HACKER KINH TẾ HOẠT ĐỘNG NHƯ THẾ NÀO?

Đó là thế giới của những cha

Đó là thế giới của những chat room, những malware và các kế hoạch phishing tinh vi. Hoạt động bên trong của chúng ra sao?

Khi TJX ra đời ngày 17 tháng 1 năm 2006, các hệ thống máy tính lưu trữ dữ liệu liên quan đến thẻ tín dụng, thẻ ghi nợ và các giao dịch mua bán bị phá hoại. Người ta nói rằng chúng đã bị hack từ tháng mười hai. Các nhân viên bảo mật ở Visa ghi nhận hoạt động lừa đảo chiếm đoạt thẻ tín dụng, thẻ nợ liên quan đến thuộc tính TJX ngày càng tăng, như ở các cửa hàng T.J. Maxx, Marshalls, HomeGoods từ giữa tháng mười một. Có nghĩa là bạn hoàn toàn có thể trộm dữ liệu người dùng trôi nổi trên Internet để bán cho thị trường đen qua website và chat room, ít nhất trong hai tháng hoặc hơn.

Hacking bây giờ không còn là trò chơi của trẻ con. Nó đã trở thành hình thức kinh doanh lớn. Các thị trường đen trực tuyến sôi động với dữ liệu thẻ tín dụng ăn trộm, mã số bằng lái xe. Và malware, chương trình cho phép hacker khai thác điểm yếu bảo mật trên phần mềm thương mại là công cụ hết sức đắc lực của giới tin tặc. Hoạt động khủng bố trở nên có tổ chức cao. Chúng dùng các hệ thống thanh toán mạng ngang hàng như mua bán trên eBay mà không sợ bị phát hiện khi làm việc với nhau.

Hacker độc lập vẫn còn, nhưng Cục điều tra liên bang Mỹ FBI nhận thấy hoạt động tội phạm có tổ chức là một phần trong cộng đồng hacking, nhất là ở Trung Đông. “Hacker luôn sẵn sàng bẻ khóa máy tính, thu thập dữ liệu cá nhân và bán chúng đi nhằm kiếm lợi”, Chris Stangl – thanh tra tội phạm khủng bố của FBI, đơn vị đứng thứ ba sau bộ phận Chống khủng bố và Tình báo nói.

Vẽ ra được bức tranh toàn cảnh về tin tặc kinh tế không phải dễ dàng. Đó là thế giới ngầm sôi động nhưng không phải ai cũng nắm bắt được hết chúng. Từ các nguồn bên trong và bên ngoài “lượm lặt” được, bạn chỉ có thể phác thảo được phần nào về thế giới này.

Phương thức trực tiếp

“Bây giờ không còn là thời hacker tấn công để chỉ ra lỗ hổng trên Net. Chúng tạo các malware tinh vi vào mục đích thương mại và lợi nhuận”, Maffret của eEye.

Một số hacker sử dụng phương thức trực tiếp theo kiểu tấn công đòi tiền chuộc. Kẻ tội phạm xâm nhập vào máy tính của công ty bằng malware và mã hóa dữ liệu trong các máy tính. Tiếp theo chúng đưa ra yêu cầu công ty phải nộp tiền chuộc mới có được khóa giải mã. Hình thức này rất phổ biến ở Nga. Uriel Maimon, chuyên gia nghiên cứu bộ phận khách hàng của RSA, hãng bảo mật hiện thuộc sở hữu của EMC nói rằng, anh thấy nhan nhản các kiểu tấn công như thế trong 5 tháng qua.

Nhưng tấn công trực tiếp không phải là hình thức phổ biến nhất, vì chúng khá mạo hiểm. Trực tiếp, tức là “có sự kết nối tài chính thẳng giữa nạn nhân và tác giả hay người sở hữu malware” - David Dagon, chuyên gia nghiên cứu ở Trung tâm Bảo mật thông tin Georgia Tech phân tích. Hình thức phổ biến hơn là thị trường dữ liệu đen. Website trực tuyến nhan nhản trên Internet, là nơi diễn ra các hoạt động mua bán nhộn nhịp mã số thẻ ghi nợ, thẻ tín dụng, tên chủ thẻ, giá trị kiểm chứng thẻ, mã ba hoặc bốn con số dùng để xác nhận thẻ…. Jeff Moss, quản lý “The Dark Tangent” và đồng thời là sáng lập viên của Black Hat, hãng nghiên cứu đào tạo bảo mật (sở hữu bởi cha đẻ của Informationweek CMP) nói rằng anh biết có một tổ chức khủng bố ở châu Âu mỗi năm kiếm được nửa triệu đô la từ việc mua bán cơ sở dữ liệu và danh sách tên khách hàng.

Thông tin trên thẻ tín dụng hầu hết được bán ra với số lượng lớn. Khi mua, chắc chắn bạn sẽ không muốn có từng cái riêng lẻ mà phải là một tập hợp, một lô, một nhóm. Bởi vì bất kỳ ai cũng có thể hủy bỏ hoặc tham gia vào số tiền bồi thường gian lận. Mặc dù một số website có đưa ra danh sách giá cả, nhưng thông tin trên thẻ cơ bản được bán ít nhất ở mức 1 đôla/thẻ, tùy thuộc vào chất lượng dữ liệu.

Những kẻ trộm thẻ tín dụng tự gọi mình là “carder” và thường thả phần mềm độc hại của chúng qua chat room trên IRC, diễn đàn công cộng hay diễn đàn riêng với những cái tên như CardersMarket hay Carder.info, thậm chí cả các website mua bán điện tử trông rất bình thường, vô hại. Hacker hay carder lão luyện thường gắn liền với các IRC riêng, được mã hóa và có mật khẩu bảo vệ.

Diễn đàn có tên CardingWorld.cc với hơn 100 000 bài viết từ 13 nghìn thành viên đăng ký, hầu hết đến từ Nga. Còn khu vực nói tiếng Anh trên website luôn đề cập đến Ngân hàng quốc gia Mỹ (Bank of America), Ngân hàng Fidelity Bank, PayPal, thông tin thẻ tín dụng đến từ khắp nơi trên thế giới, các thẻ quà hợp lệ và dịch vụ chuyển vận an toàn với số lượng tiền lớn. Hầu hết người mua kẻ bán trên diễn đàn đều yêu cầu các giao dịch, đề nghị diễn ra trên message riêng tư trong hệ thống bảng tin hay tin nhắn tức thời ICQ.

Hay như website Dumps International, cung cấp thẻ tín dụng, trang bị để mã hóa và sử dụng thẻ

tín dụng cũng như mã số bảo mật xã hội (Social Security number), ngày tháng năm sinh, tên thời con gái của mẹ, mã số PIN ngân hàng, các bản vá lỗi của "kết xuất" thẻ với mã số thẻ, tên chủ thẻ, ngày tháng hết hạn. Giá cả phải trả cho một mã số thẻ có thể lên tới 40 đô la/một thẻ tiêu chuẩn và 120 đô la/một thẻ "có chữ ký". Nếu mua theo lô 100 thẻ giá có thể hạ xuống còn 30 đô la/thẻ.

Thời gian tồn tại trung bình cho các website này là khoảng 6 tháng trước khi chúng bị định hướng lại trong proxy server mới và có sự can thiệp của pháp luật. TalkCash.net, website hoạt động cho tới mùa hè năm ngoái còn cung cấp một danh sách các "ripper", những người tham gia vào thương trường nhưng không đáng tin cậy, và các hãng "kiểm chứng", những người chứng minh rằng họ có thể phân phối hàng hóa theo cam đoan.

Một số tổ chức khủng bố sử dụng các hệ thống thanh toán ngang hàng như PayPal, E-gold để giao dịch bằng vàng và chuyển trở lại thành tiền mặt tại từng quốc gia. Một số khác dùng Western Union để tạo các thanh toán. E-gold nói rằng "không có kiểu bỏ qua" cho bất cứ người nào sử dụng dịch vụ của hãng vào mục đích tội phạm. Còn giám đốc bảo mật thông tin của PayPal, Michael Barrett cho biết hãng thường xuyên làm việc với tổ chức pháp luật khi có bất kỳ dấu hiệu nào chỉ ra rằng có hoạt động tội phạm xuất hiện.

Hoạt động chuyển tiền thường rất nguy hiểm vì hacker luôn rình rập tìm cách chiếm đoạt. Nếu số lượng tiền lớn, từ hơn 10 000 đô la trở lên, nên thông báo cho ngân hàng biết để theo dõi. Các giao dịch lớn có thể bị hacker tách nhỏ ra như khi khách hàng thanh toán tiền mua tivi plasma, xâm phạm số lượng lớn tài khoản iTunes, thông tin thẩm định World of Warcraft và có thậm chí xâm nhập cả vào các router.

Buôn bán Malware

Một hàng hóa có giá trị khác trong thế giới hacker kinh tế chính là các malware như virus, worm, Trojan. Chúng cung cấp cho tin tặc đường vào để truy nhập các hệ thống doanh nghiệp.

"Hacker hy vọng doanh nghiệp sẽ phải chuộc lại dữ liệu của họ" (Kaminsky) .

Một báo cáo gần đây của Internet Security Systems (sở hữu bởi IBM từ năm ngoái), cảnh báo hiện tượng nổi lên của ngành công nghiệp "dịch vụ khai thác lỗ hổng" với các mạng sản xuất và phân

phối tinh vi tương tự như kênh sản phẩm hợp pháp của ngành công nghiệp máy tính. "Các nhà cung cấp quản lý lỗ hổng thường mua đoạn mã bị lỗi từ thị trường đen, mã hóa nó để chống xâm phạm hay sao chép bất hợp pháp, bán nó cho những kẻ phát tán thư rác hàng đầu".

Với bất kỳ nền kinh tế thị trường nào, hàng hóa có giá trị cao nhất sẽ điều khiển mức giá cao nhất. Hồi tháng mười hai, một lỗ hổng tìm thấy trong hệ điều hành mới Vista của Microsoft được tìm thấy và bán trên diễn đàn Web Romanian với giá 50 000 đô la. Raimund Genes, giám đốc công nghệ của hãng bảo mật Trend Micro đoan chắc rằng ngành công nghiệp malware kiểm soát hơn 26 tỷ đô la của hãng bảo mật hợp pháp năm 2005.

Mức tiền khổng lồ đó hấp dẫn một số lượng tội phạm tương đương. Lỗ hổng ze-ro day được phát hiện năm ngoái và bán ra với giá từ 20 000 đến 30 000 đô la. Zero-day là lỗ hổng nguy hiểm, luôn tạo ra biến thể mới nâng cao ngay khi được phát hiện, và trước khi các hãng sản xuất có thể vá sản phẩm của họ.

Mặc dù đã cảnh báo về sự nguy hiểm của ze-ro day và nhiều lỗ hổng bảo mật khác cho các công ty và khách hàng của họ, nhưng rất ít tổ chức pháp luật có thể ngăn chặn được một người nào đó viết ra chương trình khai thác các lỗ hổng này. Bạn không thể cáo buộc ai đó phạm tội khi "chỉ ra lỗ hổng chưa được vá trên Internet" - Marc Maiffret, sáng lập viên đồng thời là giám đốc phụ trách bộ phận hacking của eEye Digital Security nói.

Phishing leo thang

Phishing cũng đang trở thành hoạt động kinh doanh ngầm đắt hàng. Spammer thường lùng kiếm địa chỉ e-mail trên Web để bán cho hacker. Còn hacker dựa vào đó để tìm kiếm lỗ hổng bảo mật có thể khai thác được, tạo ra các website phishing và nói cho những kẻ phát tán thư rác nơi gửi e-mail phishing. Trong khi đó, carder mua thông tin ăn cắp được từ hacker, tạo thẻ tín dụng giả, thẻ ghi nợ giả để trộm tiền hoặc bán cho nhiều loại tội phạm khác. Tất nhiên một hoạt động khủng bố có thể thực hiện được nhiều việc khác.

Anti-Phishing Working Group, nhóm liên hiệp của các tổ chức cộng đồng và tư nhân cho rằng công cụ những kẻ lừa đảo phishing sử dụng bây giờ ngày càng tinh vi. Báo cáo tháng mười hai của nhóm này ghi nhận có hơn 340 biến thể mới của keylogger (phần mềm ăn cắp thông tin trên bàn phím) và Trojan hours được phisher sử dụng chỉ trong một tháng. Con số ngày tăng bởi "việc dùng các công cụ tự động tạo và kiểm tra các biến thể mới tốt hơn", báo cáo viết.

Có khả năng, các công cụ đó được sinh sôi từ Đông Âu với chương trình phishing và cơ chế phát tán thư rác tự động. Những kẻ tạo ra chúng hầu hết đều còn rất trẻ, chỉ trong lứa tuổi 20. Một số được đào tạo và giáo dục chính thống, nhưng số khác thì không. Một số sống ở những đất nước như Romania, nơi băng thông Internet tại các hộ gia đình nhiều hơn một số công ty ở Mỹ. Chúng trưởng thành trên Internet từ hơn 10 năm trước và luật pháp ở đó ít nghiêm ngặt hơn những nơi như Mỹ.

Kỹ thuật tinh vi không chỉ là công cụ trợ lực duy nhất cho thương mại phishing. Thật khó tin, nhưng

những kẻ lừa đảo Nigeria "419" vẫn tiếp tục công việc của chúng một cách thành công với nhiều người dùng cả tin qua e-mail. Các e-mail đó thường bắt đầu với câu "I need your help" (Tôi cần giúp đỡ) và mô tả hoàn cảnh khiến chúng cần lượng lớn tiền để cứu giúp ai đó và chuyển tới một nước nào đó. Khoản tiền đó được gọi là "phí nâng cao" vì có thể chúng yêu cầu nạn nhân gửi tiền giúp chúng giải phóng tài khoản kếch sù nào đó với lời hứa sẽ bồi thường gấp đôi hay một khoản lời lớn. Con số 419 chính là mã tội phạm Negerian đã từng một thời gây sốt và làm mưa làm gió với các vụ lừa đảo nổi tiếng.

Tháng trước, cựu thủ quỹ Alcona County của Michigan bị bắt giữ và buộc phải thanh toán 1,2 triệu đô la anh ta đã "thụt két" và ít nhất cũng gửi một số tới kẻ lừa đảo e-mail Nigeria khét tiếng. Hội đồng thương mại Liên bang Mỹ đã phải đưa ra cảnh báo này trên website của mình: "Nếu bạn nhận được e-mail nào đó nói rằng cần sự giúp đỡ với một khoản tiền ở ngoài Nigeria hay bất kỳ nước nào khác, hãy gửi nó tới Hội đồng thương mại (FTC) tại địa chỉ spam@uce.gov".

"Pump and Dump" - Moi tin và trục lợi

Ngày 25 tháng một, Hội đồng Trao đổi và Bảo mật Mỹ (Securities and Exchange Commission) đã tóm một cậu trai 21 tuổi ở Florida khi cậu này phá hủy hàng loạt tài khoản môi giới trực tuyến, sau đó phải loại bỏ rất nhiều danh mục của mình. Các nhà đầu tư nói rằng Aleksey Kamardin của Tampa, trong khoảng thời gian 5 tuần hè năm ngoái đã kiếm được hơn 82 000 đô la khi dùng quỹ các tài khoản bị xâm hại ở Charles Schwab, E-Trade, JPMorgan Chase, TD Ameritrade và nhiều tổ chức môi giới trực tuyến khác để nhẹ nhàng mua cổ phần của các công ty thương mại. Các cuộc mua bán này tạo ra cơn sốt ảo cho hoạt động thương mại hợp pháp, làm tăng giá cổ phiếu. Sau đó, Kamardin bán ra cổ phiếu anh ta mua trước với giá cao và khiến thị trường cổ phiếu sụt giảm.

Đó là bình mới của rượu cũ của "pum and dump", một hình thức lừa đảo cổ phiếu dựa trên việc moi tin bí mật. Kẻ trộm sẽ đầu tư vào cổ phiếu giá rẻ, sử dụng các tài khoản trên Cayman Island hoặc một nơi xa đất liền nào đó có thể thiết lập ẩn danh thông tin tài khoản. Khi kẻ trộm mua hoặc đánh cắp thông tin nhân dạng, hắn ta sẽ thiết lập tài khoản giả mạo, hoặc thâm nhập tài khoản của người khác (như trong trường hợp của Kamardin) và mua số lượng lớn cổ phiếu rẻ tiền, nắm giữ điều khiển giá.

Điều này tạo ra tình thế nhạy cảm cho hãng cung cấp dịch vụ tài chính. "Họ không muốn ngăn cản hoạt động kinh doanh của mọi người. Vì thế, việc tạo ra các tài khoản lừa đảo này trở thành một phần mạo hiểm trong hoạt động kinh doanh của các hãng này" - Marc Gaffan, giám đốc marketing của bộ phận giải pháp người tiêu dùng ở RSA khẳng định. Cũng như thế, thật khó có thể xem xét kỹ lưỡng trình tự kinh doanh vì chúng bị ảnh hưởng mạnh bởi thời gian. Sự chậm trễ khiến các nhà đầu tư bị thiệt hại về tiền của và ngại ngần bỏ vốn tiếp vào công ty đó. Năm ngoái, E-Trade đã gặp phải tình huống khó xử tương tự khi một máy tính bị tấn công, mở cửa cho những kẻ khủng bố chạy pump-and-dump trên E-Trade client, dẫn đến hoạt động lừa đảo góp phần vào tổn thất 18 triệu đô la theo báo cáo trong quý ba.

Phải làm gì trước thực trạng này?

New York Electronic Crimes Task Force của Secret Service đã tiến hành cuộc khám xét lớn nhất trong năm 2002 khi khẳng định cựu nhân viên quản trị cơ sở dữ liệu của hãng bảo hiểm Prudential Insurance, Donald McNeese ăn trộm thông tin nhân dạng, lừa đảo thẻ tín dụng và rửa tiền. McNeese đã lấy cắp các bản ghi trên một cơ sở dữ liệu của Prudential chứa thông tin của 60 000 nhân viên. Khi anh ta cố gắng bán thông tin này qua Web, Bill Moylan, cựu thanh tra của Cục cảnh sát Nassau County ở Long Island vốn thực hiện các nhiệm vụ bí mật đã phát hiện và liên lạc với anh ta. McNeese gửi cho Moylan khoảng 20 thông tin nhân dạng của nhân viên và khuyên anh ta nên dùng nó để tạo các thẻ tín dụng giả, một phần được gửi tới nhà của McNeese tại Florida. McNeese cuối cùng bị xử 3 năm tù treo và buộc bối thường 3 000 đô la.

Secret Service là tổ chức liên bang của Mỹ, chịu trách nhiệm điều tra âm mưu khủng bố và hacker kinh tế. Năm 2004, tổ chức này phát hiện một nhóm hacker sử dụng website Shadowcrew.com cho mục đích bất hợp pháp. Sáu năm sau đó chúng bị đưa ra tòa án liên bang và buộc phải thuê luật sư biện hộ cho tội ăn cắp thẻ tín dụng, mã số ngân hàng và thông tin nhân dạng. Tháng ba năm ngoái Secret Service công bố bắt 7 trong tổng số 21 kẻ tình nghi ba tháng theo chương trình Operation Rolling Stone, chương trình điều tra ăn trộm nhân dạng và lừa đảo trực tuyến "qua các diễn đàn tội phạm Web".

Cho dù vậy, hacker kinh tế vẫn không chùn tay. Tại Hội nghị bảo mật RSA diễn ra ở San Francisco tuần trước, chủ tịch RSA Art Coviello nói rằng thị trường nhân dạng ăn trộm đã lên tới một tỷ đô la và malware tăng theo cấp số 10 trong 5 năm.

"Vấn đề cơ bản là chúng ta có các tổ chức thực thi pháp luật trên phương diện địa lý, nhưng không có yếu tố địa lý nào ở Internet" - Dan Kaminsky, chuyên gia nghiên cứu bảo mật của DoxPara Research nói. Và: "Chúng ta không thể nghe trộm điện thoại xuyên đại dương hay đột kích bất ngờ nhà của ai đó ở Romania mà không có sự hợp tác của địa phương. Chúng ta chỉ đủ tài năng và nhân sự trong phạm vi trong nước mà thôi".

Kết quả là việc thi hành luật pháp phải dựa trên sự hợp tác chặt chẽ của nhiều khu vực riêng như các cơ quan tài chính, hãng cung cấp dịch vụ Internet và các công ty viễn thông. Có rất nhiều tội phạm vốn hoạt động trong các tổ chức pháp luật địa phương khắp cả nước. Nhiều trong số chúng đã truy cập vào FBI InfraGard, hệ thống chia sẻ thông tin giữa FBI và các khu vực riêng. InfraGard trở thành chi nhánh của FBI trong lĩnh vực trí tuệ từ năm 1996 nhằm hỗ trợ cho các chuyên gia IT và giới học viện, phục vụ cho các cuộc điều tra liên quan đến khủng bố của FBI.

Các hãng hoạt động trong lĩnh vực công nghệ thông tin cũng phải chịu một phần trách nhiệm về việc mở cửa cho thị trường trực tuyến "ngầm" với các mã độc hại và dữ liệu bị trộm cắp khi phát hành phần mềm có các lỗ hổng bảo mật. Tổ chức ISS của IBM ghi nhận có tổng số 7247 lỗ hổng phần mềm trong năm 2006, tăng gần 40% so với năm 2005. Trong đó, lỗ hổng xuất phát từ Microsoft, Oracle và Apple là lớn nhất.

Doanh nghiệp và người dùng cuối phải sát cánh cùng nhau với một số trách nhiệm hay sự bảo mật lỏng lẻo, có khi đơn giản là việc lưu trữ quá nhiều dữ liệu. Trong trường hợp của TJX, nguyên

nhân là do việc lưu trữ dữ liệu thẻ tín dụng ngược lại với quy định của Vista. “Hệ điều hành sẽ cho rằng sai khi mọi người bỏ dữ liệu đi”.

Các công ty cần cung cấp cẩn thận dữ liệu dữ liệu họ đang quản lý và đánh giá thực tế khả năng bảo vệ nó. Nếu không, có thể họ sẽ được thấy các dữ liệu này trên một website của thị trường đen.