Chết dưới tay Trung Quốc (Kỳ 12)

ĐỐI ĐẦU VỚI CON RỒNG TRUNG QUỐC – LỜI KÊU GỌI HÀNH ĐỘNG TOÀN CẦU

Peter Navarro & Greg Autry

Dịch giả: **Nhóm dịch thuật cựu học sinh AIT**

Phần III. CHÚNG TA SẼ CHÔN NGƯƠI THEO PHONG CÁCH TRUNG HOA

Chương 10 - Chết dưới tay tin tặc mũ Đỏ: Từ "Hắc khách" Thành Đô đến những con chip Mãn Châu

Gián điệp mạng là cơ hội lớn để san bằng giàu nghèo trong thông tin. Các nước không còn phải chi nhiều tỷ đô-la để phát triển những vệ tinh phủ sóng toàn cầu nhằm thu thập thông tin tình báo cao cấp khi mà họ có thể thực hiện điều đó qua mạng Internet.

- Bóng đêm trong đám mây

Trong khi mạng lưới điệp viên của Trung Quốc đang không ngừng "bòn rút" tất cả những gì được cho là bí mật mà chúng có thể lấy từ những trường đại học Mỹ, những công ty, các phòng thí nghiệm, văn phòng chính phủ mà các trinh sát của họ có thể thâm nhập vào, thì sự phát triển của đội ngũ những kẻ tin tặc cũng tạo ra mối đe dọa ngang tài ngang thậm chí còn vượt trội hơn.

Ngày nay, những đội "tin tặc mũ đỏ" nguy hiểm của Trung Quốc đã thâm nhập vào NASA, Lầu Năm góc và Ngân hàng thế giới; đã tấn công Phòng Công nghiệp và An ninh của Bộ Thương mại Mỹ dữ dội đến mức Bộ phải vứt bỏ hàng trăm máy tính bị hỏng; đã copy sạch ổ cứng của dự án Chiến đấu cơ kiêm oanh tạc cơ F-35 của hãng Lockheed Martin; và dội bom trải thảm ảo vào hệ thống điều khiển không lưu của Không lực Hoa Kỳ. Chúng cũng đã tấn công vào máy tính của các nghị sĩ có tư tưởng cải cách cũng như của Ủy ban Đối ngoại Hạ viện.

Vào thời điểm vận động tranh cử Tổng thống Mỹ năm 2008, đội ngũ tin tặc mũ Đỏ của Trung Quốc thậm chí còn xâm nhập vào máy chủ thư điện tử của chiến dịch vận động tranh cử của cả Obama lẫn McCain cũng như vào cả Nhà Trắng của Tổng thống Bush. Và trong một vụ vi phạm nghi thức ngoại giao thô bỉ nhất, các máy tính xách tay của Bộ trưởng Thương mại Mỹ và một số nhân viên đã bị đánh cắp và bị cài những phần mềm gián điệp trong một chuyến công tác về thương mại tới Bắc Kinh.

Hơn thế nữa, khi mà bộ máy gián điệp truyền thống dựa chủ yếu vào "Bẫy mật ngọt" kiểu như quý bà xinh đẹp Mara Hari để tìm kiếm những bí mật trong những lúc thủ thỉ trên giường hoặc là một mỹ nhân qua đêm để kiếm được vị trí có lợi trong thỏa hiệp nào đó thì những gián điệp mạng ảo của Trung Quốc đang sử dụng một số " Hũ mật" kỹ thuật số để ăn cắp dữ liệu từ các máy tính. Thật vậy, ngoài gái mại dâm và các phòng khách sạn gài máy nghe lén thông thường ở Thượng Hải, các gián điệp Trung Quốc ngày nay tặng những thẻ nhớ và thậm chí cả máy chụp hình kỹ thuật số có chứa virus làm quà. Theo Cục tình báo Anh MI5, khi kết nối vào các máy tính của nạn nhân, những hũ mật kỹ thuật số tàn độc này cài các phần mềm cho phép những kẻ tấn công mạng chiếm quyền điều khiển máy tính.

Trong thực tế, theo một chuyên gia tin tặc về Trung Quốc và cũng là tác giả quyển sách *Hắc khách*[10], Scott Henderson, việc trở thành Tin tặc ở Trung Quốc được vinh danh gần như "ngôi sao nhạc rock". Nó thậm chí còn là một nghề mà trong báo cáo gần đây cho biết khoảng chừng một phần ba trẻ em Trung Quốc mơ ước.

Giống như phiên bản trực tuyến của mạng gián điệp phân tán của Trung Quốc, những lực lượng đông đảo dân nghiệp dư thực hiện phần lớn các phần việc vất vả trong nỗ lực chiến tranh mạng tổng lực. Hằng ngày, hàng ngàn người được gọi là "dân quân tin tặc"[11] liên tục dò tìm, phá hoại, và ăn cắp từ các cơ quan của phương Tây cũng như là các đối thủ ở châu Á như Nhật Bản và Ấn Độ.

Để xem xét đến quy mô của mối đe dọa của chiến tranh mạng Trung Quốc, trước nhất cần nên nhận dạng mục tiêu chính của các gián điệp mạng. Việc tấn công đơn giản nhất là làm gián đoạn hoạt động của các hệ thống các nước phương Tây bằng cách phá hoại các website hoặc làm cho quá tải các máy chủ với kiểu tấn công "từ chối dịch vụ".

Một mục tiêu thứ hai rõ ràng là đánh cắp thông tin có giá trị: số thẻ tín dụng và nhận dạng cá nhân của từng cá nhân; công nghệ, tài liệu đấu thầu, tài chính của công ty, các bí mật thương mại ở các công ty; và các hệ thống vũ khí quân sự.

Vẫn còn đó mục tiêu thứ ba trong cuộc chiến trên mạng là việc phá hỏng số liệu bằng phương thức có thể gây ra tổn thất nặng nề cho khách hàng sử dụng hệ thống. Chẳng hạn như, bằng việc can thiệp hệ thống mua bán cổ phiếu hoặc trái phiếu, bọn tin tặc mũ Đỏ Trung Quốc có thể làm gián đoạn việc mua bán, thao túng các giao dịch hoặc bóp méo số liệu báo cáo và do đó kích động gây náo loạn thị trường tài chính.

Cuối cùng bọn tin tặc có thể ảnh hưởng thế giới thực bằng việc nắm quyền kiểm soát hệ thống điều khiển các tài sản hữu hình. Chẳng hạn như, một nhóm người yêu nước trên mạng có thể làm ngưng trệ lưới điện quốc gia của New England nhằm "trừng phạt" Mỹ liên quan đến những động thái tiếp đón đức Đạt Lai Lạt Ma khi đến thăm Nhà Trắng hoặc

liên quan đến việc buôn bán vũ khí cho Đài Loan.

Những vị hắc khách đến từ Bắc Kinh dưới quốc kỳ

Câu hỏi: Trong tình huống nào thì các bạn tiến hành tấn công mạng?
Trả lời: Nếu có một vấn đề mà nó ảnh hưởng đến chúng tôi trên bình diện quốc tế thì chúng tôi sẽ tập hợp lực lượng để tiến hành tấn công.

- Trích Hội thảo "An ninh thông tin, Hacker Trung Quốc nói về hacker"

Tất cả các hoạt động chính của các nhóm tin tặc mũ Đỏ Trung Quốc có điểm tương đồng là họ tiến hành khá độc lập và chỉ chịu sự giám sát lỏng lẻo của đảng Cộng sản Trung Quốc. Dĩ nhiên là đảng cộng sản duy trì một khoảng cách thích hợp sao cho họ luôn có thể đưa ra lời phủ nhận hợp lý cho những việc gây nên sự phản ứng mạnh mẽ của công chúng - đó là vụ tấn công trơ trẽn, táo bạo vào Lầu Năm Góc, tấn công chuyển luồng đường truyền Internet trong vòng 18 phút, vụ tấn công vào mã nguồn của Google và còn nhiều vụ khác nữa.

Không còn nghi nghờ gì nữa. Cái được gọi là "dân quân tin tặc" không thể tồn tại nếu không có bàn tay của Bắc Kinh. Theo Mulvenon thuộc trung tâm Nghiên cứu và Phân tích Tình báo giải thích, "Các tin tặc trẻ tuổi này được tha thứ với điều kiện là họ không được tổ chức các cuộc tấn công vào mạng nội bộ của Trung Quốc. Họ là những thằng ngốc hữu dụng cho chế độ Bắc Kinh".

"Những thằng ngốc hữu dụng", thực sự là vậy. Trong khi tại Los Angeles có các băng nhóm bị lên án là "Crips" và "Bloods", thì nhóm theo dân quân tin tặc của Trung Quốc đã tổ chức thành hàng ngàn nhóm nhỏ với tên gọi như là "Green Army Corps", "the Crab Group", và thậm chí toàn các cô gái tập hợp lại như "Six Golden Flowers". Họ làm việc chung với nhau để cải thiện kỹ năng, chia sẻ công cụ, kỹ thuật và kích động tinh thần dân tộc của nhau. Kết hợp lại, những nhóm găng-xtơ mạng này hình thành một liên minh tư tưởng vô định hình với một trên gọi khá màu mè là "Honkers".

Tại Trung Quốc có hàng trăm "trường đào tạo tin tặc" để dạy ma thuật cho những phù thủy trẻ tuổi. Hàng loạt các quảng cáo chuyên nghiệp về đào tạo nghề gián điệp mạng và các công cụ có thể tìm thấy trong những nơi công cộng, và theo như Wang Xianbing của hackerbase.com, họ "dạy cho học sinh cách thức tấn công những máy tính không được bảo vệ và ăn cắp thông tin cá nhân". Trong khi đó chính quyền Trung ương Trung Quốc cho phép các nhóm như Liên đoàn Tin tặc Trung Quốc hoạt động công khai và thậm chí duy trì văn phòng làm việc trong khi trấn lột những người ngoại quốc, miễn là Liên đoàn đó không tấn công vào các trang hoặc các phần mềm trong nước.

Để giải thích cho những người còn hoài nghi là hoạt động của hacktivist được sự bảo trợ của Chính phủ trung ương, hãy hiểu Trung Quốc là nước có hệ thống Internet được kiểm soát và giám sát chặt chẽ nhất thế giới. Thật rõ ràng là điên rồ nếu có ý kiến cho rằng một kẻ tấn công mạng tinh nghịch nào đó có thể tồn tại trong thời gian dài ở Trung Quốc mà có thể nằm ngoài tầm kiểm soát của đội quân kiểm duyệt Bắc Kinh.

Trên thực tế, khi có nhóm tin tặc vi phạm luật bất thành văn quan trọng nhất của Trung Quốc là "đừng bao giờ tấn công hệ thống của Chính phủ", chắc chắn rằng sự trừng phạt đến ngay tức khắc. Chẳng hạn như một vài thành viên trong một nhóm tin tặc khai thác một lỗ hỏng trong phần mềm kiểm duyệt của Trung Quốc có tên là Green Dam, một công cụ quan trọng được Trung Quốc sử dụng để theo dõi hành động của người sử dụng mạng Internet Trung Quốc, những người tấn công mạng đã bị bắt ngay lập tức. Tương tự, theo tờ China Daily, một tin tặc tên là So ở tỉnh Hồ Bắc đã thay thế hình ảnh của một quan chức trên website của chính phủ bằng hình một cô gái mặc bikini. Kẻ tinh nghịch này đã được xử nhẹ tội theo chuẩn mực của Trung Quốc, đó là chỉ một năm rưỡi tù giam.

Tất nhiên, chính nhờ thỉnh thoảng có vụ bắt bớ loại này đã khiến cho đội ngũ tin tặc mũ Đỏ tập trung vào chính phủ và cơ quan nước ngoài. Và những nhóm này luôn luôn có thể bị kích động thành một đám dân tộc chủ nghĩa điên cuồng với chỉ một cái nháy mắt và gật đầu từ lãnh đạo đảng Cộng sản.

Đây chỉ là một trường hợp bẽ mặt nhỏ: Khi Thủ tướng Nhật Junichiro Koizumi thăm đền tưởng niệm chiến tranh Yasukuni – nơi mà những người theo chủ nghĩa dân tộc Trung Quốc xem là đền của tội ác chiến tranh – những tin tặc Trung Quốc đã thay đổi bộ mặt của website của ngôi đền Shinto với dòng chữ, “cô gái đang đái trên toilet Yasukuni". Liên minh tin tặc Honkers sau đó tiếp tục tấn công dồn dập vào hàng chục website của chính phủ Nhật, kể cả Sở Cứu hỏa và Thiên tai và Cục các Phương tiện phòng vệ.

Bây giờ, bạn có thể tưởng tượng được phản ứng của chính phủ Trung Quốc nếu những tin tặc Nhật làm những việc tương tự đối với website Trung Quốc về Thế vận hội Olympic hoặc Bộ Quốc phòng Trung Quốc. Và không chỉ Nhật Bản phải chịu sự quấy phá định kỳ của những người đầu tàu theo chủ nghĩa dân tộc của Trung Quốc. Khi liên hoan phim hàng năm Melbourne ở Úc dám chiếu một đoạn phim tài liệu về lãnh đạo Duy Ngô Nhĩ của Trung Quốc, những kẻ tin tặc Trung Quốc đã phá hỏng hệ thống bán vé trên mạng.

Giới tin tặc hàng đầu ở Bắc Kinh tấn công cả Vua công nghệ Google

Nếu như Google, với tất cả nguồn lực và chuyên môn tin học của họ, đang lo lắng cho

việc bảo vệ tài sản mã nguồn quí giá trước sự xâm nhập của các gián điệp tin học thì các công ty Fortune 500 khác liệu có đủ tự tin để bảo vệ thông tin của mình không?

– The Christian Science Monitor

Để thấy rõ tâm địa xảo quyệt của giới tin tặc Trung Quốc, ta nên tìm hiểu qua "Chiến dịch Aurora" tai tiếng. Chúng từng thực hiện các đợt tấn công có hệ thống vào một trong những công ty tin học có mức độ kỹ thuật phức tạp nhất thế giới – Google, cùng với hơn 200 công ty khác của Mỹ, từ Adobe, Dow Chemical, DuPont cho đến Morgan Stanley, Northrup Grumman. Theo công ty an ninh mạng iDefense, các đợt xâm nhập được thực hiện từ một nhóm nước ngoài duy nhất bao gồm các gián điệp trực thuộc hoặc được sự ủy quyền của nhà nước Trung Quốc.

Trong chiến dịch Aurora, các "hắc khách" (hacker gọi theo tiếng Hoa), thiết lập các đợt tấn công tin học hết sức phức tạp. Đầu tiên, chúng tìm cách làm quen và giúp đỡ các nhân viên của công ty mục tiêu thông qua các mạng xã hội như Facebook, Twitter, hay LinkedIn. Sau một số lần chat, các điệp viên tin học Trung Quốc sẽ tìm cách dụ số nhân viên này vào các trang chia sẻ hình ảnh mà thực ra là bình phong của một tệp cài đặt phần mềm gián điệp của Trung Quốc. Khi đã sa bẫy, máy tính của các nhân viên này sẽ bị nhiễm một loại vi rút thực hiện việc lấy và chuyển tiếp tên và mật khẩu sử dụng cho các tin tặc. Sau đó bọn tin tặc Bắc Kinh sử dụng các thông tin này để thâm nhập vào kho dữ liệu to lớn của các công ty – kể cả nguồn mã giá trị của Google.

Bọn tin tặc không chỉ quan tâm đến lấy trộm mã nguồn. Theo đúng bản chất toàn trị của nhà nước Trung Quốc được mô tả trong tác phẩm của George Orwell, bọn tin tặc còn xâm nhập vào tài khoản thư điện tử Google của các nhà hoạt động nhân quyền Trung Quốc.

Đúng như dự đoán, chính phủ Trung Quốc đã phủ nhận mọi dính líu. Tuy nhiên, lần theo địa chỉ IP ta có thể dễ dàng biết được thủ phạm thực hiện là từ một trường đại học có mối quan hệ chặt chẽ với quân đội Trung Quốc. Sự việc này còn đáng chê trách hơn vì có sự đồng lõa của đảng Cộng sản Trung Quốc, mạng WikiLeaks đã đưa ra các bức điện cho thấy "các đợt tấn công vào Google được đạo diễn bởi một ủy viên Bộ Chính trị cao cấp khi vị này đã gõ tên mình lên Google và tìm thấy các bài chỉ trích chính cá nhân ông ta".

Dáng dấp của bạo lực

Ngoài Chiến dịch Aurora còn rất nhiều cuộc tấn công của Trung Quốc đã gây ra hậu quả nghiêm trọng. Điển hình như trường hợp gây chấn động của vụ Night Dragon (con rồng bóng

đêm). Đợt tấn công đã nhắm vào các công ty năng lượng lớn phương Tây và được phát hiện bởi công ty an ninh mạng McAfee.

Gọi là gây chấn động vì đây không phải như một đợt tấn công thông thường nhằm ăn cắp số thẻ tín dụng hoặc phá phách ngẫu nhiên. Chúng đã hoạch định và tiến hành một cách bài bản nhằm kiểm soát các máy tính và hộp thư điện tử của các lãnh đạo doanh nghiệp cao cấp mà đích cuối cùng là các tài liệu nội bộ về các hoạt động, thông tin tài chính và đấu thầu.

Tại sao chính phủ Trung Quốc muốn có những thông tin này? Vì chúng rất có giá trị đối với các công ty nhà nước vốn đang cạnh tranh với các đối thủ ngoại quốc trong lĩnh vực năng lượng trên phạm vi toàn cầu.

Hiểu được mục tiêu chiến lược của Night Dragon tức là hiểu được việc Trung Quốc thật sự đang tiến hành một cuộc chiến kinh tế toàn cầu. Thật ra, hiện nay không tháng nào là không có tin phanh phui vụ lấy trộm dữ liệu qui mô lớn từ Mỹ, Nhật, Đài Loan hay châu Âu được thực hiện từ Trung Quốc.

Chúng ta chỉ có thể hình dung được bao nhiêu kế hoạch xâm nhập mạng đã thực hiện nhưng không bị phát hiện và mức độ thiệt hại mà các nền kinh tế phương Tây cũng như một số nước châu Á phải gánh chịu. Tuy nhiên, thật cực kỳ khó hiểu tại sao chính phủ các nước nạn nhân như Mỹ, châu Âu, Nhật, Ấn Độ, và các nước khác lại không có những phản ứng đủ mạnh đối với cuộc chiến tin học của Trung Quốc.

Chiếm đoạt mạng Internet toàn cầu để làm điều mờ ám

Trong thời gian 18 phút vào tháng Tư, một công ty viễn thông thuộc sở hữu của nhà nước Trung Quốc đã tạo chuyển luồng chui 15% lưu lượng thông tin trên mạng internet trên toàn thế giới, bao gồm các dữ liệu từ quân đội đến các tổ chức dân sự của Mỹ và đồng minh. Việc tái phân luồng với qui mô lớn này đã ít thu hút sự chú ý của giới truyền thông chính thống do cách thức thực hiện và mức độ ảnh hưởng là chủ đề khó hiểu đối với những người không thuộc về cộng đồng an ninh mạng.

- Tạp chí National Defense

Vâng một công cụ khác trong túi đồ ảo thuật của các đội quân tin tặc đỏ của Trung Quốc được gọi là "Chiếm tuyến". Sử dụng kỹ thuật này, Trung Quốc đã trơ trẽn cho thế giới thấy họ có khả năng chiếm quyền kiểm soát một tỉ lệ lớn các phân luồng trên mạng internet toàn cầu.

Kỹ thuật chiếm tuyến cũng cho thấy sự tiếp tay của các công ty nhà nước trong các chiến dịch chiến tranh mạng của Bắc Kinh. Chẳng hạn, bằng cách cấu hình các bộ điều tuyến internet nội địa nhằm tạo quảng cáo sai cho một thao tác đi tắt của một kênh internet tiềm năng, công ty quốc doanh China Telecom đã lừa được một lượng dữ liệu khổng lồ bên ngoài Trung Quốc chuyển luồng đi qua mạng của họ. Dĩ nhiên, sau đợt tạo chuyển luồng chui 18 phút tai tiếng nhưng ít được báo chí để ý này, chính phủ Trung Quốc như thường lệ vẫn chối bay chối biến.

Báo động DNS về Trung Quốc đang chiếm tuyến

Nếu bạn ở ngoài Trung Quốc và tình cờ truy vấn tên gốc một máy chủ ở Trung Quốc, truy vấn của bạn sẽ buộc phải qua bức Vạn lý Hỏa thành, nghĩa là bạn sẽ bị kiểm duyệt như một công dân Trung Quốc vậy.

– Earl Zmijewski

Với câu nói trên, ông Zmijewski đang nói về vấn đề gì? Đó là vấn đề được gọi là thuật xử lý DNS, và cũng có nghĩa là Trung Quốc đang kiểm duyệt cả người sử dụng internet bên ngoài bức Vạn lý Hỏa thành của họ.

DNS là chữ viết tắt của "Domain Name Services – Dịch vụ tên miền", chính các bảng ghi DNS này đóng vai trò như một danh bạ điện thoại trên internet. Thuật xử lý DNS diễn ra khi dữ liệu DNS không đầy đủ được sử dụng để ngăn chặn người dùng internet ở các khu vực khác trên thế giới truy cập đến các trang web mà chính phủ Trung Quốc cho là "không thân thiện".

Để hiểu được thuật xử lý DNS nhằm kiểm duyệt cả người dùng ngoài biên giới Trung Quốc, giả sử bạn đang là một người dùng Facebook ở một quốc gia chẳng hạn như Mỹ hoặc Chile. Vào một thời điểm nào đó, bạn muốn truy cập vào Facebook nhưng không được nên bạn cho rằng đang bị nghẽn mạng, và tính sẽ thử lại sau. Đây có thể là chuyện thật sự đang diễn ra: truy vấn của bạn có thể đã bị chuyển đến một máy chủ ở Trung Quốc vốn tự xưng như một bản sao của máy chủ có DNS "gốc" đặt tại Thụy Điển. Dĩ nhiên vấn đề là cái máy chủ ở Trung Quốc này chỉ là bản sao những gì trên Internet mà giới lãnh đạo ở Bắc Kinh muốn cho bên ngoài tiếp cận đến mà thôi – đương nhiên là không có Facebook trong đó.

Thuật xử lý DNS nói trên cho thấy Trung Quốc có thể kiểm duyệt Internet ra cả bên ngoài biên giới của họ; và tình trạng sẽ chỉ tồi tệ hơn khi Trung Quốc cố đòi thêm quyền quản trị mạng internet toàn cầu.

Đây không phải là chuyện nhỏ. Do tính toàn cầu của mạng Internet, một ngày nào đó hoàn toàn có khả năng các yêu cầu về địa chỉ Internet của bạn sẽ được chuyển qua Trung Quốc. Thật ra, hàng năm có hơn một nửa mạng Internet toàn cầu truy vấn đến các máy chủ DNS ở Trung Quốc. Khả năng có thể xảy ra là việc trang web bạn cần truy cập sẽ được báo là "không tìm thấy" vì sự kiểm duyệt của chính phủ Trung Quốc chỉ có tăng lên chứ không giảm xuống. Đó là do thay vì không ngừng mở cửa Internet như Trung Quốc vẫn luôn tuyên bố, danh sách các trang web bị kiểm duyệt thực tế luôn kéo dài thêm ra.

Như một ghi nhận cuối về các mối nguy hiểm của thuật xử lý DNS của Trung Quốc, nó đã được chủ động sử dụng liên quan đến các cuộc biểu tình chống chính phủ theo sau các chuyển biến tại Ai Cập. Thật vậy, trong thời gian diễn ra các bất ổn xã hội ở Ai Cập, thuật xử lý DNS cùng các kỹ thuật khác được sử dụng để chặn trang mạng xã hội kinh doanh LinkedIn cũng như các tìm kiếm và các trang web có chứa các từ khóa "Egypt", "Jasmine", và tên của Đại sứ Mỹ tại Trung Quốc – "Huntsman".

Với một chút hài hước, chúng ta thiết tha đề nghị giới cảnh sát mạng Trung Quốc hãy đổi tên danh sách đen các trang web bị chặn thành là danh sách trắng vì số lượng bị chặn đến lúc nào đó sẽ nhiều hơn số lượng được phép truy cập!

Nạn tin tặc có phải là nghiệp chướng mà đức Đạt Lai Lạt Ma nói đến?

Sau 10 tháng điều tra về gián điệp tin học, các nhà nghiên cứu đã tìm thấy 1.295 máy tính ở 103 quốc gia có các phần mềm đánh cắp dữ liệu từ các mục tiêu quan trọng như đức Đạt Lai Lạt Ma và các cơ quan chính phủ trên toàn thế giới. Các cuộc tấn công tin học có dấu vết từ các máy tính đặt tại Trung Quốc.

- HotHardware.com

Bên cạnh việc đánh cắp các hệ thống vũ khí từ Lầu Năm Góc và các bí mật công nghiệp và quân sự từ các công ty như DuPont, Northrop Grumman, và Google, các nhóm tin tặc mũ đỏ của Trung Quốc có thể được huy động để nghiền nát các luồng tư tưởng bất đồng chính kiến bên trong hoặc bên ngoài lãnh thổ Trung Quốc. Hãy xem xét lại những gì đã xảy ra đối với các máy tính của lãnh tụ lưu vong Đạt Lai Lạt Ma và những người ủng hộ ông ta trong phong trào chống đối ở Tây Tạng. Trong cuộc tấn công này, các e-mail "lừa đảo" được gửi tới chính phủ lưu vong Tây Tạng ở Dharamsala, Ấn Độ và các văn phòng tại London và New York. Các email từ địa chỉ trông có vẻ tin cậy đã khiến người nhận không ngần ngại mở các tài liệu bị nhiễm virus Trojan có tên là "Gh0st Rat" - chuột ma.

Khi được kích hoạt, "Gh0st Rat" chiếm quyền điều khiển hệ điều hành Windows của người sử dụng, tự sao chép sang các máy tính khác và bắt đầu tìm kiếm hệ thống tài liệu và sau đó chuyển các tài liệu tới các máy chủ ở tỉnh Tứ Xuyên của Trung Quốc. Trong một số trường hợp, các phần mềm gián điệp còn ghi nhận tất cả thông tin gõ lên bàn phím và thậm chí trưng dụng các webcam và microphone để lưu giữ và chuyển nội dung các cuộc nói chuyện trong phòng đặt máy tính nhiễm virus.

Virus "Ghost Rat" nói trên còn tấn công các máy tính bị lây nhiễm đặt tại bộ ngoại giao và đại sứ quán của Hàn Quốc, Ấn Độ, Đức và khoảng 100 quốc gia khác; các chuyên gia phân tích các cuộc tấn công mạng và công việc hắc ám phía sau các diễn đàn về tin tặc của Trung Quốc có thể lần theo dấu vết tới Thành Đô và thậm chí đến tận từng cá nhân ở Đại học Khoa học và Công nghệ điện tử. Tất nhiên, chính phủ Trung Quốc không hề có bất cứ hành động nào để ngăn chặn các cuộc tấn công tin học, càng không làm gì để truy tìm các thủ phạm. Bắc Kinh cũng không có các phản ứng, ngoại trừ việc lên tiếng phủ nhận như thường thấy.

Một lần nữa, chúng ta phải đặt câu hỏi: tại sao các chính phủ của các quốc gia như Mỹ, Ấn Độ, và Nhật Bản lại kiên nhẫn chịu đựng các hoạt động chiến tranh tin học trắng trợn như vậy?

Ứng viên Mãn Châu có gắn chíp trên vai

Tin tặc ở Trung Quốc… đã thâm nhập sâu vào hệ thống thông tin của các công ty và các cơ quan chính phủ Mỹ, đánh cắp các thông tin quan trọng từ các giám đốc doanh nghiệp Mỹ trước các cuộc họp của họ ở Trung Quốc, và trong một số trường hợp đã thâm nhập vào các nhà máy điện ở Mỹ, có thể đã gây nên hai sự cố mất điện trên diện rộng xảy ra gần đây tại Florida và khu vực Đông Bắc.

- The National Journal

Hãy cân nhắc kịch bản sau: một kỹ sư Trung Quốc thiết kế một "cửa sau" điều khiển từ xa vào hệ điều hành máy tính, hoặc một "công tắc chết người" khó bị phát hiện nhúng vào chíp máy tính phức tạp được đặt hàng tại Trung Quốc. Sau đó, các chíp "Mãn Châu" đã nhúng mạch gián điệp và phần mềm "cửa sau" được Trung Quốc bí mật xuất sang Mỹ, nơi mà chúng trở thành một bộ phận trong các hệ thống khổng lồ đang được vận hành bình thường.

Trong lúc đó, như trong bộ phim *Ứng viên Mãn Châu*[12], các thiết bị Mãn Châu đó chờ đợi các tín hiệu có thể cho phép Bắc Kinh đóng mở hoặc điều khiển các hệ thống quan trọng

như lưới điện, hệ thống tầu điện ngầm đô thị, hoặc thiết bị định vị GPS.

Đừng nghĩ rằng trên đây chỉ là khoa học viễn tưởng, bởi vì việc gắn các mạch Mãn Châu rất dễ dàng – đặc biệt là tại một đất nước được coi là công xưởng của cả thế giới. Việc gắn các đoạn mã độc vào máy tính cũng dễ dàng bởi lẽ các chương trình phần mềm hiện đại có tới hàng triệu dòng lệnh. Gắn các dòng lệnh điều khiển kiểu Mãn Châu vào vi mạch của máy tính, điện thoại và iPod – kể cả các hệ thống an ninh – cũng dễ dàng không kém bởi lẽ các vi mạch có thể bao gồm hàng trăm triệu cổng logic có thể giấu một sự bất ngờ của kỹ thuật số.

Bây giờ, nếu bạn nghi ngờ rằng những sự việc đó trên thực tế có thể không bị phát hiện, chúng tôi sẽ cho bạn biết một số thông tin. Các kỹ sư phần mềm và các nhà thiết kế vi mạch thường xuyên giấu những thứ linh tinh trong sản phẩm của họ chỉ để bày tỏ sự phản đối.

Một ví dụ truyền thống là con chim cắt mà ai đó đã tạo ra và nó xuất hiện mỗi khi một chuỗi các hành động được thực hiện trong phần mềm Adobe Photoshop. Thậm chí, nhân vật chính của quyển sách *Where's Waldo?* được một tay kỹ sư tinh nghịch đưa vào với kích thước chỉ bằng 30 micro mét vào bộ vi xử lý.

Nhìn rộng hơn, việc phát hiện các bất ngờ kiểu Mãn Châu như vậy trong mã nguồn hoặc chíp máy tính nói chung không phải là một phần trong quy trình bảo đảm chất lượng được sử dụng để kiểm tra các phụ kiện từ Trung Quốc. Tất cả những gì các nhân viên kiểm tra chất lượng thực hiện – thậm chí đối với các nhân viên kiểm tra chất lượng hàng hóa quân sự – là bảo đảm các máy móc, thiết bị sẽ vận hành theo các chỉ tiêu kỹ thuật sau khi lấy ra khỏi bao bì. Theo lời giải thích của Ruby Lee, giáo sư ngành kỹ thuật điện của Đại học Princeton "không thể kiểm tra hết được những thứ không xác định nếu chúng không được đề cập tới".

Việc các tin tặc Trung Quốc có đủ khả năng cài các chíp Mãn Châu là thực sự đáng lo ngại, bởi lẽ ngày nay, phần lớn máy tính của các hãng Hewlett-Packard, Dell và Apple được sản xuất tại Trung Quốc – thực tế, hầu hết được lắp ráp tại cùng trong một nhà máy khổng lồ tại Thâm Quyến. Hơn thế nữa, Trung Quốc là nguồn chính mà bạn tải xuống hệ điều hành Windows hoặc Mac, cùng với các chương trình phần mềm ứng dụng khác.

Một lần nữa, chúng tôi muốn nhấn mạnh rằng đó không phải là khả năng tưởng tượng bí ẩn hoặc lý thuyết gián điệp xa vời nào đó. Trong thực tế, chính nước Mỹ đã đi tiên phong trong việc sử dụng chíp Mãn Châu nhiều năm về trước trong thời gian chiến tranh Lạnh với Liên Xô. Và đây là một ví dụ lịch sử.

Theo website của CIA, Tổng thống Reagan đã đích thân thông báo cho CIA về một điệp viên hai mang quan trọng của KGB được biết dưới bí danh "Farewell", người đã tiết lộ

thông tin về cách mà Liên Xô có được các công nghệ quan trọng của phương Tây. Thay vì bịt lại chỗ rò rỉ một cách đơn giản, cố vấn chính sách Gus Weiss đã nghĩ ra một phương thức khôn ngoan, kết quả của điệp vụ đó là chíp máy tính giả được gắn vào thiết bị quân sự của Liên Xô.

Việc những con chíp máy tính được thiết kế riêng biệt có thể gây thiệt hại nghiêm trọng được minh chứng bởi vụ nổ không có tác nhân hạt nhân lớn nhất trong lịch sử. Sự cố xảy ra vào năm 1982 khi một đoạn ống ở vùng xa xôi của tuyến đường ống quan trọng dẫn khí xuyên Siberi của Liên Xô bị nổ tung. Nguyên nhân của vụ nổ được xác định, đó là phần mềm kiểm soát đường ống mà cơ quan phản gián CIA đã phá hỏng và sau đó cố tình để Liên Xô đánh cắp từ một công ty Canada. Thật là khôn ngoan?

Rõ ràng, vụ nổ đường ống xuyên Siberi do CIA sắp đặt là hậu quả nhãn tiền của "nghệ thuật đen" về quy mô sự phá hoại phần mềm đối với thế giới thật ngày càng gia tăng. Với số lượng máy tính được cấu hình như thiết bị điều khiển bán tự động ngày càng nhiều, từ thiết bị bơm truyền trong y tế đến các nhà máy điện nguyên tử, cuộc sống của con người ngày càng phụ thuộc vào chíp và phần mềm.

Thực tế, tin tặc Trung Quốc có thể đã làm mất ổn định hệ thống điện lưới quốc gia của Mỹ, không chỉ một lần mà nhiều lần. Theo tờ *National Journal*, có bằng chứng cho thấy một tin tặc Trung Quốc đã tạo điều kiện để gây ra "tình trạng mất điện lớn nhất trong lịch sử ở miền Nam nước Mỹ"; trong đó có sự cố ảnh hưởng đến khoảng 50 triệu người.

Nói rộng hơn, trích dẫn lời của một chuyên gia tình báo lâu năm của Mỹ được đăng trên tờ *The Wall Street Journal*, "người Trung Quốc đang tìm cách thâm nhập vào kết cấu hạ tầng của chúng ta, đặc biệt là lưới điện", và việc thâm nhập đã để lại các phần mềm "có thể được sử dụng để phá hủy các thành phần hạ tầng". Ông ta không nghi ngờ khi cho rằng "nếu xảy ra chiến tranh với họ, họ sẽ tìm cách khởi động các phần mềm này lên".

Quan điểm của chúng tôi, đơn giản là: các con chíp Mãn Châu là rất thực tiễn. Với hiện tượng khá nhiều công ty Mỹ đang chuyển việc sản xuất phần cứng và phần mềm – kể cả công tác nghiên cứu và phát triển – vào Trung Quốc, chúng ta có thể đã tự tạo ra việc nhập khẩu không chỉ sản phẩm Trung Quốc mà còn hàng loạt chíp Mãn Châu.

Để đánh giá các chứng cứ ngày càng gia tăng về tình trạng chiến tranh và gián điệp mạng do Trung Quốc gây ra, câu hỏi cốt yếu được đặt ra là, liệu chúng ta có nên coi các hoạt động tấn công tin học của Trung Quốc là hành động chiến tranh đúng với bản chất của chúng, hay chỉ đơn giản là khăng khăng bảo thủ và không chấp nhận các thảm họa gây ra bởi lữ đoàn tin tặc mũ Đỏ. Để cân nhắc câu trả lời, hãy đừng quên lời cảnh báo của tướng James Cartwright, nguyên là người đứng đầu Bộ tư lệnh Chiến lược Mỹ và nguyên Phó

chủ tịch của Bộ Tổng Tham mưu Liên quân. Cartwright cho rằng, tầm ảnh hưởng của những cuộc tấn công tin học được tổ chức hoàn hảo với quy mô lớn "trên thực tế có thể đã đạt tới mức độ của vũ khí hủy diệt hàng loạt".

---

10 The Dark Visitor là dịch nghĩa của chữ Hắc khách, phiên âm tiếng Hán của chữ hacker. ND

11 Hacktivist – từ chữ activist là người hoạt động tích cực. ND

12 The Manchurian Candidate (1959), của Richard Condon, là tiểu thuyết hành động chính trị về con của một gia đình chính khách nổi tiếng của Mỹ bị tẩy não để biến thành sát thủ do đảng Cộng sản kích hoạt lúc cần. ND

P.N. & G.A.

Nhóm dịch giả gửi trực tiếp cho *BVN*