VIRUS MÁY TÍNH: 20 NĂM NHÌN LẠI

Trong 3 thập kỷ phát triển của máy vi tính, tồn tại một dấu lặng đã hai mươi năm: virus máy tính. Con người đã tốn rất nhiều công sức để phát triển khoa học máy tính và cũng không ít công sức để loại trừ virus. Giống như một căn bệnh trầm kha, viru

Trong 3 thập kỷ phát triển của máy vi tính, tồn tại một dấu lặng đã hai mươi năm: virus máy tính. Con người đã tốn rất nhiều công sức để phát triển khoa học máy tính và cũng không ít công sức để loại trừ virus. Giống như một căn bệnh trầm kha, virus máy tính vẫn không hề thuyên giảm. Chúng liên tục phát triển với quy mô và tác hại ngày càng lớn hơn. Giải pháp nào cho virus máy tính? Một câu hỏi tưởng chừng đơn giản nhưng vẫn chưa có giải đáp thỏa đáng. Chúng ta hãy lật lại dòng thời gian, cùng phân tích và suy ngẫm để tìm lời giải cho bài toán "liên thế kỷ" này. Virus máy tính, trò đùa dai dẳng Thật ra virus máy tính đã có từ những năm đầu của thập niên 1970. Các virus Creeper (1970), Rabbit (1974) và Animal (1980) được xem là ông tổ của virus máy tính. Tuy nhiên do sinh ra trên các máy tính lớn nên chúng chỉ lây quanh quẩn ở các phòng thí nghiệm, chẳng được mấy ai quan tâm ngoài các chuyên gia tin học. Virus máy tính chỉ gây tác động mạnh đến xã hội khi chúng chuyển từ máy tính lớn sang máy tính cá nhân. Brain là virus máy vi tính đầu tiên (1986) thực hiện nhiệm vụ này. Mục đích ban đầu của Brain là phục vụ quảng cáo cho công ty Brain Computer Service ở Lahore (Pakistan). Khi máy tính nhiễm virus, một màn hình bất ngờ xuất hiện giới thiệu tên tuổi, địa chỉ, có cả điện thoại liên lạc của công ty! Ký sinh vào boot sector đĩa mềm loại 360KB, phương tiện lưu trữ trao đổi dữ liệu phổ biến nhất lúc bấy giờ, virus Brain đã lây nhiễm trên toàn thế giới. Mặc dù không gây hại cho máy tính nhưng Brain đã làm cho nhiều người sử dụng máy tính hoảng sợ. Sau Brain, các boot-sector virus (B-virus) khác lần lượt xuất hiện như Lehigh, Vienna, Cascade, Pingpong... Virus ở thời kỳ này đều "lành tính", phần lớn bắt nguồn từ các trường đại học nơi có nhiều sinh viên giỏi, hiếu động và thích đùa. Tuy nhiên sự hiền lành của chúng không kéo dài được bao lâu. Để tạo ấn tượng mạnh, các hacker rắp tâm đưa các đoạn mã độc vào B-virus khiến chúng trở nên hung tợn hơn. Đại diện của loại này là virus Disk Killer (Sát thủ đĩa). Sau 30 giờ lây nhiễm, virus này sẽ mã hóa số liệu định vị các phân khu đĩa khiến hệ thống bị tê liệt, đồng thời toàn bộ dữ liệu bị phá hủy. Do tấn công máy tính trước khi hệ điều hành khởi động nên dù có kích thước nhỏ (512-2048 byte) nhưng B-virus vẫn khống chế dễ dàng các tác vụ truy xuất đĩa ở mức BIOS, độc lập với hệ điều hành. Nhược điểm lớn nhất của B-virus là khả năng kích hoạt không cao (vì không phải máy tính nào cũng khởi động từ đĩa mềm). Để chống B-virus, các nhà sản xuất ROM-BIOS đã có một động thái hết sức kịp thời: cung cấp tùy chọn vô hiệu khả năng khởi động máy tính từ đĩa mềm. Một số nhà sản xuất chip còn tích hợp thủ tục nhận dạng các hành vi tựa B-virus vào ROM-BIOS. Trước tình hình này, các hacker ra sức chống đỡ bằng cách mở rộng đối tượng lây sang các tập tin thi hành COM và EXE của hệ điều hành, khai sinh loại virus mới: virus file (F-virus). Mặc dù phải lệ thuộc vào hệ điều hành, nhưng F-virus đã giải quyết được các nhược điểm cơ bản của B-virus. Sử dụng tập lệnh của hệ điều hành, F-virus không những vô hiệu các chương trình nhận dạng hành vi tựa virus trong ROM mà còn nâng cao khả năng tạo nhiều bản sao ký sinh trên các đối tượng khác trên hệ thống. Người Việt Nam thập niên 1990 vẫn còn nhớ những đợt tấn công ấn tượng của virus Friday 13th, Datalock, Little Girl, White Rose... trên hệ điều hành MS-DOS vốn có cấu trúc đơn giản với nhiều lổ hổng bảo mật nghiêm trọng. Tuy nhiên sự tồi tệ chỉ mới bắt đầu. Cùng với F-virus, các virus lưỡng tính (lây cả boot sector và tập tin thi hành) như BFD, Compback, Invader, Junkie, Natas... mặc sức hoành hành trên cả 2 tập chỉ thị ROM-BIOS và hệ điều hành. Các virus lây trên cấu trúc đĩa như

Dir2/FAT, Weichan... cũng nhảy vào tham chiến, khiến tình hình càng rối ren và ảm đạm. Nhận thức sự yếu kém của các sản phẩm 16 bit, Microsoft đã quyết định ngừng phát triển MS-DOS và Windows 3.x. Năm 1995 hãng này trình làng hệ điều hành 32 bit giao diện đồ họa. Sự ra đời của Windows 95 đánh dấu bước chuyển gam màu của bức tranh công nghệ thông tin toàn cầu đồng thời làm lay chuyển cả thế giới virus máy tính. Nếu như các ứng dụng MS-DOS chạy trong chế độ thực theo từng phiên làm việc đơn lẻ, thì ứng dụng của Windows 95 hoạt động trong chế độ bảo vệ theo mô hình đa nhiệm. Mỗi tiến trình được Windows cấp một không gian riêng, hoàn toàn tách biệt với các ứng dụng khác. Mô hình này đã xáo trộn kỹ thuật thiết kế F-virus của các hacker. Trong môi trường đơn nhiệm, từ vùng nhớ thường trú riêng của nó, F-virus có thể tự do can thiệp vào không gian của các ứng dụng khác. Trong môi trường đa nhiệm, bản thân F-virus chỉ có thể hoạt động quanh quẩn trong không gian máy ảo của ứng dụng chứa nó. Mặc dù vậy, một số F-virus trên Windows (như Spenna Spy, Bodgy, Bolzano, Pate...) cũng cố gắng khai thác các hàm tìm kiếm thư mục để chèn mã lệnh vào các tập tin đang "ngủ" trên hệ thống đĩa. Biện pháp này chỉ cải thiện tình thế tạm thời do virus rất dễ bị phát hiện (đĩa cứng bị truy cập liên tục, không gian đĩa gia tăng một cách đáng ngờ, tốc độ máy bị suy giảm đáng kể...). Có lẽ những người phát triển virus máy tính hiểu rất rõ ý nghĩa của phương ngôn "cái khó ló cái khôn". Concept là một trong những virus như thế. Khai thác tập mã lệnh macro (VB Application) trong bộ công cụ văn phòng Microsoft Office, tác giả virus này đã khai sinh một loại virus mới chỉ nhằm để "prove my point", chứng minh cho quan điểm của mình: virus cũng có thể lây vào tập tin dữ liệu! Mặc dù không phá hoại, nhưng điều tệ hại nhất mà hacker này đã làm là công bố toàn bộ mã lệnh của virus. Việc này đã châm ngòi cho giai đoạn "hậu Concept" với sự xuất hiện của các virus macro CAP, Gold Fish, CyberHack, JohnMMX... Không dừng ở đó, các virus macro còn "lấn sân" sang Microsft Excel với các "sản phẩm để đời" như Laroux, HalfCross, After-5h... Cả tập tin trình diễn của Power Point cũng bị virus TriState lây nhiễm. Không hài lòng với tập mã lệnh VBA, các hacker còn nghiên cứu các kiểu lây lan phá hoại khác. Hàng loạt các loại mã độc như worm (sâu trình), ngựa gỗ (trojan horse), cửa hậu (backdoor)... lần lượt xuất hiện. Không lây trực tiếp vào tập tin thi hành kiểu F-virus, chúng tồn tại và hoạt động như một ứng dụng độc lập. Lợi dụng giao tiếp mạng, chúng tự gửi chính mình đến các địa chỉ thu thập được trên các trạm trung gian trên đường truyền. DemiURG, loại virus mệnh danh "7 trong 1" là một điển hình. Lan truyền qua mạng đến máy đích, DemiURG phát tán thành 7 mẫu lây nhiễm dạng BAT, EXE-DOS, EXE-16, EXE-32, DLL, XLS và VBS. Khi một mẫu phát hiện "con mồi", nó tập hợp 7 anh em cùng lây vào đối tượng. Khi một mẫu nào bị tiêu diệt, các mẫu khác sẽ tiếp ứng cho kẻ bại trận. Trước tình thế lợi bất cập hại, Microsoft đành "bấm bụng" bổ sung chức năng "Warning virus macro" trong bộ MsOffice 97. Động thái này đã làm giảm số virus macro nhưng cũng khiến nhà khổng lồ một phen toát mồ hôi vì uy tín bị sút giảm: khách hàng không còn mặn mà với tập lệnh VBA, từng được quảng cáo là công cụ tùy biến mạnh mẽ cho người dùng cấp cao. Nhận thức sự lớn mạnh của Internet, năm 1998 Microsoft giới thiệu phiên bản Windows 98 bổ sung nhiều dịch vụ mạng quan trọng. Có thể nói bộ sản phẩm Windows 98 và MSOffice 97 đã giải quyết rất tốt vai trò của chúng trong môi trường cộng tác và chia sẻ. Tuy nhiên đám mây virus không thực sự tan hẳn. Mặc dù tỏ ra vượt trội hơn MS-DOS về bảo mật nhưng Windows 9x cũng có những yếu kém nhất định. CIH (hay còn gọi là Chernobyl) là một minh chứng cho sự lỏng lẻo của hệ điều hành này. CIH được phát hiện vào 7-1998 ở Đông Nam Á. Tác giả của nó cho rằng mức độ tàn phá của virus này giống như thảm họa rò rỉ lò phản ứng hạt nhân Chernobyl vào ngày 26-4-1986 ở Nga mà nhân loại phải cảnh giác. Các biến thể CIH lây vào file EXE-32 của Windows 9x. Mỗi khi kích hoạt, CIH kiểm tra ngày hiện

tại của hệ thống để quyết định "ra tay" hay chỉ lây sang các EXE khác. Nếu đúng ngày 26-4 (đối với dị bản 1003 và 1049) hoặc 26 hàng tháng (đối với dị bản 1019), CIH format track 0 tất cả các ổ đĩa cứng trên máy, sau đó CIH ghi "rác" vào flash ROM khiến máy bị phá hủy hoàn toàn. Khai thác điểm yếu của Windows 95, CIH đã làm thay đổi nhận thức chủ quan của người dùng rằng "virus máy tính chỉ phá hủy dữ liệu luận lý, chúng không thể chạm đến phần cứng của máy". Với kịch bản tội lỗi của nó, CIH đã làm hỏng hàng triệu chiếc máy tính "hàng hiệu" trên toàn thế giới (loại sử dụng chip ROM hàn chết trên bo mạch chủ). Trong khi Microsoft vẫn chưa "hoàn hồn" sau cú ra đòn của CIH thì lũ virus macro "tép riu" lại gây rối. Tháng 3-1999, Melissa (họ hàng với VicodinES) đã thực hiện một cú ngoạn mục. Chỉ sử dụng tập lệnh VBA, Melissa là virus macro đầu tiên có khả năng gửi mã lệnh của nó đến các địa chỉ email trong sổ địa chỉ máy nạn nhân. Nhờ dịch vụ thư điện tử, Melissa đã làm lây nhiễm hàng trăm nghìn máy tính trong vài giờ, một tốc độ lây đáng nể mà các hacker hằng ao ước. Đến lượt nó, Melissa đã "nêu gương" cho các virus khác như Sircam, Nimda học tập. Tuy nhiên kịch bản của bọn này khác với Melissa. Khi chiếm quyền điều khiển hệ thống, chúng ngang nhiên sục vào thư mục My Documents lục lọi tài liệu riêng tư của người dùng rồi gửi đến các máy khác. Đòn này khiến nhiều người "chết đứng", nhất là các nhà kinh doanh vì bí mật của công ty bị phơi bày trước bàn dân thiên hạ. Trước tình thế này, Microsoft quyết định thay Windows 9x bằng hệ điều hành Windows 2000 sử dụng công nghệ Windows NT với định dạng đĩa NTFS, được đánh giá là tốt hơn FAT32 về mặt tổ chức và bảo mật. Sau "gã" Windows 2000 cục mịch rắn rỏi, cô gái Windows XP đỏm dáng được ông bầu Microsoft "lăng-xê" với nhiều đặc điểm vượt trội: hỗ trợ nhiều CPU, quản lý bộ nhớ chặt chẽ, truy xuất đĩa tốt hơn, bảo vệ mã thi hành ActiveX, hỗ trợ đa phương tiện mạnh mẽ, điều khiển truy cập từ xa... Năm 2003, Microsoft chính thức thông báo ngừng hỗ trợ kỹ thuật cho người dùng Windows 9x, có nghĩa các hệ điều hành Windows 95, Windows 98 và Windows Me đã được "khai tử". Mặc cho những cố gắng cải thiện bảo mật của Microsoft, các hacker vẫn không ngơi tay phá hoại. Năm 2001 sâu Blaster, sau đó là Sasser khai thác lổ hổng bảo mật Remote Access Control để ra lệnh shutdown máy tính nạn nhân từ xa. Kịch bản này cũng được Slammer (2003) thực hiện với mức độ nguy hiểm hơn: đóng sập các SQL Server bằng cách gửi thông điệp qua cổng giao tiếp mà không cần ghi mã lệnh virus xuống đĩa cứng. Năm 2005 là một năm đầy biến động với 2 sự kiện nổi cộm trong lĩnh vực bảo mật. Đáng chú ý nhất là vụ làm giả, đánh cắp các loại thẻ tín dụng quốc tế. Các chuyên gia an ninh cho rằng trong vụ này nhất định có sự tiếp sức của các phần mềm hoạt động như virus máy tính, bí mật thâm nhập vào hệ thống lưu trữ cơ sở dữ liệu, đánh cắp số ID tài khoản người dùng cung cấp cho các cơ sở in thẻ lậu. Vụ thứ 2 ít nổi đình nổi đám hơn nhưng lại mang một ý nghĩa khác: sự đối đầu giữa các tổ chức hacker Mydoom và Netsky. Chống phá và loại trừ lẫn nhau, các nhóm hacker từ nhiều nước khác nhau đã làm náo loạn cả thế giới công nghệ thông tin. Đến nay, tuy cuộc chiến đã bớt phần căng thẳng nhưng tên tuổi các virus này vẫn còn trong danh sách xếp hạng "top-hot" của các hãng bảo mật. Đi tìm giải pháp chống virus Trong cuộc chiến chống virus máy tính, các phần mềm quét virus (còn gọi là anti-virus) đóng vai trò tích cực nhất. Sử dụng thư viện mẫu các virus đã biết, các anti-virus nhanh chóng phát hiện sự có mặt của virus trong máy tính người dùng. Khi số virus ít, tần suất xuất hiện virus lạ còn thấp, phương pháp nhận dạng dựa trên mẫu tỏ ra khá hiệu quả. Khi số virus gia tăng, các anti-virus lâm vào tình thế bất lợi: cả thế giới chỉ có khoảng 25 công ty lớn đối đầu với 150.000 virus khác nhau. Trước tình hình này, các anti-virus tìm cách nắm quyền chủ động khi có dịch bệnh xảy ra. Kế hoạch này gồm 2 mảng chính: gia tăng tốc độ cập nhật và chủ động phát hiện mẫu bệnh lạ. Mảng thứ nhất có nhiệm vụ gia tăng đội ngũ chuyên gia cập nhật virus mới và

đây mạnh chính sách hỗ trợ khách hàng trực tuyến. Mảng thứ hai tập trung nghiên cứu các giải thuật tiên tiến nhận dạng thông minh virus mới, kịp thời ngăn chặn trước khi chúng lây lan. Mỗi anti-virus chọn một hướng nghiên cứu riêng: Symantec có Bloodhount, Sophos chọn hướng gien (genetic), McAfee nghiên cứu băm (hashing), BitDefender sử dụng heuristic... Do kết quả bài toán dự đoán luôn có sai số nên khách hàng phải chấp nhận rủi ro: thỉnh thoảng các anti-virus phát hiện nhầm virus trên dữ liệu sạch. Mặc dù khó khăn và phức tạp nhưng chiến lược này là xu hướng phát triển tất yếu của các anti-virus. Mặc dù các anti-virus đã có nhiều cố gắng nhưng cục diện cuộc chiến vẫn không hề thay đổi. Trong suốt 20 năm tồn tại và phát triển, virus không hề (và cũng không cần) thay đổi kịch bản tấn công: đó là lợi dụng sự sơ hở (các lổ hổng bảo mật của hệ thống, sự ngây thơ cả tin, hiếu kỳ của người dùng) để thực hiện ý đồ lây nhiễm phá hoại. Có 2 nhân tố đáng lưu ý: hệ thống (gồm hệ điều hành và các ứng dụng) và người dùng máy tính. Thực tế cho thấy các hệ thống chặt chẽ thường ít bị virus tấn công. Những hệ hoạt động chắp vá (fix, patch) luôn là mảnh đất màu mỡ cho virus máy tính phát triển. Cứ mỗi lần hệ thống được củng cố, một vài loại virus lui về hậu trường, và tình hình an ninh tạm lắng dịu một thời gian. Không bao lâu dịch bệnh lại bùng lên với các loại virus mới thâm hiểm hơn. Vì vậy an ninh mạng và bảo mật luôn là vấn đề ưu tiên hàng đầu của Microsoft trong kế hoạch phát triển dòng hệ điều hành 64-bit tương lai. Người dùng là yếu tố quyết định sự tồn vong của các công ty hoạt động trong lĩnh vực công nghệ thông tin. Người dùng lựa chọn và chi tiền cho các sản phẩm tin học có chất lượng, nhờ vậy các công ty mới có thể tiếp tục tồn tại để sản xuất các sản phẩm tốt hơn. Tuy nhiên do chênh lệch về thu nhập của từng quốc gia, do khác biệt về tâm lý tiêu dùng, do chính sách giá cả chưa phù hợp và hàng nhiều lý do khác... nên không phải người dùng nào cũng chịu móc hầu bao. Tình trạng sử dụng phần mềm lậu ở nhiều quốc gia trên thế giới không những gây thiệt hại cho các hãng sản xuất mà còn tiếp tay cho các hoạt động phi pháp phát triển. Lướt qua một vòng các trang web đen của các nhóm hacker, người ta có thể tìm thấy vô số các công cụ bẻ khóa phần mềm, các trang hướng dẫn thâm nhập mạng trái phép, nhúng trojan vào trang web, thậm chí dạy cách tạo virus với thư viện chương trình nguồn vô cùng phong phú. Quan sát bức tranh toàn cảnh 20 năm của virus thế giới, chúng ta không khỏi băn khoăn. Xã hội phát triển, công nghệ thông tin lớn mạnh kéo theo sự gia tăng hoạt động trong thế giới ngầm của các hacker. Ngày nay không ai dám bảo đảm an toàn tuyệt đối về bất cứ hệ thống nào, kể cả những hệ thống từng mệnh danh là "bất khả xâm phạm". Nếu không thì tại sao các hệ thống mạng tiên tiến nhất của các quốc gia có trình độ kỹ thuật phát triển cao như Mỹ, Châu Âu và Hàn Quốc, vẫn bị hacker tấn công? Xã hội càng phát triển, các mối quan hệ của con người cũng phức tạp hơn. Nếu như trong thế kỷ 20, các cuộc chiến tranh thế giới chỉ nhằm giải quyết xung đột của 2 thế lực, thì ở thế kỷ 21 con người phải gánh chịu nhiều tai ương hơn: chiến tranh sắc tộc, xung đột tôn giáo, bạo loạn, khủng bố... Bản thân các lực lượng đối lập cũng có sự phân hóa sâu sắc. Trong thế giới công nghệ thông tin cũng vậy, cuộc chiến bảo mật ngày nay không đơn thuần là cuộc chiến giữa virus máy tính và các anti-virus mà còn là sự đối đầu căng thẳng giữa các nhóm hacker. Sự kiện không quân Mỹ bắn nhầm vào đại sứ quán của Trung Quốc ở Nam Tư đã châm ngòi cho cuộc chiến khốc liệt giữa các nhóm hacker ở nhiều quốc gia trên mạng Internet. Sau vụ 11/9, kết quả điều tra của các cơ quan an ninh Mỹ phát hiện các nhóm khủng bố đã từng liên lạc với nhau bằng Internet. Có giả thuyết cho rằng họ đã sử dụng virus máy tính đánh cắp thông tin tình báo từ nhiều nguồn khác nhau để chuẩn bị cho cuộc tấn công. Một số hacker còn sử dụng danh xưng Bin Laden đặt tên cho virus phát thông điệp cảnh báo thế giới! Các nhà quân sự dự kiến các cuộc chiến tương lai không tách rời sự tấn công vào mạng máy tính của đối phương, làm tê liệt hệ thống thông tin liên lạc và điều

khiển khí tài quân sự của địch quân. Đây không phải là chuyện viễn tưởng vì chẳng phải Internet từng khởi nguồn từ mạng quân sự của quân đội Mỹ hay sao? Như vậy câu giải đáp cho nhân tố con người thuộc về vấn đề nhận thức. Nếu nói như thế, hẳn các bạn sẽ phải thốt lên: "Vấn đề virus máy tính rốt cuộc lại quay về bài toán xã hội?". Thật vậy, khi nào con người chịu từ bỏ những tham vọng xấu xa thì tội phạm sẽ giảm, xã hội sẽ bình ổn và an toàn hơn. Đó là cũng là một hình ảnh xã hội lý tưởng mà con người ao ước xây dựng từ hàng ngàn năm nay. Mỗi nhà nước đều dựa trên một học thuyết triết học nhất định. Mỗi học thuyết có cách giải quyết các mối mâu thuẫn trong đời sống xã hội loài người khác nhau. Nhưng tất cả đều mong muốn xây dựng xã hội ổn định và phát triển bền vững. Vấn đề còn lại chỉ là thời gian. Chúng ta có thể tin vào tương lai về một xã hội vắng bóng tin tặc. Điều này hoàn toàn có cơ sở khi vài năm trở lại đây trong hàng ngũ hacker Việt Nam đã có sự chuyển biến quan trọng. Thay vì viết virus chọc phá thiên hạ, các hacker Việt Nam đã đầu quân vào các công ty tin học tên tuổi, hoặc chuyển sang nghiên cứu bảo mật. Đây là một dấu hiệu hết sức tốt lành cho Internet Việt Nam trong bối cảnh hacker thế giới liên tục tấn công đánh phá các hệ thống trong nước. Sự kiện hacker Việt Nam tham gia làm sáng tỏ vụ iCMS trong năm 2005 cũng là một hình ảnh thu nhỏ của thế giới công nghệ thông tin an toàn. Qua sự kiện này, một số hacker đã từ bỏ thế giới ngầm bước ra ánh sáng, cất tiếng yêu cầu trả lại sự công bằng cho cuộc chơi. Lời kết Hai mươi năm qua nhân loại đã chứng kiến nhiều sự kiện trọng đại, có cả thành tựu lẫn mất mát. Thế giới có vẻ mong manh hơn, rủi ro nhiều hơn. Virus máy tính cũng hung tợn hiểm độc hơn. Nếu như nhân loại phải hàng ngày đối phó với khủng bố, bạo loạn và thiên tai, thì người dùng máy tính phải thường xuyên cảnh giác với đủ loại hình tấn công, quấy rối của các tệ nạn nhan nhản trên mạng máy tính và các thiết bị di động. Tương lai của virus máy tính đi về đâu? Hiển nhiên là chúng sẽ song hành cùng với sự phát triển của xã hội loài người. Virus máy tính là sản phẩm của con người, là hiện thân tội lỗi của con người. Khi nào con người gột sạch tội lỗi thì virus sẽ không còn lý do gì để tồn tại.

AN TOÀN THÔNG TIN 2006 CÓ GÌ MỚI ?

Đầu năm 2006, hội nghị quốc tế thường niên về an toàn thông tin (ATTT) do IBC - thành viên của Hiệp Hội Kiểm Tra và Kiểm Toán Hệ Thống Thông Tin (Information Systems Audit and Control Association) - tổ chức đã diễn ra tại Bangkok (Thai Land). Ông Vũ Quốc Thành, giám đốc công ty Misoft, người Việt Nam đầu tiên tham dự hội nghị này, cho biết: Hội nghị ATTT 2006 dự báo về những nguy cơ chính trong năm nay. Đó là: 1. Bom thư và thư độc hại (liên quan đến thư điện tử) 2. Phần mềm gián điệp 3. Tấn công kiểu phishing và pharming 4. Tin tặc tấn công những người dùng Google 5. Nguy cơ khi sử dụng các ứng dụng ngang hàng 6. Nguy cơ của mạng cục bộ không dây 7. Bom tin nhanh (spam IM) 8. Tấn công của virus và sâu máy tính 9. Nguy cơ của thiết bị di động. Nhiều diễn giả nhấn mạnh vào hai loại hình tấn công đặc biệt nguy hiểm là Botnet và Zero-day-attack. Botnet là một mạng lưới nhiều máy tính bị nhiễm "bot" (rút gọn của từ robot), là đoạn mã có khả năng giấu mình trong máy tính và thực hiện các lệnh từ xa. Đôi khi, sau lây nhiễm

nó nằm yên trong hệ thống vài năm chờ thời cơ hoạt động, do đó rất khó bị phát hiện. Tấn công "ngày số 0" (Zero-day-attack) chỉ các tấn công có thể xuất hiện ngay cùng ngày công bố điểm yếu mới (thường cùng với bản vá tương ứng nhưng cũng có khi không kịp). Khả năng thành công của các tấn công này rất cao vì kể cả khi bản vá mới được công bố nhưng không phải ai cũng kịp "vá" ngay trong ngày đầu tiên. Một thống kê cho thấy: trong 6 tháng cuối năm 2005, kể từ khi có điểm yếu mới thì trong 6 ngày là "kẻ gian" nghiên cứu ra mã tấn công, còn các nhà sản xuất phải sau 54 ngày mới cho ra bản vá. Về mặt dịch vụ ATTT, người ta nói đến xu hướng thuê ngoài dịch vụ quản lý an ninh mạng, nhất là các tổ chức có yêu cầu đảm bảo an ninh mạng cao và đòi hỏi phản ứng nhanh (như các tổ chức tài chính ngân hàng và chính phủ). P.V thực hiện

Trương Minh Nhật Quang