hình virus máy tính tại Việt Nam.

Bùng nổ phần mềm diệt virus giả mạo Fake AV.

Năm 2010 đã chứng kiến sự bùng nổ lượng máy tính bị nhiễm virus giả mạo phần mềm diệt virus, lên đến 2,2 triệu lượt, gấp 8,5 lần so với con số 258.000 của năm 2009.

Dẫn dụ người sử dụng tới các website giả mạo quét virus trực tuyến, nhằm cài đặt mã độc lên máy tính là đặc điểm chung của các FakeAV. Theo nghiên cứu của Bkav, nguyên nhân chính khiến rất nhiều người sử dụng tại Việt Nam đã nhiễm những loại viurs này là do thói quen dùng phần mềm trôi nổi, không có bản quyền. Với thói quen này, mặc dù đã được các chuyên gia cảnh báo từ trước, nhưng người sử dụng vẫn dễ dàng hồn nhiên bấm vào mọi đường link cho dù chưa rõ nó là cái gì. Đây là sơ hở chết người để các Fake AV lây nhiễm vào máy tính.

Chuyên gia Bkav khuyến cáo: "Hãy từ bỏ thói quen dùng phần mềm không có bản quyền, điều này sẽ giảm thiểu các nguy cơ về an ninh đối với máy tính của bạn.

Giả mạo file dữ liệu, xu hướng mới của virus

Hơn 1,4 triệu lượt máy tính đã bị nhiễm dòng virus giả mạo thư mục, giả mạo file ảnh, file word, excel Theo phân tích của Bkav, dòng virus này sẽ là một xu hướng mới trong thời gian tới.

Bằng cách sử dụng icon để ngụy trang, file thực thi của virus trông có vẻ giống hệt một thư mục hay một file dữ liệu dạng ảnh, file word, file excel Điều này đã dễ dàng đánh lừa cảm quan của người sử dụng, thậm chí là cả các chuyên gia có kinh nghiệm, khiến họ dễ dàng mở file virus và bị nhiễm mà không chút nghi ngờ. Đây cũng là lý do khiến dòng virus này tuy mới xuất hiện nhưng đã lan truyền với tốc độ chóng mặt.

Bkav khuyến cáo người sử dụng cần hết sức cảnh giác với xu hướng mới này của virus. Cần sử dụng phần mềm diệt virus có bản quyền để được tự động bảo vệ, diệt virus trước khi mở file bất kì trên máy tính.

Virus phá hủy dữ liệu quay trở lại

Trong năm qua, hệ thống giám sát virus của Bkav đã 2 lần phát hiện những đợt virus phá hủy dữ liệu mới xuất hiện. Các dòng virus này được Bkav đặt tên là W32.Delfile.Worm, W32.FakeStuxer.Trojan. Tuy chưa gây hậu quả nghiêm trọng trên diện rộng, nhưng sự quay trở lại của virus phá hủy dữ liệu sẽ là mối đe dọa lớn đối với dữ liệu của người sử dụng trong thời gian tới.

Theo quy luật phát triển hình xoáy trôn ốc, sự quay trở lại của loại virus này với hình thái mới sẽ có hành vi tinh vi hơn so với những virus phá hủy dữ liệu của những năm 90. Các dòng virus phá hủy dữ liệu mới được trang bị các kỹ thuật lây lan nhanh qua Internet, nên tốc độ phát tán hơn hẳn so với việc âm thầm lây lan của những virus phá hủy dữ liệu trước đây. Chính vì vậy, mức độ nguy hiểm gấp hàng nghìn lần.

Với xu hướng tập trung nhiều dữ liệu quan trọng trên máy tính như hiện nay, virus phá dữ liệu quay trở lại với tốc độ lây lan nhanh chóng, sẽ gây ra những hậu quả khôn lường khi lây lan trên diện rộng. Để phòng tránh virus này, người dùng nên sử dụng phần mềm diệt virus có bản quyền và quét virus thường xuyên. Đồng thời, nên sao lưu dữ liệu quan trọng ra các thiết bị lưu trữ khác để đảm bảo an toàn khi máy tính xảy ra sự cố.

Báo động tình trạng phát tán virus để xâm nhập hệ thống, tấn công DDoS

Liên tiếp nhiều website lớn tại Việt Nam bị virus xâm nhập, lộ thông tin quan trọng hay bị tấn công DDoS trong thời gian qua đang là vấn đề gây lo lắng trong xã hội.

Các chuyên gia của Bkav đã phát hiện một số nhóm hacker đã cài đặt virus xâm nhập vào các hệ thống mạng tại Việt Nam, qua đó đánh cắp thông tin bí mật nội bộ của các tổ chức. Bên cạnh đó, chúng còn kiểm soát được các website chuyên download phần mềm nhằm cài đặt virus vào các máy tính tải phần mềm từ các website này. Từ đó chúng có thể điều khiển mạng lưới máy tính ma - botnet - để tấn công DDoS vào các hệ thống lớn tại Việt Nam. Đây là tình trạng đáng báo động vì ngoài việc các hệ thống lớn có thể bị tấn công bất cứ lúc nào, còn có hàng chục nghìn máy tính trên cả nước đang bị hacker điều khiển, có thể gây ảnh hưởng đến an ninh quốc gia.

Danh sách 15 virus lây nhiều nhất trong năm 2010

1 W32.Conficker.Worm
2 W32.Vetor.PE
3 W32.Sality.PE
4 W32.AutoRunUSB.Worm
5 W32.SecretCNC.Heur
6 W32.ForeverX.Worm
7 W32.CmVirus.Trojan
8 W32.UpdateUSBA.Worm
9 W32.StuxnetQKE.Trojan
10 X97M.XFSic
11 W32.SilityVJ.PE
12 W32.BedolabD.Worm
13 W32.Regsvr.Trojan
14 W32.DownRefronE.Worm
15 W32.SysdiagTHA.Trojan

Để tránh cho máy tính của mình rơi vào tầm kiểm soát của các hacker này, người sử dụng cần hết sức cảnh giác khi tải các phần mềm về máy tính của mình. Chỉ nên tải các phần mềm cần thiết từ website của chính nhà sản xuất, hạn chế tối đa việc tải phần mềm từ các nguồn trung gian, kể cả đó là các nguồn phổ biến. Đồng thời, người sử dụng cũng cần cập nhật thường xuyên phần mềm diệt virus trên máy tính của mình để kịp thời ngăn chặn virus xâm nhập.

Dự báo tình hình virus máy tính năm 2011

Theo ông Vũ Ngọc Sơn - Giám đốc Bộ phận nghiên cứu Công ty Bkav: Rootkit sẽ là một xu hướng mới khi đã trở thành công cụ đại chúng hóa chứ không còn là đặc quyền của một số tin tặc biết nghề như trước. Các dòng virus siêu đa hình sẽ kết hợp nhiều kỹ thuật mới để tạo ra những sự lây lan dai dẳng kéo dài trong nhiều năm.

Cùng sự phổ biến của Windows 7 với khả năng đảm bảo an ninh cao và mọi quyết định thực thi quan trọng trên máy tính sẽ thuộc về người sử dụng, xu hướng virus đánh lừa người sử dụng bằng cảm quan sẽ phát triển mạnh. Trường hợp các virus giả mạo file dữ liệu (Fake icon) là những biểu hiện đầu tiên và xu hướng này sẽ tiếp tục trong năm 2011.

Virus mang động cơ chính trị-xã hội sẽ xuất hiện nhiều, lợi dụng các trang download phần mềm phổ biến để phát tán, tạo ra mạng botnet, tấn công có chủ đích các mục tiêu định trước, lấy trộm các thông tin bí mật của tổ chức, cá nhân.

Sẽ có nhiều cuộc tấn công, lừa đảo trên điện thoại di động trong năm 2011. Có thể sẽ ghi nhận những cuộc phát tán mã độc đầu tiên trên điện thoại di động, với hình thức tấn công chủ yếu dưới dạng các trojan, ăn náu và ăn cắp thông tin cá nhân■

Quản lý việc truy cập Internet của nhân viên

1. Sử dụng Packetfence:

Đây là 1 trong những công cụ giám sát và quản lý các hoạt động trong toàn bộ hệ thống mạng. Chương trình miễn phí, mã nguồn mở này dễ cài đặt và quan trị trên nhiều hệ điều hành như Red Hat Enterprise Linux, CentOS, Ubuntu hoặc Debian. Với Packetfence, bạn hoàn toàn có thể giám sát và cấp quyền cho những ai được phép truy cập Internet, trong thời gian bao lâu, giới hạn trong khoảng nào... Bên cạnh đó, những tài khoản hoặc thiết bị kết nối bên ngoài không thuộc danh sách cho phép cũng không thể truy cập và sử dụng Internet.

2. Sử dụng Open DNS:

OpenDNS là 1 trong những công cụ hữu dụng nhất giúp quản lý DNS, bảo mật hệ thống... hoàn toàn dựa trên nền tảng Web. Với OpenDNS, người quản lý có thể lọc nội dung, ngăn chặn nạn lừa đảo phishing, các địa chỉ web (với phiên bản Enterprise), phòng chống malware (Enterprise)...

3. Quản lý trực tiếp mức tài nguyên hệ thống:

Và Net Spy Pro là 1 trong những công cụ giúp người quản lý có thể giám sát được hoạt động của bất cứ tài khoản nào khi họ truy cập Internet, thậm chí còn biết được mục bookmark và favorite của nhân viên. Nếu được áp dụng một cách hợp lý thì có thể xem đây là công cụ hoàn hảo nhất hiện nay, vì đôi khi người quản lý can thiệp quá sâu vào việc làm cũng như các yếu tố cá nhân khác.

4. Hãy đảm bảo chính sách sử dụng hợp lý:

Thay vì việc điều khiển và kiểm soát bằng phần mềm, dựa vào tính chất công việc và môi trường của nhân viên, hãy áp dụng những chính sách và kế hoạch sử dụng tài nguyên của công ty một cách hài hòa, hợp lý trong toàn bộ thời gian làm việc. Hãy cố gắng tự tạo ra 1 môi trường hòa đồng, nghiêm túc trong công việc, nhưng không nên quá căng thẳng. Vấn đề là người quản lý sẽ xử lý thế nào với những chính sách của họ đưa ra, với từng trường hợp nhân viên vi phạm cụ thể, họ không thể áp dụng 1 cách khô khan cũng như không thể quá đơn giản, nhẹ nhàng... vì làm như vậy sẽ mang lại kết quả không mong muốn.

Đi kèm với những chính sách áp dụng nội quy chặt chẽ, bạn cũng nên cân nhắc đến một số quy chế với tính linh hoạt cao. Bạn vẫn có thể đảm bảo được tiến độ công việc và kế hoạch, nhưng bù lại sẽ mất đi những mối liên kết cần thiết giữa nhân viên và người quản lý, đối với một số doanh nghiệp hoặc đặc thù công việc thì đây lại là điểm mấu chốt để có được thành công!

Hồng Ngọc (Theo Tech Republic)