Bản tin điện tử nội bộ - Số 81 | Tháng 08 - 2018

THẾ GIỚI THẺ

Tổng biên tập: *Bà Phan Thị Quỳnh Hoa - Giám đốc Tập đoàn MK* | **Ý kiến đóng góp vui lòng gửi về:** *marketing@mkgroup.com.vn*

Lưu ý: *Toàn bộ thông tin/hình ảnh trong Bản tin điện tử nội bộ Thế Giới Thẻ MK Group được sưu tầm từ các nguồn tin khác nhau và chỉ sử dụng cho mục đích chia sẻ kiến thức.*

Các tin bài chính

FIDO® KEYPASS S1 – Sản phẩm Token đầu tiên của Việt Nam đạt chứng chỉ FIDO U2F

FIDO® KEYPASS S1 -

Sản phẩm Token đầu tiên của Việt Nam đạt chứng chỉ FIDO U2F

Ngày 08/08/2018, Liên minh Xác thực FIDO (FIDO Alliance) - trụ sở tại bang California, Hoa Kỳ, đã cấp chứng nhận cho sản phẩm KeyPass U2F Token của Công ty Cổ phần Tập đoàn MK (MK Group) đạt tiêu chuẩn U2F (Universal Second Factor – công nghệ xác thực nhân tố thứ 2) của FIDO Alliance.

Để đạt được chứng nhận U2F này, sản phẩm FIDO® KEYPASS S1 của MK Group đã phải phát triển và đảm bảo các thuật toán về chữ ký số theo chuẩn ECDSA P-256, các thuật toán bảo vệ mật mã theo chuẩn SP800-38F và các thuật toán về hàm băm theo chuẩn FIPS180-4. Tiếp theo, để chứng minh cho tính ổn định của sản phẩm, FIDO® KEYPASS S1 đã phải vượt qua 100 nghìn lần xác thực đăng nhập /xác thực thanh toán thành công cùng với những cam kết và quy định bảo mật nghiêm ngặt khác của FIDO Alliance.

Với sản phẩm KeyPass U2F Token của MK Group, các tổ chức và doanh nghiệp sẽ trở nên an toàn hơn trong việc chống lại hành vi skimming (sao chép), phishing (lừa) và chiếm quyền sử dụng tài khoản mật mã.

Bằng nhiều những thủ đoạn tinh vi khác nhau, những kẻ lừa đảo trực tuyến luôn tạo ra được những đường link giả mạo khiến cho người sử dụng nhầm lẫn để từ đó đánh cắp toàn bộ dữ liệu bảo mật của nạn nhân và tấn công vào các tài khoản của họ. Đây luôn là một trong những vấn đề hóc búa của nhiều doanh nghiệp và tổchức, đặc biệt là các ngân hàng, khi tội phạm mạng thường xuyên giả đường link website của Ngân hàng để lừa khách hàng vào giao dịch, nhằm ăn cắp tên và mật khẩu truy cập vào tài khoản ngân hàng điện tử của khách hàng và/hoặc thông tin thẻ tín dụng quốc tế của khách hàng.

Như vậy, cho dù các tổ chức có thể đảm bảo hệ thống máy tính của mình một cách an toàn nhất nhưng các chuyên gia an ninh hầu như không thể kiểm soát việc một nhân viên
hoặc khách hàng “vô tình bị lừa” bởi một trang web hoặc một email giả mạo từ những kẻ tấn công chuyên nghiệp. Và một khi lỗ hổng bảo mật hình thành, những thiệt hại mà doanh nghiệp và cá nhân phải hứng chịu khi cuộc tấn công xẩy ra là không hề nhỏ.

Hiện nay trên thế giới, một trong những tổ chức dường như đã vô hiệu hóa được vấn đề nan giải này chính là Google với việc ứng dụng và triển khai thiết bị token bảo mật theo tiêu chuẩn U2F cho hơn 85 nghìn nhân viên. Các nhân viên của Google được yêu cầu phải sử dụng thiết bị này như một chiếc khóa an ninh cho mọi hoạt động đăng nhập máy tính. Giải pháp này đã được Google ghi nhận thành công trong việc chống lại các nỗ lực lừa đảo nhắm vào doanh nghiệp trong gần 2 năm qua (*)

MK Group đã hoàn thiện sản phẩm KeyPass U2F Token, được xác nhận tuân thủ tiêu chuẩn U2F của FIDO Alliance, với thao tác người dùng đơn giản và dễ đàng ứng dụng cho mọi tổ chức doanh nghiệp, cá nhân muốn bảo vệ tài khoản ngân hàng, mạng xã hội hay email của mình.

(84-24) 6266 2703 - 513 thegioithe@mkgroup.com.vn www.facebook.com/mkgroup1999

Không cần cài đặt phần mềm, người sử dụng chỉ cần đơn giản đăng ký sử dụng "Xác minh nhân tố thứ 2" có sẵn trong tất cả các trang chủ chấp nhận FIDO U2F *(Tham khảo tại: https://www.dongleauth.info)* gồm các bước: đăng nhập, bấm nút để Token tự động xác minh website "xịn" và đẩy cặp khóa PKI công khai và bí mật vào hệ thống để xác thực.

Trong thời gian tới, trung tâm Nghiên cứu - Phát triển của MK Group đang hoàn thiện và đưa thêm bộ cảm biến sinh trắc học vào thiết bị Token này để xác thực vân tay người dùng trước khi tiến hành xác thực OTP cho các giao dịch.

Theo chia sẻ của ông Nguyễn Trọng Khang, Chủ tịch Hội đồng Quản trị của MK Group *"Không có nhiều công ty trên thế giới làm được điều này. Chúng tôi tự hào khi MK Group là công ty Việt Nam duy nhất có thể tự nghiên cứu và cung cấp cho thị trường những giải pháp xác thực bảo mật "Made in Vietnam" - có đủ năng lực cạnh tranh về Chất lượng và Giá thành với các công ty toàn cầu bằng những sản phẩm như KeyPass U2F Token. Với định hướng Smart Digital Secuirty – Bảo mật Số Thông minh, hiện MK Group đang nỗ lực để hoàn thiện thêm những sản phẩm an ninh thú vị và giới thiệu ra thị trường trong thời gian tới."*

Về FIDO Alliance:

Liên minh Xác thực FIDO (FIDO Alliance) được thành lập năm 2013, có trụ sở tại bang California, Hoa Kỳ. Các đặc điểm kỹ thuật và các chứng nhận của FIDO Alliance cho phép một hệ sinh thái tương thích phần cứng, di động và sinh trắc học được dựa trên các trình xác thực có thể được sử dụng với nhiều ứng dụng và trang mạng khác nhau. Với hệ sinh thái này, các tổ chức và nhà cung cấp dịch vụ có thể triển khai các giải pháp xác thực mạnh giúp giảm sự phụ thuộc vào mật khẩu và bảo vệ chống lại hoạt động skimming (sao chép), phishing (lừa) và chiếm quyền sử dụng mật mã.

Về MK Group:

MK Group thành lập năm 1999, là công ty hàng đầu khu vực chuyên về các giải pháp xác thực bảo mật kỹ thuật số và Thẻ thông minh. Với gần 20 năm kinh nghiệm hoạt động và không ngừng đầu tư để nâng cao chất lượng sản phẩm và dịch vụ, MK Group đã cung cấp và triển khai thành công nhiều sản phẩm – giải pháp xác thực bảo mật và phát hành thẻ cho khối chính phủ, tài chính – ngân hàng, doanh nghiệp, viễn thông và vận tải trong và ngoài nước.

(*) Trích dẫn từ nguồn Business Insider

ĐIỂM TIN VIỆT NAM

- Từ 20/8, SCB chính thức mở rộng hình thức thanh toán qua mã QR với thẻ tín dụng SCB Visa. Trước đó nhà băng đã triển khai phương thức này cho tài khoản thanh toán hoặc thẻ tín dụng quốc tế SCB MasterCard. Theo đó, chủ thẻ SCB Visa không cần mang theo thẻ hoặc tiền mặt mà chỉ cần sử dụng ứng dụng SCB Mobile Banking trên thiết bị di động, thực hiện quét mã QR tại các đơn vị chấp nhận là có thể thực hiện ngay thanh toán mua sắm, ăn uống hay du lịch.

- Ngân hàng TMCP Kiên Long (Kienlongbank) vừa ra mắt thẻ tín dụng quốc tế Kienlongbank JCB và công bố đại sứ thương hiệu vào ngày 18/8 tại TP HCM. Theo đó, thẻ tín dụng quốc tế Kienlongbank JCB được phát hành gồm ba hạng thẻ là Platinum, Gold và Classic. Sản phẩm tích hợp nhiều tiện ích như mạng lưới chấp nhận thẻ với gần 30 triệu đối tác trên toàn thế giới, dịch vụ chăm sóc khách hàng tại JCB Plaza, quầy hỗ trợ thông tin tại nước ngoài.

- HSBC Việt Nam vừa ra mắt sản phẩm thẻ tín dụng mới được thiết kế đặc biệt cho thị trường Việt Nam, thể hiện sự am hiểu của ngân hàng đối với các nhu cầu hiện nay của khách hàng nội địa. Sản phẩm thẻ tín dụng Cash-Back mới của HSBC khuyến khích khách hàng tại Việt Nam sử dụng hình thức thanh toán phi tiền mặt thường xuyên hơn bằng cách mang đến một loạt các ưu đãi gần gũi với đời sống hàng ngày.

(Tổng hợp từ Internet)

Anh: Thanh toán thẻ ghi nợ lần đầu tiên thắng thế tiền mặt

Tổng lượng giao dịch thanh toán bằng thẻ ghi nợ tại Anh lần đầu tiên được ghi nhận vượt qua thanh toán tiền mặt. Nguyên chính dẫn tới kết quả này là sự phổ biến ngày càng rộng rãi của các dịch vụ thanh toán không tiếp xúc (TTKTX) và mua sắm trực tuyến.

Báo cáo thị trường mới nhất của Hiệp hội Tài chính Anh (UK Finance) cho thấy công nghệ mới, sáng kiến thanh toán và sự thay đổi trong thói quen tiêu dùng đã góp phần tạo nên 13,2 tỷ lượt giao dịch thanh toán thẻ, lần đầu tiên trong lịch sử vượt qua thanh toán tiền mặt với 13,1 tỷ lượt. Kết quả này đã xảy ra sớm hơn một năm so với dự báo trước đó của các chuyên gia.

Tính gộp cả thẻ ghi nợ và thẻ tín dụng, tổng lượng giao dịch TTKTX tại Anh trong năm 2017 tăng 97% lên 5,6 tỷ lượt. Trong khi đó, thanh toán tiền mặt giảm 15% so với năm 2016.

Tính đến cuối năm 2017 đã có gần 119 triệu thẻ không tiếp xúc được lưu hành và, với việc người tiêu dùng cũng như các doanh nghiệp ngày càng ưa chuộng sử dụng thẻ TTKTX và các thiết bị chấp nhận thẻ TTKTX, giới chuyên môn dự đoán 36% tổng số giao dịch thanh toán tại Vương quốc Anh vào năm 2027 sẽ là các giao dịch TTKTX.

Tổng lượng thanh toán bằng tiền mặt tại Anh dự kiến sẽ vẫn tiếp tục giảm trong thập kỷ tới. Và dự kiến sẽ chỉ còn khoảng 6,4 tỷ lượt giao dịch thanh toán bằng tiền mặt được thực hiện tại xứ sở sương mù vào năm 2027, chiếm khoảng 16% tổng lượng giao dịch thanh toán. Tuy nhiên, tiền mặt vẫn sẽ là phương thức thanh toán phổ biến thứ hai tại nước này vào năm 2027.

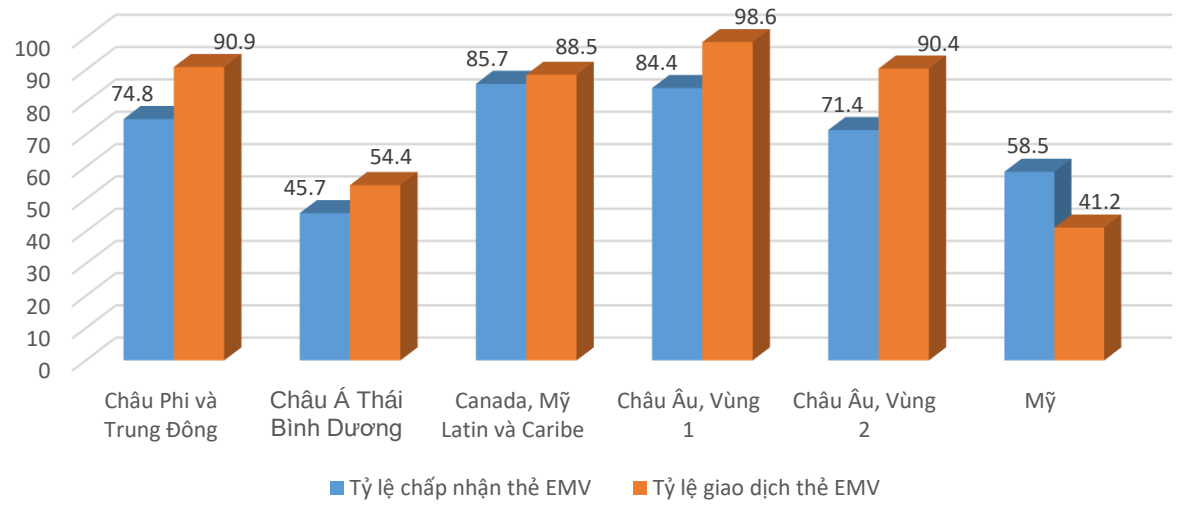
“Nước Anh còn cách xa mục tiêu xã hội không tiền mặt. Mặc dù chúng tôi đang chuyển dần sang nền kinh tế mà tại đó vai trò của tiền mặt ngày càng trở nên ít quan trọng hơn so với trước đây, song tiền mặt sẽ tiếp tục là phương thức thanh toán được nhiều người ưa thích”, Stephen Jones - GĐĐH UK Finance dự báo./.

(Finextra)

Phát hành và giao dịch thẻ EMV tăng trưởng hơn 50% trên toàn cầu

Tính đến cuối năm 2017 đã có 54,6% tổng lượng thẻ thanh toán được phát hành trên toàn cầu hợp chuẩn EMV, và tổng số thẻ thanh toán EMV đang được lưu hành trên toàn thế giới đạt mức 7,1 tỷ, tăng 1 tỷ thẻ so với năm 2016. Bên cạnh đó, khoảng 64% tổng lượng giao dịch thanh toán trực tiếp sử dụng thẻ trên toàn cầu trong năm 2017 đã sử dụng công nghệ chip EMV, cao hơn đáng kể so với tỷ lệ 52,4% của một năm trước đó, theo số liệu thống kê của EMVCo.

Biểu đồ tỷ lệ chấp nhận và giao dịch thẻ Chip EMV từng khu vực
(Đơn vị: %)



"Việc lượng phát hành thẻ chip EMV và giao dịch bằng thẻ chip EMV đều đã vượt mức 50% trên toàn cầu là minh chứng rõ nét về sự phát triển ngày càng hoàn thiện của cơ sở hạ tầng trên toàn thế giới, đồng thời là dấu mốc quan trọng đối với cộng đồng thanh toán", Jack Pan - Chủ tịch Ủy ban điều hành EMVCo nhận định./.

(ATM marketplace)

Trung Quốc phát hành hơn 7 tỷ thẻ ngân hàng

Tính đến cuối năm 2017, Trung Quốc đã phát hành 7,03 tỷ thẻ ngân hàng, tăng 10,3% so với năm 2016 và đạt tỷ lệ bình quân khoảng 5 thẻ/người, số liệu thống kê chính thức của Hiệp hội Ngân hàng Trung Quốc (CBA).

CBA cho biết số lượng giao dịch qua thẻ ngân hàng trong năm 2017 tại nền kinh tế lớn thứ hai thế giới đạt tốc độ tăng trưởng 29,4% lên 149 tỷ lượt, với tổng giá trị vào khoảng 735 nghìn tỷ NDT (khoảng 113 nghìn tỷ USD).

Theo Tổng thư ký CBA - Hoàng Nhuận Trung, tiêu dùng thông qua thẻ ngân hàng chiếm 48,7% tổng doanh số bán lẻ hàng tiêu dùng của Trung Quốc, và tăng trưởng liên tục trong 4 năm qua, đồng thời trở thành động lực mạnh mẽ đối với xu hướng tăng trưởng và nâng cao chất lượng tiêu dùng.

Trong khi đó, tỷ lệ sử dụng thẻ ghi nợ đang có xu hướng giảm trong 2 năm gần đây xuống còn 66,2% trong năm 2017. Ngoài ra, tỷ lệ sử dụng thẻ tín dụng tại Trung Quốc đã tăng lên 73,1% trong năm 2017, qua đó cho thấy sự phát triển với chất lượng ngày càng cao của ngành thẻ ngân hàng./.

(Xinhua)

Na Uy dự chi 86 triệu USD cho hệ thống thẻ ID quốc gia mới

Na Uy dự kiến sẽ đầu tư khoảng 700 triệu Kroner (tương đương với 86 triệu USD) để phát hành thẻ căn cước (ID) quốc gia mới.

Theo tờ báo địa phương Afterposten, những số liệu mới trong ngân sách quốc gia của Chính phủ Na Uy đã ước tính chi phí triển khai dự án là vào khoảng 596 triệu Kroner. Bên cạnh đó, hoạt động nâng cấp hệ thống văn phòng phát hành hộ chiếu trên toàn quốc để tương thích với công nghệ thẻ mới sẽ đòi hỏi phải đầu tư thêm khoảng 120 triệu Kroner nữa.

Thẻ ID quốc gia mới của Na Uy dự kiến sẽ được phát hành sớm nhất vào năm 2020. Aftenposten cho biết chi phí đã tăng dần theo quá trình triển khai dự án do nhiều vấn đề phát sinh và phạm vi triển khai được mở rộng.

Mục đích của dự án phát hành thẻ ID mới của Na Uy là cung cấp cho các công dân nước này giấy tờ du lịch để sử dụng trong Khu vực Schegen và tạo điều kiện thuận lợi cho họ trong hoạt động sử dụng các dịch vụ công khác nhau./.

(Security Document World)

Anh: Google ra mắt chuông cửa tích hợp công nghệ nhận dạng khuôn mặt

Google sẽ tung ra một loại chuông cửa tích hợp công nghệ nhận dạng khuôn mặt, với tên gọi là Nest Hello, để cạnh tranh trực tiếp với sản phẩm Ring của Amazon tại thị trường Anh.

Ra mắt lần đầu ở Mỹ vào tháng 3, Nest Hello đóng vai trò tiên phong trong dòng sản phẩm bảo mật mới của Google tại "xứ sở sương mù". Tiếp đó, công ty sẽ ra mắt hệ thống báo động Nest Secure. Nest Hello là chuông cửa thông minh kết nối wifi, được trang bị máy ảnh góc rộng với khả năng quay video HDR độ nét cao mang lại hình ảnh rõ ràng ngay cả trong điều kiện ánh sáng yếu. Tuy nhiên, tính năng khác biệt của Nest Hello là công nghệ máy học để phân tích video. Google tuyên bố sản phẩm có thể phân biệt giữa những người đi ngang qua, bao gồm khách hoặc người giao hàng với kẻ trộm đang lảng vảng quanh đó để cảnh báo chủ nhà khi cần thiết.

Khi ai đó rung chuông, hệ thống sẽ gửi cảnh báo với hình ảnh từ máy ảnh đến điện thoại của chủ nhà, cho phép họ nói chuyện với khách từ bất kỳ nơi nào có kết nối Internet. Ngoài ra, Nest Hello còn có thể tự động phát những câu chào ngắn/.

(Planet Biometrics)

Trung Quốc phát hành thẻ ID điện tử thông qua mã QR trên smartphone

Hệ thống chính phủ điện tử của Trung Quốc sẽ sử dụng điện thoại thông minh (smartphone) và công nghệ mã QR để công dân có thể thoải mái quét khuôn mặt của họ.

Sự phổ biến của thanh toán di động tại Trung Quốc đang dần "giết chết" tiền mặt, và hiện nay xu hướng quét và chạm để thanh toán đã trở nên hết sức phổ biến tại quốc gia đông dân nhất thế giới.

Chính phủ Trung Quốc đã nhanh chóng chấp nhận công nghệ dựa trên smartphone nhằm đơn giản hóa các dịch vụ công, từ các yêu cầu trực tuyến cho đến hàng loạt ứng dụng và kênh chính phủ điện tử, thường được cung cấp trên các ứng dụng mạng xã hội phổ biến, không yêu cầu người dùng phải đến quầy xử lý thủ tục hoặc xếp hàng để điền vào biểu mẫu hoặc đơn đăng ký.

Hiện nay, chính quyền tỉnh Chiết Giang, địa phương dẫn đầu cả nước về hoạt động ứng dụng hệ thống chính phủ điện tử, đang phối hợp với AliPay triển khai dự án thí điểm phát hành thẻ ID điện tử.

Tân Hoa Xã cho biết mọi công dân Trung Quốc đều có thể đến kiosk tự phục vụ tại cơ quan công an địa phương, và quét khuôn mặt họ trước khi trả lời một vài câu hỏi bắt buộc. Chỉ vài phút sau, tấm thẻ ID điện tử - có giá trị pháp lý tương đương với thẻ ID vật lý - với mã QR duy nhất sẽ được gửi tới tài khoản AliPay của họ.

Trước đây, Trung Quốc yêu cầu các công dân của nước này xuất trình thẻ ID để xác thực khi nhận phòng tại khách sạn, lên tàu hoặc máy bay hay truy cập các dịch vụ của chính phủ.

Để đăng ký, người dùng chỉ cần đến kiosk tự phục vụ tại cơ quan công an địa phương, và quét khuôn mặt. Vài phút sau, hệ thống sẽ gửi thẻ ID điện tử và mã QR duy nhất đến smartphone của họ. Ảnh: Tân Hoa Xã

Với thẻ ID điện tử mới, người dùng có thể chỉ cần chạm vào ứng dụng AliPay để trình ra mã QR cá nhân nhằm xác thực danh tính, và có thể bỏ ví cũng như thẻ ID vật lý tại nhà.

Theo Tân Hoa Xã, việc mất điện thoại sẽ không khiến người dùng mất thẻ ID hay các dữ liệu cá nhân liên quan, bởi mọi bước từ việc khởi chạy ứng dụng AliPay cho đến nhận mã QR đều yêu cầu xác thực sinh trắc như quét vân tay hay khuôn mặt, sử dụng thiết bị đọc và camera trên smartphone.

Người dùng có thể đăng nhập vào ứng dụng AliPay bằng vân tay và quét khuôn mặt của họ để chuyển tất cả thông tin và cài đặt sang thiết bị mới./.

(Asia Times)

Mobile Vakten SDK của Keypasco - "Vạn lý trường thành" trước những cuộc tấn công thiết bị di động

Kỳ 2: Các hướng tấn công và biện pháp phòng thủ

1. Hướng tấn công số 1 - Root/Jailbreak

Quá trình truy cập vào hệ điều hành của máy, chiếm quyền điều khiển toàn bộ thiết bị Android được gọi là "root". Root mở ra khả năng xóa hoặc bổ sung bất cứ thứ gì và cấp quyền truy cập vào những chức năng mà nhà sản xuất mặc định ẩn đi đối với người dùng cuối. Trên thiết bị iOS, chiếm quyền truy cập root được gọi là "jailbreak", nhưng trong môi trường iOS, quy trình này thậm chí còn mang tính can thiệp nhiều hơn, thậm chí cho phép sửa đổi cả hệ điều hành của thiết bị.

Có một vài cách thức ẩn giấu hành vi root đối với thiết bị di động. Ứng dụng phần mềm smartphone có tên "RootCloak" hoặc "HideMyRoot" là công cụ đắc lực phục vụ cho thủ đoạn này. Dưới đây là một số ứng dụng không thể phát hiện quyền truy cập root khi " RootCloak" hoạt động.

- Mobile Pay của Apriva
- IKO của PKO Bank Polski SA
- Sparkasse của Star Finanz GmbH
- Barclays Mobile Banking của Barclays

Biện pháp bảo vệ của Keypasco: Với Mobile Vakten SDK, Hệ thống Keypasco có khả năng phát hiện hành vi "root" thiết bị trong mọi thời điểm. RootCloak, đã được chứng minh, luôn "bó tay" trước những thuật toán của Keypasco.

2. Hướng tấn công số 2 - Gỡ lỗi

Khi phát triển một ứng dụng smartphone, lập trình viên thường sử dụng trình gỡ lỗi để theo dõi luồng dữ liệu trong mã nguồn. Ngoài ra còn có các trình gỡ lỗi độc lập có thể hoạt động từ xa, mà không cần quyền truy cập trực tiếp vào thiết bị. Các ứng dụng Android được nén, đóng gói và phân phối dưới dạng tệp "*.apk", tương tự các tệp "*.jar" hoặc "*.zip". Tuy vậy, định dạng tệp apk không có bất kỳ hình thức bảo mật nào. APK có thể được sao chép hoặc trích xuất bằng phần mềm lưu trữ đơn giản, và mã nguồn được đã biên dịch có thể bị giải mã một cách dễ dàng bằng các công cụ mã nguồn mở và miễn phí như "APKTool" và "Dex2Jar".

Tất cả các trình gỡ lỗi đều cho phép đọc và ghi vào bộ nhớ. Đây là nơi tiềm ẩn các mối đe dọa. Trên thực tế, người ta có thể sử dụng kỹ thuật đảo ngược về mã nguồn trên mọi ứng dụng smartphone. Vì vậy, hacker có thể đính kèm trình gỡ lỗi vào đó. Khi sử dụng trình gỡ lỗi, kẻ gian sẽ tìm ra điểm yếu của ứng dụng, và với quyền truy cập vào smartphone, các khóa mã hóa chỉ tồn tại tạm thời trong bộ nhớ sẽ bị phát hiện và cho phép trích xuất dữ liệu đã bị khóa.

Biện pháp bảo vệ của Keypassco: Cơ chế giám sát thời gian hoạt động của Mobile Vakten SDK sẽ quét và phát hiện mọi hành vi gỡ lỗi ứng dụng đang chạy ở mức sâu nhất có thể. Tác vụ này được thực hiện mỗi khi gọi một chức năng của SDK nhằm liên tục bảo vệ tất cả dữ liệu của ứng dụng.

3. Hướng tấn công số 3 - Sao chép

Sao chép thiết bị là hoạt động copy tất cả các thuộc tính và bộ nhớ của thiết bị đó vào một thiết bị khác. Một cách sao chép thiết bị phổ biến là mô phỏng thiết bị đó - có nghĩa là người dùng không thực sự chèn dữ liệu vào thiết bị khác, mà là tạo ra một thiết bị ảo sở hữu các thuộc tính và nội dung bộ nhớ giống hệt thiết bị vật lý. Không có chương trình mô phỏng nào cho nền tảng iOS nguồn đóng, nhưng nhiều chương trình có thể bắt chước các thiết bị Android. Những chương trình này có thể mô phỏng hầu hết các máy tính bảng và smartphone hiện có trên thị trường.

Nhà cung cấp dịch vụ không ứng dụng công nghệ bảo mật bằng vân tay thiết bị, hoặc ứng dụng không đầy đủ, sẽ không thấy được sự khác biệt giữa thiết bị thực và bản sao mô phỏng của thiết bị đó.

Biện pháp bảo vệ của Keypassco: Các cơ chế phát hiện giả mạo của Mobile Vakten SDK sẽ dò tìm từng trình giả lập Android có sẵn. Sáu lớp vân tay thiết bị của Keypasco khiến cho những nỗ lực hòng tạo ra bản sao vật lý trở thành nhiệm vụ bất khả thi. Tuy nhiên, nếu kẻ tấn công có thể tạo một bản sao hoàn hảo ngay khi thiết bị gốc đang chạy, thì cả hai thiết bị đều sẽ bị khóa nhờ thuật toán dán nhãn ẩn của Keypasco.

4. Hướng tấn công số 4 - Chèn phần mềm độc hại (malware)

Hướng tấn công này bao gồm các công cụ như virus, sâu (worm), Trojan horse, mã độc tống tiền (ransomeware) và phần mềm gián điệp (spyware). Malware có thể ở dưới dạng mã thực thi, tập lệnh hoặc nội dung hoạt động, nhưng được thực hiện với mục đích xấu, trái ngược với mong muốn của người dùng.

Các thiết bị iOS thường trở thành mục tiêu của phần mềm độc hại. Hơn nữa, nguy cơ bị nhiễm malware không chỉ giới hạn ở những thiết bị iOS đã bị bẻ khóa (jailbreak). Năm 2016, giới chuyên môn đã phát hiện malware “AceDeceiver” có khả năng “miễn dịch” với các biện pháp bảo mật của Apple. Sau khi thâm nhập thành công vào thiết bị, phần mềm độc hại sẽ được sử dụng để đánh cắp mật khẩu và số tài khoản từ ĐTDĐ, tính phí giả trên tài khoản người dùng và thậm chí theo dõi vị trí và hoạt động của nạn nhân mà họ không hề hay biết.

Biện pháp bảo vệ của Keypasco: Phát hiện phần mềm độc hại vốn rất khó. Thông thường, malware ẩn trong một ứng dụng đầy đủ chức năng, thực hiện một tác vụ hữu ích, thí dụ như xử lý ảnh hoặc xóa các tệp không cần thiết khỏi hệ thống. Mobile Vakten SDK của Keypasco sẽ phát hiện ra các loại phần mềm độc hại khác nhau trong quá trình quét thiết bị giả mạo. Tuy nhiên, khi thiết bị di động bị nhiễm phần mềm độc hại, hacker cũng không thể tìm thấy thông tin gì để đánh cắp. Với Hệ thống Keypasco, mật khẩu, mã PIN, khóa.... không được lưu trữ trong bộ nhớ hoặc trên ổ đĩa.

5. Hướng tấn công số 5 - Thư viện thay đổi thông tin phần cứng của thiết bị

Nền tảng smartphone và thiết bị di động Android có sẵn một số thư viện. Các thư viện này không được coi là phần mềm độc hại bởi chúng không che giấu ý định. Tuy nhiên, mục đích của các thư viện này có thể được coi là đặc biệt nguy hiểm đối với mọi nhà cung cấp dịch vụ ứng dụng di động. Chẳng hạn như Thư viện Xposed cho phép người dùng thay đổi hầu hết mọi thuộc tính trên thiết bị sau khi được cài đặt.

Đối với các ứng dụng xác thực bằng vân tay của thiết bị, đây sẽ là cơn ác mộng. Các yếu tố nhận dạng tĩnh như IMEI, số seri ID, IMSI... đều có thể thay đổi được. Những thuộc tính này có thể khiến cho thiết bị trở nên khác biệt so với chính nó ở thời điểm ban đầu, hoặc y hệt như một thiết bị vật lý khác đã được định danh. Điều này có nghĩa là việc liệt kê thiết bị trong danh sách đen không còn là hình thức bảo vệ đáng tin cậy nữa, bởi một thiết bị bị liệt vào danh sách đen có thể thay đổi định danh sao cho giống với thiết bị không nằm trong danh sách đó.

Biện pháp bảo vệ của Keypasco: Công nghệ giám sát trong thời gian hoạt động của Mobile Vakten SDK luôn có khả năng phát hiện tất cả các thư viện nguy hiểm nói trên. Hơn nữa, các thư viện này không thể thao túng được vân tay thiết bị do Hệ thống Keypasco tạo ra và duy trì.

TỔNG KẾT

Chi tiết vân tay thiết bị: Điểm mạnh của giải pháp Keypasco không nằm ở dữ liệu thu thập và được cài đặt trên thiết bị di động, mà nằm ở các thuật toán xử lý dữ liệu thu thập được của Borgen. Giải pháp nâng cao khả năng bảo vệ vòng đời của các thuộc tính, theo đó thuộc tính nào được phép cập nhật theo điều kiện nào và thuộc tính nào cần được xem xét với mức độ quan trọng nào.

Ứng dụng vân tay thiết bị không phải là một nhiệm vụ đặc biệt khó khăn. Tuy nhiên, cần có vân tay thiết bị mạnh để xử lý tất cả các tình huống cập nhật và thay đổi trong suốt vòng đời của smartphone. Ngoài ra, sự đa dạng của các thương hiệu và mẫu mã khiến nhiệm vụ này càng trở nên khó khăn.

Vân tay thiết bị của Keypasco gồm nhiều cấp độ phân tích, bao gồm cả phần cứng, phần mềm, các thiết bị IoT gắn ngoài, những giá trị được chèn vào, vị trí, thuộc tính cố định, thuộc tính động và các thành phần khác. Góc nhìn toàn diện về thiết bị đảm bảo rằng với bất kỳ thương hiệu hoặc mẫu mã nào, nếu đã được ghi nhận vân tay, thiết bị sẽ được nhận diện mãi mãi.

Những hạn chế và điểm mạnh: Bộ phận R&D của Keypasco liên tục cập nhật công nghệ vân tay thiết bị, song như chúng ta đều biết, thông tin thu thập được trên mỗi nền tảng đều có giới hạn. Tuy vậy, điểm mạnh của Hệ thống Keypasco là khả năng phân tích dữ liệu từ tất cả các thiết bị của khách hàng. Với cách thức này, thiết bị bị liệt vào danh sách đen sẽ bị ngăn chặn ngay lập tức khi thực hiện các hoạt động gian lận với bất kỳ khách hàng nào.

Điểm mạnh của Mobile Vakten SDK là sẽ luôn phát hiện xem thiết bị có bị "root" hay không, thiết bị có cài phần mềm độc hại hay không, thiết bị có bị mô phỏng hay không và thiết bị có cài đặt thư viện cho phép can thiệp sâu hay không. Cuối cùng, Mobile Vakten SDK của Keypasco không lưu trữ bất kỳ thông tin đăng nhập, khóa hoặc mã nào trên thiết bị, do đó, hacker không thể phát hiện ra thông tin có giá trị để đánh cắp./.

Giới thiệu về Keypasco

Kể từ khi được ra mắt vào năm 2010, giải pháp Keypasco đã góp phần vào sự chuyển đổi mô thức trong lĩnh vực an ninh mạng. Giải pháp đã được cấp bằng sáng chế độc đáo của Keypasco sử dụng công nghệ mới mang tính cách mạng để xác thực người dùng, đồng thời nâng cao khả năng bảo mật cho nhà cung cấp dịch vụ trực tuyến và người dùng.

Giải pháp Keypasco mở ra cơ hội cho những mô hình kinh doanh sáng tạo mới và cho phép tạo ra các dịch vụ mới. Hiện nay, các sản phẩm của công ty công nghệ đến từ Thụy Điển đang mang lại khả năng bảo mật di động mạnh mẽ cho hàng triệu người dùng trên toàn thế giới.

MK® group

Smart Digital Security

www.mkgroup.com.vn | contact@mkgroup.com.vn | www.facebook.com.vn/mkgroup1999

Hà Nội: Tầng 11, tòa nhà TTC, 19 Duy Tân, Cầu Giấy | Tel: (+84-24) 6266 2703

Tp. Hồ Chí Minh: Tầng 7 Thiên Sơn Building, 5 Nguyễn Gia Thiều, Quận 3 | Tel: (+84-28) 3930 5023