KEYPASCO MOBILE VAKTEN SDK – "Vạn lý trường thành" trước những cuộc tấn công thiết bị di động

www.mkgroup.com.vn • contact@mkgroup.com.vn

"Trong kỷ nguyên công nghệ ngày nay, điện thoại thông minh (smartphone) đã trở thành công cụ thiết yếu, gắn liền với mọi hoạt động thường ngày như trao đổi thông tin, làm việc, giải trí, và đặc biệt là các giao dịch tài chính."

Trước sức hấp dẫn vô cùng mạnh mẽ này, giới hacker đã tạo ra hàng loạt thủ đoạn hòng đánh cắp thông tin tài khoản mà chủ thẻ tiến hành giao dịch qua thiết bị di động. Bởi vậy, trong cuộc đấu tranh bảo vệ chủ thẻ, các tổ chức tài chính cần phải cân nhắc đến những biện pháp chống lại các phương thức tấn công thiết bị di động.

Để tiếp thêm sự linh hoạt cho các tổ chức tài chính trong cuộc đấu tranh với những manh khóe của các hacker, Keypasco - công ty công nghệ nổi tiếng của Thụy Điển đã góp phần quan trọng vào sự chuyển đổi mô thức trong lĩnh vực an ninh mạng - đã sáng tạo ra giải pháp 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.

Sự độc đáo trong cách thức bảo vệ người dùng của Keypasco thể hiện qua cách thức sử dụng DeviceID trên chính thiết bị của người dùng cuối, như smartphone, máy tính bảng (tablet) hoặc máy tính để bàn/máy tính xách tay. Keypasco có thể đảm bảo rằng tên người dùng và mật khẩu chỉ hoạt động khi ở trên đúng thiết bị và ở đúng vị trí. Để đảm bảo trải nghiệm người dùng được diễn ra một cách thuận tiện, công nghệ tiên tiến của Keypasco hoạt động ở chế độ nền nhằm duy trì khả năng bảo mật phía sau giao diện ứng dụng thông thường của tổ chức tài chính.

Để mang lại góc nhìn tổng thể, các chuyên gia bảo mật đã điểm lại những hướng tấn công chủ yếu nhằm vào thiết bị di động và cách thức bảo vệ tương ứng của Keypasco.

Các thuật ngữ trong tài liệu:

- ***Borgen***
  - Tên máy chủ ứng dụng của Hệ thống Keypasco
  - Còn được gọi là "appnode" hoặc "Borgen appnode"
- ***Vakten***
  - Tên máy khách của Hệ thống Keypasco
  - Mobile Vakten SDK

Cách thức tấn công	Mối đe dọa	Biện pháp bảo vệ của Keypasco	Giám sát trong thời gian hoạt động / phát hiện giả mạo
Brute force (kỹ thuật đoán thử đúng sai liên tục) PIN hoặc mật khẩu	Phá vỡ khả năng xác thực	Ngăn chặn Brute force	
Bẻ mã PIN hoặc mật khẩu ngoại tuyến	Phá vỡ khả năng xác thực	Không lưu trữ bất kỳ mã PIN hoặc thông tin đăng nhập nào trên thiết bị	
Trích xuất OTP	Phá vỡ khả năng xác thực	Không sử dụng OTP ngoại trừ GeoOTP ở chế độ ngoại tuyến; phát hiện giả mạo nhằm trích xuất dữ liệu	X
Gỡ lỗi	Trích xuất dữ liệu và khóa	Khóa hoặc thông tin đăng nhập không được lưu trên thiết bị; phát hiện tất cả các trình gỡ lỗi	X
Tạo bản sao	Phá vỡ khả năng xác thực	Vân tay thiết bị (device fingerprint) sáu lớp ngăn cản việc sao chép dễ dàng; thuật toán bảo vệ chống tạo bản sao	
Root	Truy cập trái phép	Truy cập root sẽ bị phát hiện và không thể che giấu.	X
Bẻ khóa (Jailbreak)	Truy cập trái phép	Thủ đoạ bẻ khóa thiết bị sẽ bị phát hiện và không thể che giấu	X
Mô phỏng	Vân tay thiết bị không hoạt động được	Phát hiện mọi trình giả lập	X
Chèn phần mềm độc hại	Hành vi trái phép	Phát hiện phần mềm độc hại	X
Thư viện thay đổi thông tin phần cứng của thiết bị	Xâm phạm vân tay thiết bị	Phát hiện tất cả các thư viện	X
Truy cập bộ nhớ bảo mật	Phá vỡ khả năng xác thực	Không lưu khóa trên thiết bị	
Mở khóa trình khởi động trên Android	Truy cập trái phép	Phát hiện trình khởi động bị mở khóa	X
Tấn công lỗ hổng chưa được khắc phục (Zero day)	Phá vỡ khả năng xác thực	Tất cả các phiên bản iOS và Android mới được thử nghiệm ở giai đoạn beta, SDK được cập nhật trước bản phát hành cuối cùng	
Những hướng tấn công chưa được xác định rõ ở thời điểm hiện tại	Truy cập trái phép, phá vỡ khả năng xác thực, trích xuất dữ liệu...	Đội ngũ nghiên cứu và phát triển (R&D) của Keypasco liên tục tìm hiểu những mối đe dọa mới, cách thức giảm nhẹ và bảo vệ, các bản vá lỗi cho Mobile Vakten SDK được cung cấp trong vòng 24 giờ	

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.