Những nguy cơ bảo mật mới

Bạn cần theo dõi kỹ hóa đơn ngay sau khi thanh toán và kiểm tra xem liệu iPhone của mình có bị jailbreak hay không.

Hàng năm, có ba sự kiện về bảo mật lớn nhất thế giới diễn ra, mà phần lớn đều rơi vào mùa hè, đó là: Cyber Week tổ chức tại Tel Aviv (Israel), Black Hat và DEF CON tại Las Vegas (Mỹ). Mỗi sự kiện đều có những đặc điểm đặc trưng riêng. Với Cyber Week, nhà quản lý của các công ty bảo mật lớn nói về những nguy hiểm, mối đe dọa mới. Trong khi các nhà nghiên cứu bảo mật làm việc cho nhiều công ty khác nhau thảo luận chi tiết về các kiểu tấn công, phương thức tấn công tại Black Hat. Ngược lại, hiếm có diễn giả nào sử dụng tên thật của mình tại DEF CON, nơi mà những tấn công trình diễn trên màn hình thường ít nhiều dây dưa đến pháp luật. Thực tế, năm nay đã có một vụ bắt giữ ngay tại DEF CON.

Thông thường, những sự kiện như vậy bàn xa hơn về những kỹ thuật tấn công mang mới, không phải chỉ thảo luận làm cách nào để ngăn chặn những tấn công hiện có. Các chuyên gia có chung nhận định rằng, những gì thể hiện trong sự kiện rất có thể sẽ sớm diễn ra ngoài đời thực. Từ ba sự kiện bảo mật diễn ra năm nay, chúng ta có thể biết được xu hướng và những rủi ro bảo mật tiềm tàng sắp đến.

Tấn công vào điện thoại thông minh

Tin tặc đã xem điện thoại thông minh là một trong những mục tiêu đáng để quan tâm nhất, bởi vì những thiết bị này chứa đủ mọi loại dữ liệu như email, hình ảnh, dữ liệu thẻ tín dụng… Nếu có đúng phần mềm, dữ liệu có thể truy xuất và chỉnh sửa được, thậm chí dữ liệu xác định vị trí của thiết bị cũng có thể bị giả.

Vòng lặp thanh toán di động

Hệ thống thanh toán di động Apple Pay của Apple vốn được xem là một trong những hệ thống bảo mật nhất thế giới. Nhưng mọi thứ có vẻ tan biến sau bài trình diễn qua mặt hệ thống này của Tim Yunusov tại Black Hat. Mặc dù nhiều chuyên gia tin rằng Apple Pay đủ an toàn ngay cả khi hệ thống bảo mật thiết bị iOS bị vô hiệu hóa khi người dùng sử dụng jailbreak, nhưng Yunusov sử dụng các công cụ mà anh tự viết để đọc được dữ liệu, chứng minh nhận định trên là sai. Vì thế, người dùng cần kiểm tra xem thiết bị mình có đang bị là đối tượng cho kẻ xấu jailbreak hay không. Một cách kiểm tra là sử dụng ứng dụng SystemGuard.

Tuy nhiên, những lỗi này liên quan đến các trường hợp khi người dùng sử dụng thiết bị để thanh toán qua Apple Pay. Yunusov phát hiện rằng quy trình thanh toán có thể được thực hiện ngay cả khi người bán không xác thực thông tin chính xác của người mua. Kết quả là xảy ra một kiểu tấn công giống như vòng lặp, tạo cho khóa mã hóa (crypto-key) kết hợp với quy trình thanh toán một vài lần. Khóa này có chứa thông tin về số thẻ tín dụng mà Apple phân bổ cho mỗi lần thanh toán và tin tặc có thể dùng nó để khởi chạy các quy trình thanh toán ngẫu nhiên cho những số tiền ngẫu nhiên. Chỉ có một điều kiện cần phải đáp ứng và đó là cho các thủ tục thanh toán liên quan đến cùng nhà cung cấp dịch vụ, cũng như chỉ tồn tại trong khoảng thời gian

ngắn. Nên khi xảy ra mất tiền, người dùng không thể tự bảo vệ mình được. Apple và các ngân hàng phải tắt khóa crypto-key ngay lập tức khi giao dịch vừa hoàn tất, còn không người dùng buộc phải theo dõi sát sao số tiền và thời điểm giao dịch của mình.

Phần mềm lén lút theo dõi trên Android

Cách đây một năm, một vụ việc tai tiếng mà các cơ quan tình báo một số quốc gia dây vào là phần mềm Pegasus do NSO Group Technologies phát triển nhằm theo dõi gián điệp trên các thiết bị iOS. Mọi thứ mà kẻ tấn công làm chỉ là gửi một tin nhắn SMS giả mạo đơn giản, dụ người dùng đến một trang web. Nhưng nay, các nhà nghiên cứu bảo mật của Lookout vừa phát hiện một phiên bản tương tự liên quan đến nền tảng Android và họ cũng đã trình diễn tại Black Hat. Phần mềm này tên là Chrysaor và phương pháp tấn công của nó là hướng đến đối tượng rất cụ thể. Theo Lookout, phần mềm nhiễm được chỉ hơn hơn 0,000001% thiết bị Android trên thế giới. Nó thâm nhập thiết bị thông qua lừa đảo giống Pegasus hay yêu cầu người dùng tải về một ứng dụng nào đó, sau đó nó lập tức tự cài đặt vào thiết bị và kiểm tra ngay xem nó có quyền root (quyền cao nhất) trên điện thoại đó hay không.

Nếu có quyền, nó sẽ bắt đầu theo dõi và trích xuất dữ liệu. Nếu nó không dành được quyền root thì không theo dõi thời gian thực. Trong trường hợp đó, Chrysaor đơn giản là duyệt qua thiết bị, thu thập dữ liệu và gửi dữ liệu đến một máy chủ giám sát. Công cụ này ảnh hưởng đến hầu hết mọi phiên bản Android hiện nay. Nhưng không như Pegasus, NGO Group thậm chí không cần phải sử dụng các lỗ hổng zero-day, nên người dùng rất khó tự bảo vệ mình. Cách bảo vệ tốt nhất là chỉ nhấn vào những link mà người dùng biết chắc là an toàn và sử dụng ứng dụng chuẩn, đã được Google xác thực.

Giả địa chỉ GPS để loại bỏ xác thực 2 yếu tố

Trong sự kiện DEF CON vừa qua, một tin tặc có nickname "Karit" trình diễn cho mọi người thấy anh dễ dàng giả địa chỉ GPS như thế nào, và một công cụ phần mềm đánh lừa được hệ thống theo dõi chỉ có giá khoảng 500 USD. Có rất nhiều cách tấn công khi giả được địa chỉ GPS. Ví dụ, một chuyến Uber tính toán chi phí dựa trên quãng đường và thời gian. Karit có thể giả lập giá trị khoảng cách bằng cách áp dữ liệu GPS đã bị giả, lấp lên dữ liệu GPS truyền từ vệ tinh ở khoảng cách 20.000km trên bầu trời.

Một ứng dụng khác là sử dụng dữ liệu định vị và GPS để giả time zone trên thiết bị. Cách này rất hữu hiệu để vượt mặt bảo mật hai yếu tố, qua mặt nhiều công ty và nhiều dịch vụ. Karit sử dụng bộ truyền GPS để quay ngược đồng hồ với mốc thời gian sai lệch. Và mật khẩu nhập một lần, không cần qua xác thực bước thứ hai, sẽ hoạt động như lối cũ. Theo Karit, tấn công kiểu này là khả thi nếu bộ nhân dữ liệu GPU của công ty nào đó bị tin tặc làm nghẽn. Dĩ nhiên, một số công ty lớn như Google và Amazon không chỉ dựa vào mỗi tín hiệu GPS về thời gian, mà họ còn dựa vào các nguồn khác như NIST (National Institude of Standard and Technology) để xác thực.

Tấn công vào thiết bị có kết mạng

Thiết bị này được rao bán trực tuyến chỉ với 22 USD, sử dụng sóng radio để tấn công các thiết bị điều khiển từ xa.

Các thiết bị thông minh trong nhà rất ít tính năng bảo mật, hoặc chúng có hệ thống mã hóa đơn giản, nên kẻ tấn công chỉ cần chiếm dụng được đường truyền tín hiệu radio.

Tấn công bằng sóng âm

Các nhà nghiên cứu tại công ty thương mại điện tử Alibaba của Trung Quốc vừa phát hiện ra các thiết bị hiện đại có thể bị đánh lừa bằng sóng âm. Các chuyên gia này đã dùng một phần cứng tầm khoảng 350 USD để làm hỏng màn hình điện thoại thông minh và thậm chí khiến thiết bị bay không người lái (drone) bị rơi. Theo họ, tấn công nguy hiểm nhất của kiểu này là hướng đến các thiết bị như bàn trượt hoverboard và xe tự cân bằng hai bánh ngang (scooter). Trong một đoạn video trình diễn, họ đã tấn công xe scooter Segway Minipro. Sóng âm can thiệp vào các cảm biến của scooter, khiến người lái bị té ngã. Trong trường hợp này, người dùng thiết bị không thể tự bảo vệ được mình nên các nhà sản xuất chính là bên chịu trách nhiệm và phải khắc phục nhược điểm này. Các nhà nghiên cứu đề nghị sử dụng một bộ xử lý chuyên để bảo vệ mạch điện, đồng thời nhà sản xuất cũng cần đưa ra bản sửa lỗi phần mềm, chẳng hạn một thuật toán để lọc các tín hiệu sóng âm độc hại, không cho chúng xâm nhập vào luồng truyền dữ liệu của cảm biến.

Nhiều thiết bị IoT có thể bị tấn công dễ dàng

Caleb Madrigal (có biệt danh là Metem) cũng sử dụng sóng âm để tấn công. Anh vài lần sử dụng phần cứng chỉ có giá tầm vài trăm đô la, dựa trên tín hiệu radio và dải tần sóng âm để phát sóng và tấn công thiết bị.

Anh phát hiện ra được có nhiều thiết bị IoT như các cảm biến thông minh chỉ có lớp bảo mật bằng phần mềm, dùng tín hiệu radio để điều khiển các thiết bị khác nên những tín hiệu ấy có thể dễ dàng bị ghi lại và bị giả lập. Anh sử dụng công cụ âm thanh

miễn phí Audacity để vận hành và chiếm dụng thiết bị mà không cần một công cụ phần mềm chuyên dụng nào khác. Tại DEF CON, Madrigal trình diễn phương thức này để làm tê liệt các hệ thống cảnh báo trong nhà.

Tin tặc chỉ mất vài giây với máy ATM

Thậm chí, có một chương trình huấn luyện khoảng một giờ cho tin tặc tại Tel Aviv. Tại đây, các chuyên gia bảo mật từ khắp nơi trên thế giới sử dụng những kỹ thuật sẵn có để cùng tấn công và đáp trả tấn công. Trong số giảng viên có những cựu quân nhân từng nằm trong đơn vị Unit 8200 nổi tiếng trong quân đội Israel. CEO CyberGym, Ofir Hason, cho biết: "Chương trình này cho phép các doanh nghiệp giả lập nhiều kiểu tấn công khác nhau, như tấn công vào các nhà máy công nghiệp vận hành các hệ thống tự động SCADA."

Khách hàng của Hanson có những ngân hàng lớn, nên một trong những đối tượng thử nghiệm tấn công là máy rút tiền ATM. Khoảng 50.000 máy loại này có ở châu Á. Nên chương trình đã cho các ngân hàng thấy họ gặp rủi ro ở mức nào, bởi vì máy ATM cũng sử dụng máy tính, trong đó nhiều máy còn chạy hệ điều hành Windows NT 4.0 hay Windows XP rất dễ bị tấn công. Các phiên bản Windows cũ vẫn còn được sử dụng vì vài ngân hàng thấy việc nâng cấp quá đắt đỏ. Tuy nhiên, Hason cũng như các chuyên gia bảo mật khác rất kín tiếng về các lỗ hổng của ATM.

Tại Black Hat, các chuyên gia của IOActive cho mọi người thấy họ có thể truy cập các cổng USB ẩn của những máy ATM đời mới như thế nào chỉ trong vài giây, với mục đích cài malware để vô hiệu hóa mọi cơ chế bảo mật của máy. Kỹ thuật này còn có tên gọi "jackpotting", là phương pháp dù không mới vẫn còn áp dụng được. Hồi tháng 8 vừa qua, một thủ phạm đã bị ghi hình tại một chi nhánh của Postbank, sử dụng thanh nhớ USB để cài malware vào máy ATM và rút sạch tiền từ máy. Tuy nhiên, kẻ này phải mất nửa giờ đồng hồ để thực hiện, còn các chuyên gia IOActive làm nhanh hơn nhiều.

Tấn công ô tô

Các nhà sản xuất ô tô dần nhận thấy máy tính tích hợp trên bo mạch của xe cũng cần được bảo vệ tốt. Ngay cả hãng xe thuần chất công nghệ như Tesla cũng thấu hiểu được tầm quan trọng của vấn đề này, bởi vì các chiếc xe Tesla liên tục bị lấy ra làm mẫu tấn công của tin tặc và các chuyên gia, mặc dù chúng cũng được update thường xuyên.

Ô tô Tesla chưa thể lấp lỗ hổng

Hồi tháng 9/2016, các chuyên gia ở công ty bảo mật Keen Security Lab cho thấy họ có thể xâm nhập được vào máy tính điều khiển của xe Tesla và chiếm quyền mọi thứ, từ mái trần xe cho đến phanh thắng của xe. Chỉ trong vòng 10 ngày, Tesla bịt ngay lỗ hổng bằng một bản vá cập nhật trực tiếp. Đến nay, hơn một năm sau, cũng những người đó lại khiến Tesla đau đầu lần nữa. Lần này, các chuyên gia lại chiếm dụng được các hệ thống quan trọng, trong đó có phanh thắng.

Trong trường hợp này, tin tặc sử dụng một mạng guest mở (thường có trong các workshop của Tesla) để truy cập vào máy tính trong xe, và họ tìm thấy một lỗi trong engine trình duyệt WebKit. Từ đó, họ có thể xâm nhập được vào hệ thống điều khiển của xe.

Nhờ vào một lỗ hổng trong chứng nhận mã nguồn, các chuyên gia có thể đưa mã nguồn của họ vào, nên chiếm dụng được hệ thống quản lý của xe. Thậm chí, kẻ tấn công cũng có thể mở cửa và bật/tắt đèn xe. Theo Keen Security Lab, Tesla cũng ngay lập tức phản ứng và đưa ra bản vá trong vòng 10 ngày. Nhưng với ô tô của các hãng khác, bảo mật của các xe này rất thấp, kể cả với những dòng xe mới nhất của BMW, Mercedes hay VW vì chúng phải cần cập nhật qua ngõ USB trực tiếp tại xưởng, nên người dùng mất rất nhiều thời gian.

Tấn công hàng loạt vào các hãng ô tô

Viễn cảnh tấn công đồng loạt vào hàng loạt xe đang chạy trên đường mới khiến Elon Musk, CEO của Tesla e ngại. Trong trường hợp này, tội phạm mạng có thể tấn công vào máy chủ chính của Tesla, nên chúng có thể chiếm dụng từ xa mọi xe Tesla trên thế giới. Nhưng Musk không phải là người duy nhất e ngại vấn đề này, nỗi lo sợ này bắt nguồn từ Yuval Diskin, cựu giám đốc cơ quan tình báo quốc nội của Israel. Ông cho rằng mối hiểm họa này trước sau gì cũng sẽ xảy ra. Ví dụ, một tổ chức bí mật nào đó nếu có đủ nguồn lực về tài chính và nhân sự thì có thể làm tê liệt mọi xe BMW trên toàn cầu.

Chính dịch vụ rửa xe cũng là lỗ hổng

Các nhà nghiên cứu ở Whitescope lại có cách khác chứng minh được rằng các dịch vụ rửa xe cũng có thể là nơi tin tặc thèm thuồng. Họ lấy ví dụ như ở Laserwash, là công ty chuyên cung cấp giải pháp rửa xe. Để đảm bảo không ai bị thương, các chuyên gia lập trình một phần mềm cho thấy các dịch vụ rửa xe có thể gây hại cho ô tô thế nào. Họ chỉ cần truy cập vào web để chiếm dụng cảm biến từ xa của xe.

Trong trường hợp này, các dịch vụ rửa xe tự động có thể bị nghẹt ở xe và làm cho người dùng bị thương. Tin tặc có thể dùng phương pháp này để tấn công, bằng cách sử dụng kiểu mật khẩu đơn giản để truy cập vào proxy web của dịch vụ rửa xe. Không may là các nhà sản xuất ô tô xem nhẹ lỗ hổng dạng này nên họ không mấy quan tâm việc vá lỗ hổng. Các nhà sản xuất chỉ để xuất dịch vụ rửa xe thay đổi mật khẩu chuẩn nhưng nhiều dịch vụ vẫn để hệ thống của họ tự do kết nối internet.

ĐỒNG ANH