NGUY CƠ ĐE DỌA AN NINH MẠNG TỪ IoT

ThS Phạm Tiến Đạt, ThS Đỗ Thị Minh Thu
Học viện Cảnh sát nhân dân

Theo dự báo, sẽ có khoảng 24 tỷ thiết bị Internet of Things (IoT) trên thế giới vào năm 2020. Tổng vốn đầu tư trong lĩnh vực IoT trong 5 năm tới sẽ đạt mức 13.000 tỷ USD. Tuy nhiên, đi kèm với sự bùng nổ của IoT vì các tiện ích của nó sẽ là những nguy cơ về bảo mật ngày càng lớn, bởi càng có nhiều kết nối được tạo ra, dữ liệu được chia sẻ càng rộng rãi thì càng có nhiều lỗ hổng bảo mật. Chính vì vậy, việc dự báo, phòng ngừa và khắc phục các lỗ hổng mạng và nâng cao nhận thức về bảo mật an ninh mạng là một trong những mối quan tâm hàng đầu của các tổ chức/cá nhân.

Sự bùng nổ của IoT

Thuật ngữ Internet vạn vật (IoT) được hiểu là một mạng lưới của các đối tượng vật lý hay "các sự vật" được nhúng với thiết bị điện tử, phần mềm, cảm biến; mỗi đối tượng này được cung cấp một định danh của riêng nó, và tất cả có khả năng truyền tải, trao đổi thông tin, dữ liệu với nhau qua một cơ sở hạ tầng mạng. Hiểu một cách đơn giản thì IoT là tất cả các thiết bị có thể kết nối với nhau. Việc kết nối có thể thực hiện qua Wi-Fi, mạng băng thông rộng (3G, 4G), Bluetooth, hồng ngoại… Các thiết bị có thể là điện thoại thông minh, máy pha cafe, máy giặt, tai nghe, bóng đèn, và nhiều thiết bị khác. Theo dự báo của Cisco, công ty hàng đầu thế giới về công nghệ thông tin và kết nối mạng, IoT sẽ là mạng khổng lồ kết nối mọi thứ, bao gồm cả con người và sẽ tồn tại các mối quan hệ người - người, người - thiết bị, thiết bị - thiết bị. Một mạng IoT có thể chứa 50 đến 100 nghìn tỷ đối tượng được kết nối và mạng lưới này có thể theo dõi sự di chuyển của từng đối tượng.

Một dự án nghiên cứu của Business Insider Intelligence chỉ ra rằng, có khoảng 24 tỷ thiết bị IoT trên thế giới vào năm 2020. Tổng

Biểu đồ tăng trưởng của IoT từ năm 2009 đến nay.

vốn đầu tư trong lĩnh vực IoT trong 5 năm tới sẽ đạt mức 13.000 tỷ USD. Các đối tượng chính sử dụng thiết bị IoT bao gồm: các chính phủ, doanh nghiệp và người tiêu dùng. Các nhóm thị trường này được dự đoán sẽ đóng góp chủ yếu cho thị trường IoT. Đến năm 2020, sẽ có khoảng 5 tỷ thiết bị IoT được người tiêu dùng cài đặt, với chi tiêu khoảng 900 triệu USD, dự báo vốn đầu tư vào thị trường này là 400 triệu USD. Đối với các chính phủ, sẽ có khoảng 7,7 tỷ thiết bị IoT được cài đặt, chi tiêu khoảng 2,1 tỷ USD và vốn đầu tư khoảng 4,7 tỷ USD. Đối với thị trường doanh nghiệp, sẽ có khoảng 11,2 tỷ thiết bị, với chi phí 3 tỷ USD và khoảng 7,6 tỷ USD cho đầu tư.

Đe dọa bảo mật đến từ hệ thống IoT

Ngày nay, khi càng nhiều kết nối được tạo ra, dữ liệu càng được chia sẻ rộng rãi thì càng trở thành mục tiêu tấn công của tội phạm mạng. Vì vậy, trong bối cảnh bùng nổ của IoT, việc dự báo, phòng ngừa và khắc phục các lỗ hổng mạng là một trong những nhiệm vụ hàng đầu của các tổ chức và cá nhân. Qua phân tích

IoT luôn là "miền đất hứa" của các hackers.

thực tế có thể chỉ ra một số vấn đề đe dọa bảo mật đến từ hệ thống IoT như sau:

Lỗ hổng bảo mật trong IoT

Theo ước tính, mỗi ngày có ít nhất 6 triệu thiết bị IoT mới xuất hiện và tham gia vào hệ thống, đồng nghĩa với việc số lượng lỗ hổng bảo mật ngày càng gia tăng trong hệ thống IoT. Điển hình tại Hội nghị về tin tặc thế giới DefCon, các nhà nghiên cứu đã tìm thấy 47 lỗ hổng bảo mật trong 23 thiết bị IoT của 21 nhà sản xuất. Theo dự án bảo mật web mở OWASP, trong năm 2019, top 10 lỗ hổng bảo mật thường gặp trên các thiết bị IoT gồm có: 1) Mật khẩu yếu, có thể đoán được hoặc mật khẩu được đặt mặc định; 2) Các dịch vụ mạng được sử dụng để truy cập các thiết bị IoT không an toàn; 3) Các kết nối mở rộng trong hệ sinh thái IoT không an toàn; 4) Thiếu các cơ chế cập nhật an toàn, hoặc cơ chế cập nhật còn nhiều thụ động; 5) Sử dụng các thành phần, thư viện phần mềm không an toàn hoặc lỗi thời; 6) Bảo vệ quyền riêng tư không đầy đủ; 7) Truyền và lưu trữ dữ liệu không an toàn; 8) Thiếu sự quản lý các thiết bị IoT; 9) Cài đặt mặc định không an toàn; 10) An ninh vật lý kém.

Khả năng bị tấn công trên diện rộng

Hệ thống IoT luôn là "miền đất hứa" cho tội phạm mạng tấn công, xâm nhập và khai thác do số lượng thiết bị khổng lồ sẽ làm tăng xác suất, tần số và mức độ nghiêm trọng của các cuộc tấn công. Trong trường hợp tấn công thành công, hacker sẽ nhanh chóng kiểm soát toàn bộ hệ thống mạng và làm tê liệt nhiều thiết bị IoT cùng lúc.

Nghiên cứu bảo mật của TrapX Security đã chỉ ra cách hack một bộ điều khiển nhiệt gia dụng kết nối Internet - NEST (thuộc sở hữu của Google). Từ đó, khai thác lỗ hổng bảo mật này để giành quyền kiểm soát toàn bộ các thiết bị kết nối trong ngôi nhà. Hay theo báo cáo gần đây của Công ty an ninh mạng Darktrace, các hacker đã chiếm quyền điều khiển một bể nuôi cá thông minh tại một sòng bạc ở Bắc Mỹ để kiểm soát hệ thống máy chủ của sòng bạc và đánh cắp 10 GB dữ liệu người chơi về máy chủ ở Ba Lan.

Những ví dụ trên đây chỉ là số ít trong rất nhiều dẫn chứng về việc thiết bị IoT là một trong những mắt xích yếu gây hiệu ứng lan truyền dẫn đến toàn bộ hệ thống mạng của một tổ chức, doanh nghiệp hay cá nhân bị tê liệt. Thông qua việc kiểm soát các thiết bị IoT, hacker không chỉ đánh cắp dữ liệu mà còn gây ra nhiều hậu quả đáng tiếc.

IoT - "mỏ dữ liệu" không giới hạn

Với hàng chục tỷ thiết bị trong hệ thống, IoT tạo ra lượng dữ liệu khổng lồ từ cảm biến được gắn vào các bộ phận của máy móc, các hệ thống camera, thành phố thông minh, nhà thông minh, điện thoại thông minh… Có thể khẳng định IoT là "mỏ dữ liệu" không có giới hạn. Theo dự báo của IDC (International Data Corporation), vào năm 2025, IoT sẽ tạo ra khoảng 79,4 Zettabyte dữ liệu. Không những thế, mỏ dữ liệu này còn chứa thông tin dữ liệu, mật khẩu người dùng. Những dữ liệu này được các công ty, doanh nghiệp sử dụng trong quảng cáo, tiếp thị và cũng là thứ để hacker tống tiền, tấn công tài khoản ngân hàng hoặc các loại tài khoản khác của người dùng.

Nguy cơ của các cuộc tấn công từ chối dịch vụ phân tán (Distributed Denial of Service - DDoS) khổng lồ

Xu thế mới của DDoS là lợi dụng các lỗ hổng từ các thiết bị IoT để biến chúng thành các botnet (các mạng máy tính được tạo lập từ các máy tính mà hacker có thể điều khiển từ xa). Nghiên cứu mới đây của Symantec đã cho thấy nạn tấn công thiết bị IoT đang ngày càng gia tăng. Tội phạm mạng đã lợi dụng những lỗ hổng bảo mật này để chiếm quyền điều khiển (hijack) các mạng gia đình và các thiết bị tiêu dùng được kết nối, từ đó thực hiện những cuộc tấn công từ chối dịch vụ DDoS.

Ví dụ điển hình của việc lợi dụng các thiết bị IoT thực hiện tấn công DDoS chính là mã độc Mirai. Các tội phạm mạng đã lợi dụng mã nguồn của Mirai để lây nhiễm sang các thiết bị IoT nhằm tạo ra các botnet sau vai trò rất lớn của phần mềm độc này trong việc tạo ra một cuộc tấn công DDoS vào website của phóng viên an ninh mạng Brian Krebs - đây là cuộc tấn công từ chối dịch vụ đạt kỷ lục với lưu lượng 620 Gbps từ các thiết bị

IoT bị nhiễm. Đặc điểm của mạng botnet này là nó không dựa trên máy tính, mà được xây dựng từ các thiết bị IoT bị nhiễm Mirai như máy ảnh, máy quay kỹ thuật số (DVR), hay CCTV... Những thiết bị này chủ yếu bị lây nhiễm do người dùng sử dụng tên và mật khẩu có độ bảo mật yếu, hoặc dùng mặc định. Kể từ khi mã nguồn của Mirai được phát tán thì tội phạm đã nhanh chóng phát triển các biến thể mới của nó, theo ghi nhận của Level 3 Communications, một công ty cung cấp dịch vụ Internet và viễn thông đa quốc gia của Mỹ, đã có 4 máy chủ ra lệnh kiểm soát kết hợp với kích hoạt Mirai trong tháng. Công ty này cũng cho biết, khoảng một nửa số botnet là đến từ Mỹ và Brazil, 80% là từ các DVR, nhiều cuộc tấn công là nhằm vào máy chủ điều hành game hay địa chỉ IP riêng. Một số cuộc tấn công được Level 3 Communications ghi nhận đạt tới hơn 100 Gbps với một số lượng lớn botnet được điều khiển, cá biệt có trường hợp lên tới 100.000 botnet để tấn công.

Theo Symantec, 2015 là năm kỷ lục về tấn công IoT, với nhiều vụ chiếm quyền điều khiển tự động hóa nhà và các thiết bị an ninh nhà. Trong đó, kẻ tấn công thường ít quan tâm đến nạn nhân mà phần lớn muốn chiếm quyền điều khiển thiết bị để thêm nó vào botnet, rồi sử dụng để thực hiện tấn công DDoS. Hầu hết phần mềm độc hại nhằm mục tiêu vào thiết bị IoT như máy chủ web, router, modem, thiết bị lưu trữ dữ liệu qua mạng NAS, hệ thống camera quan sát CCTV và hệ thống điều khiển. Bảo mật yếu kém trên nhiều thiết bị IoT đã khiến chúng dễ dàng trở thành mục tiêu tấn công, và thậm chí ngay cả khi đã bị nhiễm mã độc, nạn nhân vẫn không hề hay biết.

Kết luận và khuyến nghị

IoT là mạng kết nối hàng tỷ thiết bị, với nền tảng là sự liên kết chặt chẽ, cốt lõi và giá trị của hệ thống là tập dữ liệu khổng lồ. Có thể thấy rằng, hệ sinh thái IoT ngày càng đa dạng và phát triển không ngừng. Trong tương lai, tất cả các sự vật, thiết bị sẽ được kết nối với nhau và trở thành IoE (Internet of Everything). IoT thúc đẩy việc số hóa thông minh của các ngành, các tầng lớp xã hội, trở thành động lực thúc đẩy sự chuyển đổi số trên khắp thế giới, mang lại giá trị kinh tế rất lớn.

Lợi ích mà IoT đem lại là không thể phủ nhận, nhưng nguy cơ và thách thức mà IoT đặt ra cũng không hề nhỏ. Các công cụ được sử dụng để tấn công IoT ngày càng trở nên tinh vi hơn, các thuật toán tấn công và trí thông minh nhân tạo góp phần tạo nên mối đe dọa với IoT. Do đó, việc nâng cao nhận thức của các tổ chức/cá nhân là vô cùng cần thiết.

Qua đây, chúng tôi xin có một vài khuyến nghị nhằm nâng cao bảo mật hệ thống IoT, cụ thể như sau:

Một là, các nhà sản xuất và phát triển thiết bị IoT cần đảm bảo theo đúng tiêu chuẩn, quy định và không ngừng cải tiến các thiết bị IoT; đưa ra yêu cầu bắt buộc người dùng thay đổi mật khẩu mặc định khi sử dụng; thường xuyên cập nhật phần mềm, gói bảo mật một cách tự động, không cần người dùng phải thực hiện thủ công; đặt vấn đề an toàn thông tin cho thiết bị IoT lên hàng đầu và lấy đó làm lợi thế cạnh tranh của doanh nghiệp.

Hai là, các doanh nghiệp cung cấp dịch vụ Internet, dịch vụ viễn thông chủ động giám sát, ngăn chặn các máy chủ có khả năng điều khiển, phát tán mã độc IoT; hỗ trợ người dùng trong công tác rà quét, tháo gỡ mã độc IoT; kiểm tra thiết bị IoT trước khi cho phép kết nối mạng.

Ba là, các doanh nghiệp cung cấp sản phẩm, dịch vụ bảo mật cần đẩy mạnh nghiên cứu, phát triển, nâng cấp các sản phẩm bảo mật thông tin cho hệ thống IoT; hợp tác với nhà cung cấp thiết bị IoT, nhà cung cấp dịch vụ mạng để tích hợp các biện pháp bảo mật thông tin trong các thiết bị IoT.

Bốn là, người dùng là các cá nhân, tổ chức cần cân nhắc khi sử dụng các thiết bị IoT, lựa chọn sản phẩm của các nhà sản xuất uy tín; thay đổi mật khẩu, cấu hình mặc định và thường xuyên, định kỳ thay đổi mật khẩu, cấu hình để nâng cao tính bảo mật; sử dụng các sản phẩm bảo mật hệ thống IoT, đặt các thiết bị IoT dưới sự giám sát, theo dõi của hệ thống tường lửa; nâng cao nhận thức, hiểu biết về bảo mật IoT để giảm thiểu rủi ro ✍

TÀI LIỆU THAM KHẢO

1. Ovidiu Vermesan, Peter Friess, et al. (2009), *Internet of Things Strategic Research Roadmap*, 44pp, European Research Cluster on the Internet of Things (IERC).

2. Cục Thông tin Khoa học và Công nghệ Quốc gia (2016), *Tổng luận Internet vạn vật: hiện tại và tương lai.*

3. W.E. Summary and S. Plants (2015), *Power and the Industrial Internet of Things (Ilo T)*, pp.1-14.

4. IoT.Business.News (2016), *Symantec Research Finds IoT Devices Increasingly Used to Carry out DDoS Attacks*, https://iotbusinessnews.com/.