# ĐÁNH GIÁ THỰC TRẠNG CỦA TỘI PHẠM CÔNG NGHỆ CAO TRONG AN NINH PHI TRUYỀN THỐNG

Ngày nay, internet đã và đang trở thành một công cụ không thể thiếu đối với các cơ quan, tổ chức và cả với người sử dụng các dịch vụ. Tuy nhiên, số lượng khổng lồ các dữ liệu có giá trị được truyền nhận trên mạng thông tin toàn cầu cũng đang trở thành đích hướng tới cho các băng nhóm tội phạm mạng lợi dụng hoạt động. Cùng với sự bùng nổ công nghệ cao không chỉ ở Việt Nam mà trên toàn thế giới, đã làm cho tội phạm công nghệ cao ngày càng gia tăng về số lượng và tinh vi trong phương thức thực hiện.

Đối tượng để loại tội phạm này xâm hại là hệ thống mạng thông tin nội bộ, mạng quốc gia, kể cả mạng thông tin của các cơ quan an ninh, quốc phòng, các cơ sở dữ liệu về tài chính, ngân hàng, giao thông, năng lượng, thông tin liên lạc, hệ thống thương mại điện tử, hệ thống kinh doanh điện tử, các hệ thống tự động hóa bán hàng, thanh toán (ATM)... Hiện nay đang hình thành ngày càng rõ nét hơn sự phối hợp của bọn tội phạm trong nước và quốc tế tấn công vào các mạng máy tính. Tình trạng tấn công, từ chối dịch vụ các trang web của những đơn vị, doanh nghiệp, đặc biệt là những doanh nghiệp kinh doanh thương mại điện tử diễn ra rất phổ biến gây tắc nghẽn giao dịch, thiệt hại rất lớn cho doanh nghiệp.

### *1. Thực trạng tội phạm công nghệ cao ở một số nước trên thế giới*

Hiện nay, tội phạm công nghệ cao ở các nước trên thế giới trở nên hết sức phổ biến, với các thủ đoạn chính là: tấn công máy tính, mạng máy tính; lợi dụng lỗ hổng bảo mật web, tấn công truy cập, lấy cắp, phá hoại dữ liệu (hacking of PCs and networks); phát tán virus, phần mềm gián điệp (các loại trojan, worms, malware...); tấn công từ chối dịch vụ (denial of service attacks - botnet).

Hoạt động của tội phạm có mục đích chiếm đoạt tài sản có thể phân loại thành: tội phạm gian lận thẻ ngân hàng (credit card fraud), phổ biến là sử dụng botnet với một số trojan như Spyey, Zeus, Flame, Gauss...; tội phạm lừa đảo (online fraud), sử dụng thủ đoạn kinh doanh đa cấp (đầu tư, kinh doanh dịch vụ đa cấp (vụ MB24, vicongdongviet..), kinh doanh sàn vàng, ngoại tệ ảo; lừa đảo trong thương mại điện tử C2C, B2C, B2B; lừa đảo bằng email, nick chat, tin nhắn SMS - mass marketing fraud; gửi email, tin nhắn lừa đảo để lấy cắp account và password của email, nick chat... để lừa đảo, yêu cầu chuyển tiền, thẻ

cào. Nguy hiểm hơn, tội phạm công nghệ cao còn thực hiện tấn công hệ thống cơ sở hạ tầng thông tin, truyền thông quốc gia, gây ảnh hưởng đến an ninh, hòa bình thế giới.

***a. Tội phạm công nghệ cao ở Mỹ***

Nước Mỹ với nền kinh tế lớn mạnh nhất thế giới, GDP năm 2012 là 15.643 tỷ USD; GDP năm 2022 (dự báo) là 23.496 tỷ USD. Mỹ là quốc gia xếp hạng nhất trên thế giới trong bảng xếp hạng 10 nền kinh tế mạnh nhất thế giới kể từ năm 2000 và có thể giữ vững thứ hạng này trong 10 năm tới. Vì thế đây là địa điểm lý tưởng, mảnh đất màu mỡ cho bọn tội phạm công nghệ cao hoạt động. Ngày nay, với sự phát triển nhanh chóng của máy tính, mạng máy tính và những tiện ích của nó mang lại tạo thuận lợi cho việc điều khiển công việc từ xa. Vì thế, bọn tội phạm đã lợi dụng những điều kiện thuận tiện này để thực hiện các vụ án gây thiệt hại kinh tế nghiêm trọng.

Hiện nay, tình hình tội phạm công nghệ cao ở Mỹ rất phức tạp, với những mánh khóe khôn lường. Một số phương pháp tấn công phổ biến mà tội phạm mạng thường dùng là: phát tán virus, phần mềm gián điệp, keylogger, điều khiển từ xa, worm, spam... lên mạng. Phương thức phát tán chủ yếu qua spam email, websex, forum như Twitter, Facebook, YouTube và trên những phần mềm cài đặt phổ biến như Unikey, Windows, Adobe... Chúng làm lây lan mã độc vào máy người dùng để lấy thông tin cá nhân như password của email, nick chat.

Đánh cắp đồng tiền ảo Bitcoin (BTC) phát hiện loại mã độcmới: Ra đời năm 2009, tiền ảo BTC hiện được sử dụng trong các giao dịch mua bán rất nhiều hàng hóa và dịch vụ trên thế giới. BTC hoạt động không thông qua bất kỳ một ngân hàng trung ương nào mà qua ví điện tử hoặc một trang web. Vì vậy, các giao dịch của BTC không phải chịu những loại phí giao dịch trung gian. Tỷ giá hiện tại của đồng tiền này là 636 USD/1 BTC. Tuy nhiên, kể từ khi ra mắt đến nay, giá trị của đồng tiền này thiếu tính ổn định. Tháng 9 năm ngoái, tỷ giá của BTC chỉ vào khoảng 150 USD/1 BTC, song đã từng vượt mốc 1.000 USD/1 BTC hồi cuối tháng 12 năm ngoái. Ước tính hiện có khoảng 12 tỷ BTC lưu hành trên thị trường.

Công ty an ninh Trustwave công bố ngày 24-02-2014 sau vụ trộm BTC lớn trên khu chợ trực tuyến nhiều tai tiếng Silk Road, một nhóm các tin tặc đã lợi dụng hàng trăm nghìn máy tính bị nhiễm mã độc để đánh cắp các đồng Bitcoin

và hàng chục đồng tiền ảo khác từ người dùng. Các chuyên gia an ninh của Trustwave đã phát hiện các bằng chứng cho thấy bọn tội phạm mạng đã cài đặt mẫu mã độc mới có tên "Pony" vào hàng nghìn máy tính để kiểm soát máy chủ và đánh cắp khoảng 85 "chiếc ví ảo" của chủ sở hữu, đồng thời lấy đi ít nhất 350 BTC cùng với 27 loại tiền ảo khác. Cũng theo thống kê của Trustwave, trong khoảng thời gian từ tháng 9-2013 đến giữa tháng 01-2014, các mạng lưới máy tính bị nhiễm virus "Pony" này cũng đã giúp bọn tin tặc đánh cắp các thông tin cá nhân của 600.000 tài khoản đăng ký trên mạng và 100.000 tài khoản thư điện tử cùng với các dữ liệu tài khoản bảo mật khác. Theo Trustwave, lý do bọn tội phạm chủ yếu nhằm vào đồng tiền BTC vì đồng tiền ảo này dễ dàng bị đánh cắp và quy đổi sang đồng tiền khác, thậm chí là USD, so với việc thực hiện cướp ngân hàng. Các chuyên gia an ninh cũngcảnh báo tin tặc sở hữu BTC có thể sử dụng các trang giao dịch buôn bán để lấy tiền mặt trong khi danh tính không bị phát hiện.

Trước đó, ngày 11-02-2014, sàn giao dịch BTC lớn nhất thế giới BitStamp đã buộc phải yêu cầu các nhà đầu tư tạm ngừng rút tiền do bị tin tặc tấn công với chiêu thức đưa mã độc vào hệ thống của sàn, dẫn tới tình trạng dịch vụ bị từ chối. Mới đây nhất, chợ đen trực tuyến Silk Road cũng bị tin tặc "ghé thăm" và đánh cắp khoảng 4.400 BTC từ người dùng, tương đương với khoảng - 2,7 triệu USD.

Nguy cơ lộ thông tin cá nhân từ mạng xã hội: Nhiều cuộc điều tra gần đây cho thấy các trang thông tin điện tử và mạng xã hội đang làm lộ thông tin cá nhân của người dùng, kể cả những người đặt profile của họ hoàn toàn ở chế độ cá nhân. Nếu như các thông tin cá nhân bị lộ thì người dùng sẽ phải đối mặt với rất nhiều nguy cơ, ví dụ như các phần mềm virus, mã độc, hoặc đối mặt với nguy cơ tin tặc tấn công vào mạng máy tính ăn cắp thông tin khách hàng để lừa đảo. Theo đánh giá của Tổ chức Hình sự thế giới, mỗi năm tội phạm mạng gây thiệt hại khoảng 400 tỷ USD, và cứ 14 giây lại có một vụ án liên quan đến tội phạm sử dụng công nghệ cao. Điều này cho thấy mức độ lan tỏa nhanh chóng của loại tội phạm này.

Những vụ lừa đảo trên internet nhằm lấy cắp mật khẩu, thông tin cá nhân, thẻ tín dụng ngân hàng... số vụ việc do hacker gây ra thời gian qua ngày càng tăng về số vụ, tính chất và hậu quả cũng ngày càng nghiêm trọng hơn. Việc các thành viên của các nhóm hacker phổ biến và dạy nhau cách tạo, lan truyền virus,

đánh cắp mật khẩu, phổ biến các kỹ thuật hack... diễn ra công khai hên mạng internet. Nhiều địa chi mua hàng, dữ liệu về thẻ tín dụng, tàikhoản thanh toán Paypal, rửa tiền, các phần mềm dùng để phá mã, cách cài đặt để lấy cắp mật khẩu, thông tin cá nhân, thẻ tín dụng ngân hàng... đều được chia sẻ trên các trang web. Hầu hết các hoạt động này đều nhằm vào việc ăn cắp tiền từ các thẻ tín dụng, tài khoản cá nhân, máy rút tiền tự động ATM, mua hàng trực luyến, rửa tiền... Đặc biệt, bọn tội phạm tìm cách đột nhập vào hệ thống quản lý dữ liệu của ngân hàng, bệnh viện, trường học, siêu thị để lấy cắp thông tin dữ liệu làm thẻ giả (siêu thị Mỹ và một số nước phương Tây có hệ thống dữ liệu khách hàng khổng lồ, lưu trữ thẻ tín dụng cũng như các thông tin liên quan khách hàng nhằm phác họa chiến dịch tiếp thị). Mỹ là một quốc gia có nền văn hóa thẻ tín dụng lâu đời, thẻ tín dụng là đại diện một cá nhân nên nếu bị phát hiện gian trá, chủ thẻ có thể không xin được việc làm, không lấy được hộ chiếu (passport) hoặc thậm chí không được mua nhà. Trong khi đó, sự gian trá do bọn tội phạm gây ra đối với chủ thẻ thì chủ thè lại không hề hay biết. Hơn nữa, bàng kỹ thuật đánh cắp thông tin cá nhân từ các ngân hàng dữ liệu, bọn tội phạm có thể mạo danh thực hiện rút tài khoản. Trong thực tế, chi cần một chút sơ suất, tin tặc có thể lấy được hàng triệu thông tin dữ liệu cá nhân, đặc biệt dữ liệu liên quan đến tài chính. Các hacker dùng thủ đoạn tạo website giả của các ngân hàng uy tín, yêu cầu khách hàng khai báo thông tin cá nhân và số thẻ tín dụng, mã số cá nhân. Sau đó các đối tượng này sẽ dùng những thông tin đó để lấy tiền, thay đổi tên truy cập và mật mã rồi chiếm đoạt cơ sở dữ liệu thông tin, kết quả sản xuất kinh doanh của các doanh nghiệp...

Một trong những loại hình tội phạm công nghệ cao phổ biến nhất và gây nhiều thiệt hại nhất là đột nhập mạng máy tính để đánh cắp mật khẩu và dữ liệu thẻ tín dụng của khách hàng. Tháng 6-2012, mạng xã hội nghề nghiệp Linkedin có hơn 150 triệu người trên khắp thế giới đăng ký sử dụng và dịch vụ hẹn hò trực tuyến eHarmony đã bị tin tặc đột nhập đánh cắp 65 triệu mật khẩu, có 30.000 mật khẩu đã bị bẻ khóa và 1,5 triệu mật khẩu của eHarmony đã bị tung lên mạng. Tháng 12-2012, website của Ngân hàng Mỹ Wells Fargo đã bị tin tặc đột nhập phong tỏa, gây thiệt hại cho 70 triệu khách hàng. Hàng loạt ngân hàng khác như Bank of America, J.P.Morgan, U.S.Bank, PNC Financial Services... cũng bị tin tặc tấn công. Tháng 01-2012, website Zappos.com bị tin tặc đánh cắp số thẻ tín dụng, thông tin cá nhân, hóa đơn và địa chỉ nhận hàng của 24 triệu

khách hàng. Và không thể không kể đến một vụ việc người phụ trách thu ngân của chi nhánh Park Avenue thuộc Ngân hàng Tiết kiệm Union Dime ở New York đà lấy được hơn 1,5 triệu USD từ hàng trăm tài khoản trong suốt 3 năm. Đây là vụ án nghiêm trọng nhất kể từ năm 1970.

Tấn công các website: Thời gian qua cũng đã xảy ra hiện tượng hacker tấn công các website, chiếm đoạt quyền sử dụng tên miền (domain) rồi yêu cầu chủ sở hữu phải trả một khoản tiền lớn để chuộc lại. Theo thông tin từ Văn phòng Interpol Việt Nam, trong năm 2004, hàng tháng các vụ tấn công qua mạng đã gây thiệt hại hơn 80 tỷ USD cho các doanh nghiệp trên toàn thế giới. Còn theo nhóm nghiên cứu Computer Economics của Mỹ, riêng loại tội phạm trộm cắp trực tuyến trong năm 2004 đã gây thiệt hại tới 17,5 tỷ USD cho các doanh nghiệp trên toàn cầu (tăng 30% so với năm 2003). Theo báo cáo của Viện Bảo an máy tính Mỹ (Computer Security Institute) thì thiệt hại do các loại hình tấn công qua mạng trên 700 công ty của Mỹ trong năm 2005 đã gây ra tổn thất hơn 130 triệu USD. Bộ Tư pháp Hoa Kỳ đã khẳng định, tội phạm trực tuyến là một trong những thách thức lớn nhất đối với các hoạt động tội phạm hiện nay, trong khi đó cứ 700 tên tội phạm trực tuyến tại Mỹ thì mới có 1 tên bị bắt. Theo số liệu do Quốc hội Mỹ công bố năm 2005: Việc đánh cắp thông tin cá nhân làm thiệt hại 53 tỷ USD mỗi năm cho nền kinh tế Mỹ nói chung và làm mất khoảng 5 tỷ USD/năm cho những người sử dụng thẻ tín dụng nói riêng. Theo nghiên cứu của hãng dịch vụ trực tuyến VeriSign, trong thời gian từ cuối năm 2005 đến đầu năm 2006, việc sử dụng internet vẫn tiếp tục tăng nhanh, trong khi số vụ gian lận và lừa đảo qua mạng thông tin toàn cầu cũng đã tăng gấp đôi. Đứng sau Mỹ về số vụ lừa đảo trực tuyến còn có Anh, Ôxtrâylia, Nigiêria...

Thư rác (spam), virus, phishing, phần mềm gián điệp (spyware), trojan, key-logging... cũng khiến các nhà quản lý mạng dữ liệu và công nghệ thông tin đang phải ra sức chống đỡ. Những vụ mất cắp hoặc thất lạc dữ liệu mật tại các tổ chức tài chính đã trở thành những bản tin chính trong vài năm gần đây. Một trường hợp điển hình trong năm 2005, những tên tội phạm đã truy cập và lấy cắp 676.000 tài khoản của 4 ngân hàng ở New Jersey, Mỹ. Đây được coi là vụ việc nghiêm trọng nhất trong lịch sử ngành ngân hàng Mỹ. Quy mô của các vụ tấn công mã khách hàng đã gia tăng một cách nghiêm trọng, khi những tác giả viết các chương trình virus tung ra nhiều phiên bản của các chương trình virus cùng một lúc để tăng sự nguy hiểm. Chỉ trong 3 tháng cuối năm 2004, số lượng virus

đã tăng gần 3 lần so với quý III năm 2004. Theo thống kê từ Trung tâm điều phối cứu hộ khẩn cấp các sự cố máy tính CERT (Computer Emegency Response Team), tổng số vụ tấn công trên mạng ngày càng tăng, mặt khác các kỹ thuật ngày càng mới.

Nguy hiểm hơn là bọn tội phạm còn xâm nhập vào các cơ quan của Chính phủ, đánh cắp các thông tin cơ mật, gây ảnh hưởng nghiêm trọng đến vấn đề an ninh quốc gia.

Ngày 22-01-2014, chính quyền Rumani đã bắt giữ một người đàn ông bị tình nghi là hacker "Guccifer" khét tiếng, từng thâm nhập hòm thư điện tử của nhiều nhân vật nổi tiếng trong giới chính trị và giải trí. Từ tháng 02-2012, Guccifer trở nên nổi tiếng sau khi thâm nhập được vào hòm thư điện tử của gia đình Tổng thống Bush và cho đăng lên mạng những bức ảnh cá nhân của cựu Tổng thống G.W.Bush. Nhiều nhân vật nổi tiếng khác như cựu Tư lệnh Không quân Mỹ George Roche, các thành viên gia đình Rockerfeller hay một số quan chức trong chính quyền Tổng thống Obama cũng là nạn nhân của Guccifer. Theo tài liệu của cảnh sát, Guccifer cũng đã nhiều lần truy nhập bất hợp pháp các tài khoản thư điện tử cá nhân ở Rumani với mục đích lấy trộm dữ liệu mật.

Bang California của Mỹ - nền kinh tế lớn thứ tám thế giới - đang trở thành mục tiêu số một của các tổ chức tội phạm quốc tế "đóng đô" tại Đông Âu, châu Phi và Trung Quốc. Ngoài hình thức phạm tội truyền thống như buôn bán ma túy, buôn lậu súng và buôn người, các tổ chức tội phạm tại California giờ đây hướng tới hình thức phạm tội công nghệ cao nhằm vào những người giàu có, các hãng lớn và tổ chức tài chính của bang. Mục đích của tội phạm mạng là phá "tường lửa" để đánh cắp dữ liệu, gây thiệt hại nghiêm trọng cho các nạn nhân. Khu vực Los Angeles là nơi đặc biệt dễ bị tấn công vì đặc thù hoạt động trong lĩnh vực truyền thông và điện ảnh. California hiện đang dẫn dầu các bangtại Mỹ về số lượng hệ thống máy tính bị tin tặc tấn công hoặc lây nhiễm phần mềm độc hại; số nạn nhân của tin tặc và các thiệt hại vật chất. Điều đáng nói là những hoạt động này lại do các tổ chức tội phạm quốc tế giật dây. Theo thống kê sơ bộ, hàng trăm triệu USD của các doanh nghiệp và các cá nhân tại bang này đã bị các tổ chức tội phạm quốc tế điều hành từ Rumani, Ai Cập, Ixraen, Nga, Ucraina, Trung Quốc, Nigiêria... đánh cắp. Ngoài ra, California cũng là thiên đường "rửa tiền" mới của tội phạm quốc tế. Tổng sản phẩm quốc nội của bang này là khoảng 2.000 tỷ USD, hoạt động ngoại thương tích cực và đường biên giới dài

với Mexico là những yếu tố thuận lợi mà các tổ chức tội phạm hướng tới. Báo cáo của Bộ Tư pháp bang cho biết, mỗi năm có khoảng 30 tỷ USD "tiền bẩn" đã được hợp thức hóa dưới hình thức đầu tư vào các hoạt động hợp pháp hoặc "hô biến" dưới dạng tiền ảo như đồng Bitcoin. Số lượng "tiền bẩn" mà các lực lượng an ninh tịch thu được đã tăng mạnh và California đang dẫn đầu nước Mỹ trong hoạt động chống loại hình tội phạm này.

Theo các chuyên gia quốc phòng Mỹ, các cuộc tấn công mạng là mối đe dọa nghiêm trọng nhất mà nước Mỹ đang phải đối mặt hiện nay, thậm chí nghiêm trọng hơn so với khủng bố. Kết quả thăm dò trong giới hoạch định chính sách an ninh quốc gia, quân sự, quan chức quốc hội và công nghiệp quốc phòng được công bố trên ấn phẩm đặc biệt mang tên *Defense News*số ra ngày 06-01-2014 cho thấy gần một nửa trong số các nhà lãnh đạo an ninh quốc gia Mỹ (45,1%) xác định chiến tranh mạng đang trở thành mối đe dọa chủ yếu đối với đất nước. Đảm bảo an ninh mạng luôn là một trong những vấn đề được chính quyền của Tổng thống Mỹ Barack Obama ưu tiên hàng đầu.

***b. Tội phạm công nghệ cao ở Đức***

Cơ quan an ninh thông tin của Đức ngày 21-01-2014 cho biết tin tặc đã bẻ khóa 16 triệu hộp thư điện tử của công dân Đức gây thiệt hại cho 1/5 dân số đất nước. Theo nhà chức trách Đức bọn tội phạm đã tạo ra phần mềm độc hại đặc biệt phát tán ranhiều máy tính nhằm ăn cắp mật khẩu và dữ liệu từ hộp thư điện tử. Sau khi có thông tin trên, người dân Đức đã đổ xô đi kiểm tra lại độ an toàn hộp thư điện tử của mình, khiến cho trang webdùng để kiểm tra tài khoản có bị tấn công hay không đã không thể hoạt động do quá tải số lượng truy cập.

***c. Tội phạm công nghệ cao ở Xingapo***

Tại Xingapo, mỗi năm có tới hàng chục vụ tấn công, đột nhập vào các mạng máy tính của Chính phủ cũng như của các tổ chức thương mại, gây thiệt hại đáng kể. Theo thông báo của cảnh sát, rất ít trong số các vụ tấn công bị phát hiện kịp thời, và mỗi năm chỉ có khoảng 7-10 đối tượng bị phát hiện, bắt giữ.

***d. Tội phạm công nghệ cao ở các nước châu Phi***

Vào năm 2014, khi các thiết bị điện thoại di động được tăng lên ở châu Phi thì mối đe dọa đến an ninh mạng ở nước này đến từ các thiết bị di động. Biểu đồ về sự phát hiển to lớn từ năm này sang năm khác của internet ở châu Phi đã biến lĩnh vực này trở thành mục tiêu ưu tiên của tội phạm tin học. Trong một phân

tích tháng 12-2013, Yogi Chandiramani và Tim Stah, hai nhà nghiên cứu tại FireEye, một công ty Mỹ chuyên về bảo mật website, giải thích: "Các phần mềm độc hại di động sẽ làm tăng sự phức tạp về quang cảnh của các mối đe dọa". Họ bổ sung thêm: "Vì tội phạm tin học xuất hiện ở những nơi nào có sự nhấp chuột, chúng ta sẽ thấy các cuộc tấn công nhằm vào các thiết bị này phát triển như thế nào. Theo trang web Digital Maghreb, trên thực tế, người ta đã thống kê có hơn 100.000 cuộc tấn công trên toàn thế giới trong năm 2012 nhằm vào công nghệ Android, số liệu từ WB cho thấy số lượng thẻ thông minh cho điện thoại di động được bán ra ở châu Phi đã bùng nổ từ 16,5 triệu năm 2000 lên hơn 735 triệu vào cuối năm 2012. Hơn nữa, theo Hiệp hội các nhà khai thác GSM (mạng thông tin di động với công nghệ GSM) trên toàn thế giới, trong năm 2011, châu Phi đã trở thành lục địa hàng đầu về thanh toán qua điện thoại di động với 80% các giao dịch được thống kê. Theo một nghiên cứu của Pew Center Researsh, Kênia với 68% người dùng đã thông báo sử dụng công nghệ này để gửi hoặc nhận tiền trong năm 2013. Adiel Akplogan, Giám đốc điều hành Afrinic - một tổ chức phi chính phủ chịu trách nhiệm đăng ký địa chỉ IP cho châu Phi, dự đoán: "Người ta lo ngại rằng có những phương pháp mới của tội phạm tin học" .

Nguyên nhân dẫn đến tình trạng này là do khung pháp lý chưa phù hợp: Một số quốc gia đã tiến hành các biện pháp chống tội phạm tin học như Bờ Biển Ngà, Nigiêria, Kênia và Nam Phi. Tuy nhiên ở nhiều nước, việc này vẫn chưa có trong chương trình nghị sự. Adiel Akplogan, Giám đốc điều hành Afrinic - một tổ chức phi chính phủ chịu trách nhiệm đăng ký địa chỉ IP cho châu Phi nhận định: "Vấn đề ở chỗ là các nước chúng ta đã có quá nhiều vấn đề kinh tế và trong các ưu tiên xem xét, tội phạm tin học vẫn được xem tương đối nhẹ". Đặc biệt, trên toàn châu lục, các sáng kiến vẫn bị tách rời nhau. Ngoài một cam kết cụ thể hóa việc thống nhất pháp luật tại ECOWAS, do Nigiêria và Bờ Biển Ngà đưa ra trong năm 2009, Liên minh châu Phi muốn có thời gian để hiểu đượcmột đề nghị về tội phạm tin học, dựa theo Công ước Budapest để tham khảo trong lĩnh vực này. Kể từ đó, dự án vẫn nằm nguyên trên giấy. Trong khi đó, theo cảnh sát Bờ Biển Ngà từ năm 2012-2013, nước này đã mất khoảng 6 tỷ franc CFA. Một cuộc điều tra của tờ nhật báo *East African,*xuất bản năm 2013, ngành ngân hang Kênia đã bị bốc hơi 17,5 triệu USD trong năm 2012 do các hành vi của tội phạm tin học. Tuy nhiên, điều này mới chỉ là sự khởi đầu với những cải tiến việc kết nối, triển khai cáp quang và khuôn khổ pháp lý chưa phù hợp, tội

phạm tin học có thể tìm thấy ở châu Phi một thiên đường sinh lợi cho các hoạt động của chúng.

Hợp tác cảnh sát gần như bị đình trệ: Ngoài yếu kém về pháp lý, châu Phi cũng đã có những nỗ lực trong lĩnh vực hợp tác cảnh sát, khi tội phạm tin học rõ ràng là xuyên biên giỏi Stephane Konan, người chịu trách nhiệm chính trong cuộc chiến chống tội phạm tin học của Bờ Biển Ngà cho rằng: Điều cần thiết là cảnh sát châu lục cần có những trao đổi thông tin về nhận dạng thủ phạm tin học. Angiê (thủ đô của Angiêri) cũng đã tổ chức hội nghị các giám đốc và tổng thanh tra công an châu Phi.

Trong chương trình nghị sự, bên cạnh những vấn đề khác có hợp tác chống tội phạm mạng. Tuy nhiên, các cuộc họp giữa các cơ quan cảnh sát của châu Phi rất hiếm, ngoại trừ các sáng kiến của Interpol, FBI hay Liên hợp quốc.

***đ. Tội phạm công nghệ cao ở Canada***

Heartbleed tấn công hệ thống máy tính Thuế vụ Canada: Cơ quan Thuế vụ Canada đã bị các tin tặc sử dụng con bọ điện toán Heartbleed tấn công dữ liệu thông tin cá nhân của khoảng 900 khách hàng. Con bọ Heartbleed là một lỗ hổng an ninh nghiêm trọng trong thư viện OpenSSL, một phần mềm được 2/3 website trên thế giới sử dụng để bảo mật thông tin. Các tin tặc sử dụng Heartbleed để lấy các thông tin cá nhân như số thẻ bảo hiểm xã hội, thường được dùng cho việc tuyển dụng hoặc nhận các khoản trợ cấp của Chính phủ. Con bọ Heartbleed cho phép tin tặc đánh cắp thông tin mà không để lại dấu vết nào. Cơ quan thuế bị tấn công nên phải đóng cửa dịch vụ trực tuyến trong ngày 09-4-2014, thời điểm "nóng" trong hoạt động thu thuế định kỳ hàng năm, làm chậm công tác thu thuế tại nước này gây thiệt hại lớn.

Các nhà nghiên cứu cũng thừa nhận mặc dù Heartbleed tồn tại trong OpenSSL đã vài năm, song họ không xác định được thủ phạm đã sử dụng con bọ này để tiến hành các vụ tấn công vào hệ thống bảo mật. Một chuyên gia an ninh mạng cảnh báo thậm chí cả những tin tặc không phải là những người thành thạo trong lĩnh vực công nghệ thông tin cũng có thể sử dụng Heartbleed để thực hiện các vụ đánh cắp thông tin nhằm vào những tài khoản có độ bảo mật thấp vì Heartbleed được công khai trên internet. Các chuyên gia an ninh mạng không loại trừ nguy cơ xảy ra những vụ tấn công mới theo hình thức này trong tương lai và khuyến cáo người dùng mã hóa các dữ liệu dễ bị tấn công.

***e. Tội phạm công nghệ cao ở Trung Quốc*** Trung Quốc đóng cửa, chặn 19.000 trang web "đen": Trong một chiến dịch truy quét kéo dài từ tháng 12-2009 đến nay, các cơ quan chức năng Trung Quốc đã đóng cửa và ngăn chặn khoảng 19.000 trang web "đen" có nội dung đồi trụy hoặc hình ảnh khiêu dâm. Trong số này, có 15.500 trang web "đen" sử dụng giao thức không dây (WAP) phục vụ các thuê bao điện thoại di động. Các cơquan chức năng Trung Quốc cũng đã nhận được hơn 159.000 nguồn tin do người dân báo về các trường hợp phát tán tin bài, hình ảnh đồi trụy trên mạng, vi phạm quy định của Chính phủ.

Trung Quốc hiện là nước đứng đầu thế giới về số người sử dụng internet. Tính tới cuối tháng 6-2014, tại Trung Quốc có 420 triệu người đã đăng ký sử dụng internet, 277 triệu người dùng điện thoại di động có khả năng truy cập internet. Đây là thiên đường tiềm năng cho loại hình tội phạm này phát triển.

***2. Thực trạng tội phạm công nghệ cao ở Việt Nam***

Việt Nam đang trong quá trình phát triển hệ thống công nghộ cao nên cũng không tránh khỏi những làn sóng tấn công trên internet. Lực lượng cảnh sát Việt Nam đã phối hợp với cảnh sát quốc tế phát hiện một số vụ việc các đối tượng người Việt sử dụng tài khoản lấy cắp được mua tên miền ở nước ngoài để sử dụng và bán cho những người có nhu cầu lập trang web riêng, các vụ trộm cắp cước viễn thông, sử dụng thẻ giả rút tiền tại các ngân hàng của Việt Nam, các vụ tấn công DDOS... Việc những đối tượng thanh thiếu niên có kiến thức về tin học ở Việt Nam sử dụng tài khoản bị đánh cắp để thực hiện những giao dịch bất hợp pháp hiện đang diễn ra rất phức tạp. Trên nhiều diễn đàn (forum) bất hợp pháp thường cung cấp những tài khoản (account) đã bị hacker đánh cắp và một bộ phận giới trẻ thường sử dụng những tài khoản này để vào các website đồi trụy yêu cầu phải trả tiền khi đăng nhập Tình trạng phát tán virus, sử dụng virus tấn công qua mạng internet ở Việt Nam cũng rất nghiêm trọng, như: virus tình yêu, virus mật mã đỏ, virus Ninda... (Điển hình như vụ Bùi Hải Nam và Bùi Hải Long là hai anh em ruột viết phần mềm virus tin học cótên Xrobot để tung lên mạng ngày 09-4-2006 đã bị các trinh sát Phòng 9/C15 phát hiện, lập hồ sơ chuyển cho Thanh tra Bộ Bưu chính Viễn thông xử phạt hành chính 10 triệu đồng).

Theo số liệu từ Trung tâm VNCERT Việt Nam, số lượng virus mới được phát hiện tại Việt Nam ngày càng nhiều: năm 2005 là 232, tỷ lệ máy tính bị

nhiễm là 94%; năm 2006 có 880 virus mới, 93% máy tính bị nhiễm. Riêng năm 2007 là 6.752 virus mới, với 96% máy tính bị nhiễm, số virus xuất hiện trung bình 18,5 virus mới/ngày; đã có trên 33,6 triệu lượt máy tính bị nhiễm virus, trong đó virus lây lan nhiều nhất trong năm là W32. Winib.Worm làm 511.000 máy tính lây nhiễm. Không những tán phát virus, nhiều đối tượng còn sử dụng kiến thức tin học để đột nhập trái phép vào mạng nội bộ, website thương mại điện tử của nhiều cơ quan tổ chức, doanh nghiệp,... gây ảnh hưởng xấu đến hoạt động thương mại điện tử đang bước đầu hình thành và phát triển ở Việt Nam, như vụ 156 trang web của Công ty điện toán và truyền số liệu VDC bị tấn công hàng loạt vào cuối năm 2001 hay các vụ tấn công của hacker khiến hàng loạt các trang web của Công ty FPT, hệ thống máy chủ của Công ty Nhân Hòa, VMS Mobifone, website chodientu.com... gây ngập lụt đường truyền, không thể truy nhập, sập hệ thống quản trị. Gần đây, sáng 27-7- 2008, tin tặc đã tấn công và cướp quyền điều khiển 3 tên miền của Công ty PA Vietnam, là công ty đăng ký tên miền và cung cấp dịch vụ hosting (đặt máy chủ) thuộc hàng lớn nhất Việt Nam, khiến gần 8 nghìn website Việt Nam bị tê liệt. Sau khoảng một tuần, hàng trăm website thuê dịch vụ hosting tại một số công ty bị tin tặc tấn công làm tê liệt hoặc suy yếu tốc độ xử lý. Ngay khi vụ tấn công xảy ra, quản trị mạng các website trên không thể truy cập vào để thay đổi thông tin điều khiển tên miền, không thể sử dụng email dùng tên miền chung với website, và chịu bị động để tin tặc dẫn tới bất cứ trang web nào. Theo thống kê sơ bộ, máy chủ tên miền PAVietnam.com quản lý 1.155 tên miền và máy chủ PAVietnam.net quản lý 5.456 tên miền. Các website bị ảnh hưởng do cuộc tấn công của tin tặc hiện đã được khắc phục. Tuy nhiên, thiệt hại vẫn chưa thể được thống kê thành con số cụ thể.



Đặc biệt, ngày 05-10-2008, website của Trung tâm an ninh mạng BKIS ở địa chỉ www.bkav.com.vn đã bị tấn công từ chối dịch vụ (lãnh đạo BKIS không khẳng định vụ việc này). Tuy nhiên theo diễn đàn Vietnam Sercurity, việc tấn công này bắt đầu từ khoảng 7 giờ sáng ngày 05-10 với quy mô lớn, khoảng 3.000-5.000 botnet (mạng máy tính ma). Đến 18h39’ vẫn không thổ truy cập vào trang web này. Sự việc được đánh giá là nghiêm trọng bởi BKAV được xem là trung tâm an ninh mạng hàng đầu tại Việt Nam, có ảnh hưởng đến rất nhiều khách hàng đang sử dụng chương trình chống virus BKAV.

Thống kê từ hệ thống giám sát virus của Công ty an ninh mạng Bkav cho

thấy, trong 11 tháng qua đã xuất hiện 273 triệu virus máy tính mới. Nhận định "thế giới ngày nay quá nguy hiểm", năm 2013, Bkav nhận được thông tin trợ giúp từ khắp các tổ chức, doanh nghiệp với trên 5,1 triệu email, hơn 2 triệu cuộc gọi liên quan đến virus máy tính với hàng loạt các phương thức lây nhiễm virus mới. Ví dụ tiêu biểu nhất là việc hacker còn xâm nhập vào một tài khoản email quan trọng của tổ chức, cá nhân rồi tạo tập tin quan trọng (như: danhsachtangluong.docx) rồi đính kèm mã độc trước khi gửi hàng loạt. Người nhận tải tập tin này và mờ ra sẽ lập tức bị nhiễm độc máy tính, trở thành một phần của mạng máy tính ma hoặc bị rò rỉ thông tin quan trọng... Các máy tính ở Việt Nam đang phát tán hơn 3,33 tỷ tin nhắn rác/ngày. Có ít nhất khoảng 500.000-1.000.000 máy tính đang bị lây nhiễm mã độc và nằm trong các mạng máy tính ma. Năm 2013, giới an ninh bảo mật của Việt Nam đã chứng kiến nhiều cuộc tấn công từ chối dịch vụ (DDOS) của tin tặc. Trong đó, nổi bật là đợt tấn công vào các báo điện tử VietNamNet, Dantri, Tuoitre. Nghiên cứu của Bkav cũng chỉ ra thời điểm các máy tính ma cùng truy cập cao nhất vào một tờ báo lên tới hơn 100.000 máy. Các máy này bị nhiễm độc do tải phần mềm trên không gian mạng.

Về điện thoại di động, đến tháng 11-2013, Bkav đã thống kê có tới 528.000 mẫu virus mới trên điện thoại, cao hơn rất nhiều so với 2012 là 34.000 mẫu; mỗi ngày có 17 triệu tin nhắn rác được phát tán. "Chiếc điện thoại ngày nay đang dần thay thế máy tính, lưu trữ nhiều dữ liệu quan trọng. Và nó là mục tiêu nhắm tới hiện hữu của tin tặc. Xu hướng tấn công này sẽ còn tiếp tục phát triển trong năm 2014".

Có thể nói, tính chuyên nghiệp của tội phạm mạng thể hiện ở chỗ phần lớn các hành vi phạm tội diễn ra trên môi trường mạng, chứ không chỉ đơn thuần thực hiện trực tiếp trên máy tính của người sử dụng. Chiều hướng sử dụng các chương trình hoặc mã độc đang có xu hướng gia tăng. Sâu máy tính và phần mềm gián điệp đã chiếm tới 70% phần mềm độc hại trên mạng. Tội phạm mạng đang chuyển hướng tấn công sang các doanh nghiệp nhỏ vốn yếu kém trong khâu bảo mật. Hậu quả do tội phạm mạng gây ra khá lớn. Ước tính bình quân thiệt hại do virus máy tính gây ra cho mỗi người sử dụng vào khoảng 496.000 đồng/năm. Nếu mỗi máy tính cần khoảng 2 USD để khắc phục hậu quả nhiễm virusthì với số máy tính hiện có ở Việt Nam khoảng vài triệu chiếc tính thiệt hại cũng lên tới hàng chục triệu USD.

*Các hình thức tội phạm công nghệ cao ở Việt Nam hiện nay*

- Ở Việt Nam đã phát hiện một số doanh nghiệp thuê "chuyên gia" tấn công các đối thủ kinh doanh trên mạng.

- Một số học sinh, sinh viên đã cố ý tạo, lan truyền các virus trên mạng internet gây tắc nghẽn đường truyền, lây lan virus sang hàng chục nghìn máy tính, ảnh hưởng nghiêm trọng đến hoạt động bình thường của máy tính và mạng máy tính.

- Tình trạng các trang tin điện tử, trang web đăng ký tên miền nước ngoài vi phạm các quy định về quản lý internet diễn ra rất phổ biến, gây khó khăn cho việc đăng ký, quản lý tên miền tại Việt Nam.

- Sử dụng "sim rác" để nhắn tin trên điện thoại nhằm thực hiện các hành vi lừa đảo, lan truyền tin tức "thất thiệt".

- Một số vấn đề khác, đó là Games Online đang diễn biến ngày càng phức tạp, nhất là khó quản lý việc mua bán account ảo, tài sản ảo khi tham gia trò chơi Online.

- Tạo lệnh chuyển tiền điện tử khống trong hệ thống thanh toán trực tuyến sang tài khoản "ma", tài khoản của người khác để chiếm đoạt.

- Tình trạng người nước ngoài vào Việt Nam đi du lịch sử dụng hộ chiếu giả, thẻ tín dụng giả, thẻ của người khác hoặc thông đồng với các đại lý, điểm chấp nhận thanh toán thẻ tại các khách sạn của các ngân hàng thanh toán các dịch vụ khách sạn, mua hàng, đặt tour du lịch, mua đồ trang sức, đặt vé máy bay.

- Tình trạng đột nhập trái phép vào cơ sở dữ liệu của các lĩnhvực kinh tế quan trọng như bưu chính, viễn thông, ngân hàng, các website... để lấy cắp thông tin, chiếm đoạt tên miền, tài khoản thẻ tín dụng "chùa" để mua bán, thanh toán trực tuyến ngày càng phổ biến, gây thiệt hại về kinh tế và uy tín của Việt Nam trong giao dịch điện từ và thanh toán trực tuyến.

- Một số đối tượng lợi dụng lòng tin của khách hàng để quảng cáo nhận tiền đặt cọc mua hàng trực tuyến trên mạng internet như gửi hàng không đúng chủng loại, số lượng, xuất xứ để chiếm đoạt tiền đặt trước, gây thiệt hại cho khách đặt mua hàng và hoạt động thươmg mại điện tử.

Theo Hiệp hội an toàn thông tin tại Việt Nam (VNISA), trong năm 2011, tại Việt Nam nổi lên hiện tượng tội phạm nước ngoài tới tạm trú sử dụng công nghệ cao để lừa đảo, ăn cắp thông tin, tài khoản cá nhân không chỉ tại Việt Nam

mà trên toàn thế giới. Ngoài ra, việc các tội phạm nước ngoài sử dụng thẻ tín dụng giả tại Việt Nam vẫn tiếp tục diễn ra và có chiều hướng gia tăng. Theo số liệu của Tổ chức Cảnh sát quốc tế Interpol, cứ 14 giây lại có một người là nạn nhân của loại tội phạm này.

Theo nhận định của các cơ quan chức năng, các loại tội phạm khác đang dần có xu hướng chuyển sang tội phạm sử dụng công nghệ cao, ví dụ cá độ, buôn bán ma túy, lừa đảo... diễn ra ngày một nhiều trên mạng.

Thiệt hại do loại tội phạm này gây ra rất nghiêm trọng, theo đánh giá thì người Việt thiệt hại 8.000 tỷ đồng do virus máy tính. Ngày 14-11-2013, tại Thành phố Hồ Chí Minh, Sở Thông tin và Truyền thông Thành phố Hồ Chí Minh và Chi hội An toàn thông tin phía Nam (VNISA) tổ chức hội thảo "Ngày an toàn thông tin Việt Nam 2013" với chủ đề "Thể chế hóa an toàn thông tin - con đường tất yếu của sự phát triển xã hội thông tin hiện đại", cho biết tỷ lệ đầu tư cho an toàn thông tin chỉ chiếm 0-5% trong tổng đầu tư cho công nghệ thông tin của doanh nghiệp, đây là một con số quá khiêm tốn.

Khảo sát của VNISA cho thấy, hiện có tới 38% doanh nghiệp không có cán bộ chuyên trách hoặc bán chuyên trách về an toàn thông tin, 56% doanh nghiệp không có phòng ban về an toàn thông tin, 53% doanh nghiệp chưa có kế hoạch xây dựng hệ thống bảo vệ an toàn thông tin theo chuẩn ISO 2700. Nguy hiểm hom, có tới 65% doanh nghiệp không tính đến an toàn thông tin từ khâu thiết kế và xu hướng này gia tăng so với năm ngoái. Khi có tấn công mạng xảy ra, nhiều doanh nghiệp chọn cách tự giải quyết, 48% tổ chức không báo cáo về sự cố cho cơ quan hữu quan.

Mặt khác, các biện pháp kỹ thuật bảo vệ tấn công mạng như phần mềm chống virus, tường lửa và bảo mật mạng không dây cũng không được các doanh nghiệp quan tâm. Do sự thiếu quan tâm đến an toàn thông tin này, tại Việt Nam trong năm qua có 2.405 website của các cơ quan, doanh nghiệp bị hacker xâm nhập. Thiết bị di động thông tin ngày càng là đích tấn công quan trọng và là điểm yếu lớn của hệ thống quản lý, lưu trữ và xử lý thông tin trong tương lai. Điển hình là vụ việc hai khách hàng sử dụng dịch vụ internet Banking bị đánh cắp số tiền hơn 100 triệu đồng trong tài khoản, gây hoang mang trong dư luận.

Khảo sát của Trung tâm an ninh mạng BKAV cho thấy, người Việt Nam thiệt hại gần 8.000 tỷ đồng do virus máy tính. Riêng tại khu vực phía Nam, theo

khảo sát thực tế vào tháng 10-2013 của VNISA ở 300 tổ chức, doanh nghiệp tại Thành phố Hồ Chí Minh và các vùng lân cận, hiện khả năng nhận biết bị tấn công mạng của các doanh nghiệp bị sụt giảm từ 42% năm 2011 xuống 40% năm 2012 và 26% năm nay. Theo đó, khả năng ước tính thiệt hại do tấn công cũng sụt giảm từ 45% năm 2012 xuống còn 21% năm nay. Vai trò của quy trình chuẩn phản ứng lại tấn công mạng dường như bị lu mờ, không có quy trình phản ứng lại sự cố.

Tóm lại, tội phạm công nghệ cao đang ngày càng gia tăng và hoạt động tinh vi hơn. Nó gây ra thiệt hại lớn cho nền kinh tế mỗi quốc gia nói riêng và nền kinh tế thế giới nói chung, gây nhiều tổn thất lớn; làm "tổn thương" nghiêm trọng đến mối quan hệ ngoại giao, quan hệ kinh tế giữa các nước với nhau. Đặc biệt thời gian qua, Trung Quốc luôn bị nghi ngờ đóng vai trò chủ chốt trong các cuộc tấn công trên internet. Điều này khiến Lầu Năm Góc lên tiếng cảnh báo rằng Mỹ phải cẩn thận phòng vệ trước một trận "Trân Châu Cảng kỹ thuật số". Một báo cáo tại Quốc hội Mỹ đã gán biệt danh "thế lực nguy hiểm nhất trên mạng" cho Trung Quốc. Nếu chiều hướng này tiếp tục gia tăng có thể sẽ dẫn đến nguy cơ "chiến tranh mạng".