|  |  |
| --- | --- |
| Posts__Telecoms_Institute_of_Technology_logo  **www.ptit.edu.vn** | HỌC VIỆN CÔNG NGHỆ BƯU CHÍNH VIỄN THÔNG  KHOA CÔNG NGHỆ THÔNG TIN |

**BÁO CÁO**

**MÔN HỌC**

**QUẢN LÝ AN TOÀN THÔNG TIN**

***Tên đề tài:* Đánh giá rủi ro hệ thống Bluezone**

**Giảng viên hướng dẫn : Phạm Hoàng Duy**

**Nhóm lớp : 04**

**Sinh viên thực hiện** :Nguyễn Mạnh Tâm : B17DCAT159

: Nguyễn Ngọc Bách: B17DCAT019

: Đỗ Mạnh Hùng: B17DCAT087

\ : Nguyễn Minh Tuệ: B17DCAT204

HÀ NỘI, 11/2020

**MỤC LỤC**

[I. Tổng quan về ứng dụng Bluzone 3](#_Toc56845959)

[A. Bluzone là ứng dụng gì ? 3](#_Toc56845960)

[B. Bluezone hoạt động thế nào ? 3](#_Toc56845961)

[C. Các nguyên tắc hoạt động phía Bluezone cung cấp: 4](#_Toc56845962)

[II. Phân tích Bluzone 4](#_Toc56845963)

[A . Phân tích tĩnh 4](#_Toc56845964)

[1. Đường dẫn phân tích "permalink" của Virus total : 4](#_Toc56845965)

[2. Các quyền cần thiết cho hoạt động của chương trình: 5](#_Toc56845966)

[III. Xác định các lỗ hổng và những mối đe dọa có thể xảy ra 6](#_Toc56845967)

[A. Lỗ hổng và các mối đe dọa có thể xảy ra 8](#_Toc56845968)

[1. Dữ liệu nhạy cảm bị đánh cắp trên đường truyền (Ensure sensitive data is protected in transit) 8](#_Toc56845969)

[2. Bluezone có thể bị nhiễm mã độc ẩn trong các file cá nhân của người dùng(Secure data integration with third party services and applications) 9](#_Toc56845970)

[3. Nguy cơ dữ liệu của người dùng bị phát tán khi sử dụng Bluezone(Pay specific attention to the collection and storage of consent for the 11](#_Toc56845971)

[4. Người dùng quản lí thiết bị không tốt, dễ bị hack, chiếm quyền điều khiển, đọc ghi dữ liệu. 12](#_Toc56845972)

[5. Thiết bị nằm ngoài sự hỗ trợ của Google, không thỏa mãn sự tương thích của hệ điều hành mà ứng dụng yêu cầu. 13](#_Toc56845973)

[6. Người dùng cố tình sửa, thay đổi dữ liệu, cấu trúc chương trình 14](#_Toc56845974)

[7. Sử dụng một mã ID duy nhất 15](#_Toc56845975)

[8. Tập trung dữ liệu một chỗ dẫn đến có được đồ thị tiếp xúc xã hội 17](#_Toc56845976)

[9. Nguy cơ bị chơi xấu bằng việc thu thập tín hiệu BLE 18](#_Toc56845977)

[10. Số lượng người cài đặt ứng dụng không đủ để phát huy hiệu quả của ứng dụng. 20](#_Toc56845978)

[11. F0,F1,F2 có thể bị làm giả 21](#_Toc56845979)

[12. Cung cấp quyền Camera cho ứng dụng BZ 22](#_Toc56845980)

[IV. KẾT LUẬN 23](#_Toc56845981)

Tổng quan về ứng dụng Bluzone

1. Bluzone là ứng dụng gì ?

* Bluezone là một ứng dụng do Cục Tin Học Hóa thuộc Bộ Thông tin và Truyền thông phối hợp với Bộ Y tế Việt Nam phát hành chỉ dành riêng cho Android và iOS nhằm truy vết tiếp xúc và cảnh báo người nhiễm COVID 19 bằng cách sử dụng giao thức BLE. Ứng dụng được phát triển bởi Công ty cổ phần BKAV, và được giới thiệu và phát hành vào ngày 18 tháng 4 năm 2020 bởi Bộ Thông tin và Truyền thông và Bộ Y tế Việt Nam

1. Bluezone hoạt động thế nào ?

****

**Hình 1. Cách thức hoạt động của bluzone.**

* Các smartphone cài ứng dụng Bluezone có thể giao tiếp với nhau trong khoảng cách 2m, ghi nhận sự tiếp xúc gần vào lúc nào và trong bao lâu. Khi có một ca nhiễm SARS-CoV-2 mới, cơ quan y tế nhập dữ liệu F0 này lên hệ thống. Hệ thống sau đó gửi dữ liệu F0 đến các smartphone khác cài ứng dụng Bluezone. Lịch sử tiếp xúc với F0 trong 14 ngày trước đó sẽ được phân tích, đối chiếu và nếu trùng khớp, ứng dụng Bluezone sẽ cảnh báo cho người dùng có nguy cơ lây nhiễm, đồng thời hướng dẫn họ liên hệ với cơ quan Y tế để nhận trợ giúp.

1. Các nguyên tắc hoạt động phía Bluezone cung cấp:

* **Bảo mật dữ liệu**: Ứng dụng chỉ lưu dữ liệu lịch sử tiếp xúc trên máy của bạn, không chuyển lên hệ thống. Khi cài đặt Bluezone, bạn được khuyến khích đăng ký thông tin liên lạc (tên, số điện thoại, địa chỉ) để nhận được sự hỗ trợ trực tiếp trong trường hợp bạn bị nhiễm COVID-19 hoặc tiếp xúc gần với người nhiễm COVID-19.
* **Không thu thập vị trí**: Ứng dụng không thu thập dữ liệu về vị trí của bạn.
* **Ẩn danh**: Mọi người tham gia cộng đồng ẩn danh với những người khác. Chỉ cơ quan Y tế cóthẩm quyền mới có thể biết những người nhiễm và nghi nhiễm do tiếp xúc gần với người nhiễm SARS-CoV-2.
* **Minh bạch**: Mã nguồn của dự án được phân phối theo giấy phép GNU GPL v3. Người dùng các nước trên Thế giới được tự do tìm hiểu hoạt động hệ thống ở mức mã nguồn, được tự do sử dụng, nghiên cứu, sửa đổi và chia sẻ.

Phân tích Bluzone

A . Phân tích tĩnh

Dưới đây là những thông số mà chúng tôi có được sau khi đưa bluzone vào AndroPyTool để phân tích

1. Đường dẫn phân tích "permalink" của Virus total :

"https://www.virustotal.com/gui/file/af40bf32ade2342ad3b07f8cd87420ab9583354e1e49c2f1981895751ac48b1c/detection/f-af40bf32ade2342ad3b07f8cd87420ab9583354e1e49c2f1981895751ac48b1c-1600873331",

|  |  |  |  |
| --- | --- | --- | --- |
|  | **Nhiều nhất** | **Ít nhất** | **Tổng** |
| **API** | "invoke-virtual"  92429 lần | "rem-double"  1 lần | 208 |
| **OPCODE** | "java.lang.StringBuilder": 17173 lần | "android.widget.TextView.getCompoundPaddingTop" 1 lần | 5291 |

1. Các quyền cần thiết cho hoạt động của chương trình:

android.permission.ACCESS\_FINE\_LOCATION

android.permission.BLUETOOTH

android.permission.BLUETOOTH\_ADMIN

android.permission.INTERNET

com.mic.bluezone.permission.C2D\_MESSAGE

android.permission.ACCESS\_BACKGROUND\_LOCATION

android.permission.ACCESS\_NETWORK\_STATE

android.permission.ACCESS\_WIFI\_STATE

android.permission.FOREGROUND\_SERVICE

android.permission.READ\_APP\_BADGE

android.permission.RECEIVE\_BOOT\_COMPLETED

android.permission.REQUEST\_IGNORE\_BATTERY\_OPTIMIZATIONS

android.permission.REQUEST\_INSTALL\_PACKAGES

android.permission.VIBRATE

android.permission.WAKE\_LOCK

com.anddoes.launcher.permission.UPDATE\_COUNT

com.android.vending.CHECK\_LICENSE

com.google.android.c2dm.permission.RECEIVE

com.google.android.finsky.permission.BIND\_GET\_INSTALL\_REFERRER\_SERVICE

com.htc.launcher.permission.READ\_SETTINGS

com.htc.launcher.permission.UPDATE\_SHORTCUT

com.huawei.android.launcher.permission.CHANGE\_BADGE

com.huawei.android.launcher.permission.READ\_SETTINGS

com.huawei.android.launcher.permission.WRITE\_SETTINGS

com.majeur.launcher.permission.UPDATE\_BADGE

com.oppo.launcher.permission.READ\_SETTINGS

com.oppo.launcher.permission.WRITE\_SETTINGS

com.sec.android.provider.badge.permission.READ

com.sec.android.provider.badge.permission.WRITE

com.sonyericsson.home.permission.BROADCAST\_BADGE

com.sonymobile.home.permission.PROVIDER\_INSERT\_BADGE

me.everything.badger.permission.BADGE\_COUNT\_READ

me.everything.badger.permission.BADGE\_COUNT\_WRITE

* Cùng với các thông số dịch vụ, thư viện lập trình,… được nhà phát hành sử dụng trong quá trình phát triển ứng dụng Bluezone.Trong dó ta thấy rất nhiều dịch vụ, thư viên,… của các bên thứ 3 như google, Huawei,… có thể kể đến như cơ sở dữ liệu Fire base,…

Xác định các lỗ hổng và những mối đe dọa có thể xảy ra

* Đối với mỗi ứng dụng sẽ luôn tiềm ẩn rất nhiều mối nguy hiểm đe dọa đến ứng dụng đó, cũng như bản thân người sử dụng, mối đe dọa có thể nhắm đến các thông tin, tài nguyên hệ thống, dữ liệu quan trọng từ mức độ cá nhân và rộng hơn là quốc gia. Bluezone cũng không phải là một ngoại lệ, ứng dụng này đã và đang tiềm ẩn rất nhiều những lỗ hổng, mối đe dọa – là cơ hội tốt cho kẻ xấu (hacker) lợi dụng mưu cầu chuộc lợi, hành động phi pháp, những mối đe dọa có thể xuất phát từ cách sử dụng phía người dùng và những lỗ hổng trong quá trình phát triển ứng dụng. Bản thân là một phần mềm đang được sử dụng rộng dãi với hơn 20 triệu lượt tài và sẽ còn tiếp tục tăng, thì những mối đe dọa này sẽ còn nguy hiểm và đáng báo động hơn bao giờ hết.
* Và dưới đây là những lỗ hổng mà chúng mình đã tìm kiếm, phân tích, cũng như những các mối đe dọa có thể xảy ra nếu những lỗ hổng đó không được khắc phục kịp thời.

Các lỗ hổng dưới đây được chúng mình đưa ra và đánh giá dựa theo chuẩn NIST SP 800-30 công bố vào tháng 9 năm 2012

|  |  |  |  |
| --- | --- | --- | --- |
| Mức độ nguy hiểm | Số điểm ước lượng | | Mô Tả |
| Rất Cao | 96-100 | 10 | Các tổ chức đối lập gần như **chắc chắn** sẽ thực hiện **tấn công** |
| Cao | 80-95 | 8 | Các tổ chức đối lập **có khả năng cao** sẽ thực hiện **tấn công** |
| Trung bình | 21-79 | 5 | Các tổ chức đối lập **có phần nào** **khả năng** thực hiện **tấn công** |
| Thấp | 5-20 | 2 | Các tổ chức đối lập có **ít khả năng** thực hiện **tấn công** |
| Rất thấp | 0-4 | 0 | Các tổ chức đối lập **không có hứng thú** với việc **tấn công** |

**Bảng 2: Đánh giá khả năng bị tấn công**

|  |  |  |  |
| --- | --- | --- | --- |
| Mức độ nguy hiểm | Số điểm ước lượng | | Mô Tả |
| Rất Cao | 96-100 | 10 | Các mối nguy mất án toàn có thể **gây ra nhiều tác động bất lợi nghiêm trọng** đối với hoạt động và tài sản cá nhân, tổ chức ,những tổ chức liên quan hoặc quốc gia |
| Cao | 80-95 | 8 | Các mối nguy mất an toàn có thể gây ra **một số tác động nghiêm trọng** đối với hoạt động và tài sản của cá nhân tổ chức thậm chí là quốc gia  Ví dụ : -Gây gián đoạn dịch vụ,ảnh hưởng tới hoạt động của tổ chức  -Gây thiệt hại lớn về kinh tế  -Gây thiệt hại lớn về tài sản… |
| Trung bình | 21-79 | 5 | Các mối nguy mất an toàn **có thể đoán được trước** sẽ gây ra **một số tác động bất lợi nghiêm trọng** |
| Thấp | 5-20 | 2 | Các mối nguy mất an toàn **có thể đoán được trước** sẽ gây ra **một số tác động bất lợi nhỏ** |
| Rất thấp | 0-4 | 0 | Các mối nguy mất an toàn sẽ gây ra **một số tác động bất lực không đáng kể** |

**Bảng 3: Đánh giá mức độ thiệt hại có thể xảy ra**

1. Lỗ hổng và các mối đe dọa có thể xảy ra
2. Dữ liệu nhạy cảm bị đánh cắp trên đường truyền (Ensure sensitive data is protected in transit)

B1: Đặc điểm hệ thống

* Dữ liệu nhạy cảm

B2: Xác định đe dọa

* Rủi ro: xảy ra trên đường truyền dữ luyện giữa user và ứng dụng.
* Nguyên nhân : là do phần lớn điện thoại thông minh có khả năng sử dụng nhiều cơ chế mạng khác nhau Wifi, 3G, GSM, CDMA, BlueTooth,…
* Bên cạnh đó, khi sử dụng BlueZone, user được khuyến khích liên tục bật BlueTooth. Ứng dụng BZ cũng có quyền truy cập vào mạng wifi.Dữ liệu nhạy cảm của người dùng khi đi qua các kênh truyền này có thể không an toàn, hoặc bị tấn công.
* Nguồn đe dọa: Con người, kênh truyền dữ liệu

B3: Xác định lỗ hổng:

* Attacker nếu vào được mạng truyền dữ liệu của người sử dụng. Kế tiếp sẽ lấy trộm thông tin của người sử dụng.
* Việc gửi mật khẩu hay mã ID qua SMS có thể bị Attacker chiếm được.

B4: Phân tích kiểm soát:

* Hiện thời: Kiểm tra xem BlueZone sử dụng mạng lưới truyền dữ liệu giữa người dùng và ứng dụng có an toàn hay không
* Kiểm tra các thông tin được truyền qua lại có sử dụng mã hóa không. Nếu có thì mã hóa đó có tốt không.
* Sắp tới: sử dụng các kênh truyền an toàn, cơ chế mã hóa mạnh.

B5: Xác định mức độ chắc chắn

* Thấp
* Các biện pháp kiểm soát ngăn chặn đáng kể việc khai thác lỗ hổng:
* Các mạng truyền dữ liệu bây giờ đã khá là an toàn bảo mật, rất khó cho attacker có thể lấy được dữ liệu trên đường truyền.

B6: Phân tích tác động

* Cao
* BlueZone là 1 ứng dụng mang tính chất quốc gia, được khuyến nghị sử dụng đối với nhân dân cả nước và được quảng bá ở trên rất nhiều phương tiện đại chúng nên nếu BZ bị tấn công ở trên đường truyền như vậy thì sẽ lộ rất nhiều thông tin của user.
* Làm ảnh hướng tới danh tiếng của bộ thông tin truyền thông, và các đơn vị tham gia xây dựng ứng dụng BlueZone.

B7: Xác định rủi ro

* Thấp
* Vì BlueZone là 1 ứng dụng chống dịch của 1 quốc gia nên khó có thể mắc phải lỗ hổng này.

B8: Khuyến nghị các biện pháp kiểm soát

* Sử dụng các cơ chế mã hóa dữ liệu có độ an toàn cao
* Sử dụng các kênh bảo mật end-to-end chẳng hạn như SSL, TLS, STS,…

1. Bluezone có thể bị nhiễm mã độc ẩn trong các file cá nhân của người dùng(Secure data integration with third party services and applications)

B1: Đặc điểm hệ thống

* Các dữ liệu chứa mã độc.

B2: Xác định mối đe dọa

* Rủi ro: Dữ liệu khác ở trong thiết bị của user .
* Nguyên nhân: Xảy ra ở phía dữ liệu cá nhân của người dùng khi mà BZ có yêu cầu quyền truy cập vào các file cá nhân trên điện thoại: ảnh, tài liệu, danh bạ,…
* Nguồn đe dọa: Con người, dữ liệu phía user.

B3: Xác định lỗ hổng

* Attacker có thể cài đặt sẵn trong máy những tệp tin tài liệu, những tập ảnh có chứa mã độc, khi Bluzone truy cập vào có thể bị nhiễm ngược mã độc rồi truyền tải lên server.
* Khi mã độc đã lên server thì có thể khiến cho Bluezone bị tấn công. Tấn công như nào còn tùy thuộc vào mục đích xấu của attacker và mã độc được truyền tải.

B4: Phân tích kiểm soát

* Hiện thời:Kiểm tra xem khi truy cập vào các file tài liệu như vậy, Bluezone có cơ chế rà quét hay phát hiện các file mà trong đó có gì khác thường hay không.
* Sắp tới: Thêm các cơ chế rò quét, phát hiện mạnh để tránh việc Bluezone bị nhiễm ngược lại mã độc từ phía người dùng.

B5: Xác định mức độ chắc chắn

* Thấp
* Các biện pháp kiểm soát ngăn chặn đáng kể việc khai thác lỗ hổng:
* Việc cài cắm trong các file cá nhân của người dùng mobile android/ios có những mã độc phức tạp có thể gây nguy hiểm ngược trở lại phía Bluezone là rất khó, đòi hỏi trình độ cực cao.
* Những mã độc như vậy sẽ có kích thước nặng hơn bình thường nên Bluezone có thể sẽ dễ dàng phát hiện được những file đó khác thường.

B6: Phân tích tác đông

* Cao
* Nếu kịch bản trên xảy ra thì phía máy chủ server có thể bị tân công, gây thiệt hại về nhiều loại tài sản: dữ liệu người dùng, tài sản của Bluezone,… thời gian, tính sẵn dùng của hệ thống ứng dụng.

B7: Xác định rủi ro

* Thấp
* Bluezone khó có thể bị mắc vấn đề này.

B8: Khuyến nghị các biện pháp kiểm soát

* Kiểm tra tính bảo mật, tính xác thực của bất kỳ code hoặc các libraries của bất kỳ bên thứ ba nào.

1. Nguy cơ dữ liệu của người dùng bị phát tán khi sử dụng Bluezone(Pay specific attention to the collection and storage of consent for the

collection and use of user’s data)

B1: Đặc điểm hệ thống

* Dữ liệu cá nhân của user ở phía Bluezone.

B2: Xác định mối đe dọa

* Rủi ro: User lo sợ dữ liệu của mình được sử dụng sai mục đích.
* Nguyên nhân: Bluezone là ứng dụng được truyền thông khuyến khích sử dụng trên phạm vi toàn dân, toàn quốc. Lượng thông tin thu thập được là rất lơn.
* Nguồn đe dọa: Con người.

B3: Xác định lỗ hổng

* Cơ quan, tổ chức, đội ngũ quản lý ở phía server sử dụng thông tin sai mục đích

B4: Phân tích kiểm soát

* Hiện thời: Có những chính sách và luật pháp mang tính răn đe nặng đối với cơ quan, tổ chức, đội ngũ quản lý ở phía server của BZ. Gắn trách nhiệm cụ thể để tránh trường hợp đùn đẩy, chối bỏ trách nhiệm cho nhau trong trường hợp xấu xảy ra.
* Sắp tới: Truyền thông với toàn thể nhân dân rằng thông tin sẻ chỉ sử dụng trong mục đích phòng dịch. Không lưu trữ thêm nếu hết dịch. Tạo các chính sách đền bù thiệt hại nếu có trường hợp xấu xảy ra nhằm tăng niềm tin sử dụng ứng dụng của mọi người.

B5: Xác định độ chắc chắn

* Vừa
* Việc quản lý thông tin này đều là do con người.
* Đây là lượng thông tin rất lớn và cực kỳ quý giá. Giá trị rất cao, nếu không có các chính sách luật pháp răn đe đủ mạnh thì có thể bị lộ hoặc sử dụng sai mục đích chống dịch.
* BlueZone là 1 ứng dụng mang tính chất quốc gia. Đội ngũ xây dựng đều là các bộ quan trọng như bộ y tế, bộ thông tin và truyền thông. Thông tin của người dân có lẽ sẽ được đảm bảo ở bên phía server.

B6: Phân tích tác động

* Thấp
* Nước ta đã ban hành ra rất nhiều luật, chính sách về an ninh mạng nhằm bảo vệ thông tin của người dùng. Nên cơ quan, tổ chức ở phía Bluezone hoàn toàn có thể nắm rõ được điều đó. Mặt khác, đây là ứng dụng được quan tâm nhất trên toàn quốc nên người sử dụng có thể yên tâm về dữ liệu cá nhân của mình trong quá trình tham gia sử dụng Bluezone.

B7: Xác định rủi ro

* Vừa
* Rủi ro là hoàn toàn có thể nhưng ứng dụng BZ rất là đặc biệt trong bối cảnh nhà nước chống dịch nên nhân dân hoàn toàn có thể tin tưởng Bluezone.

B8: Khuyến nghị các biện pháp kiểm soát

* Tạo chính sa
* Xây dựng khung pháp lý, ban hành các luật chính sách nghiêm cấm và xử phạt nặng đối với cơ quan lưu trữ thông tin của BZ nhằm ngăn cản yếu tố con người thực thi hành động

1. Người dùng quản lí thiết bị không tốt, dễ bị hack, chiếm quyền điều khiển, đọc ghi dữ liệu.

B1: Đặc điểm hệ thống :

* Dữ liệu cá nhân của user

B2: Xác định mối đe dọa :

* Người dùng quản lí thiết bị không tốt, dễ bị hack, chiếm quyền điều khiển, đọc ghi dữ liệu.

B3: Xác định lỗ hổng :

* Dữ liệu được ghi ở máy người dùng mà không đẩy lên server.

B4: Phân tích kiểm soát :

* Tham khảo một số cách bảo vệ dữ liệu hợp lý.
* Không cài những chương trình độc hại để tránh việc làm giả dữ liệu
* Sắp tới: Khuyến cáo người dân về phần mềm không rõ nguồn gốc, độc hại

B5: Xác định mức độ chắc chắn:

* Mức độ chắc chắn là CAO
* Nguy cơ mất dữ liệu nếu không có cơ chế bảo vệ kĩ càng khỏi những

B6: Phân tích tác động:

* Tác động CAO: Đa số người dùng chưa có ý thức về những phần mềm an toàn cũng như tải các ứng dụng trên trang uy tín, đã được cấp phép những chứng chỉ tin cậy.

B7: Xác định rủi ro:

Rủi ro = Tác động x Độ chắc chắn.

* Độ chắc chắn là cao nhưng tác động lại vừa, đề ra bài toán quản lý dữ liệu cho mỗi cá nhân sử dụng ứng dụng.

B8: Khuyễn nghị các biện pháp kiểm soát

* Đảm bảo mã hóa tốt cũng như có cơ chế kiểm soát những dữ liệu nhạy cảm này một cách hiệu quả.
* Đưa ra những phương án chống lại những phần mềm độc hại cho máy người sử dụng ứng dụng.

1. Thiết bị nằm ngoài sự hỗ trợ của Google, không thỏa mãn sự tương thích của hệ điều hành mà ứng dụng yêu cầu.

B1: Đặc điểm hệ thống :

* Hệ thống ứng dụng Bluezone

B2: Xác định mối đe dọa :

* Thiết bị nằm ngoài sự hỗ trợ của Google, không thỏa mãn sự tương thích của hệ điều hành mà ứng dụng yêu cầu.

B3: Xác định lỗ hổng :

* Thiết bị của Huawei không còn được Google hỗ trợ.

B4: Phân tích kiểm soát :

* Phát triển, nâng cấp ứng dụng để smart phone nào cũng có thể sử dụng.

B5: Xác định mức độ chắc chắn:

* Mức độ chắc chắn là CAO
* Nguy cơ cao những phần mềm bluezone mà những thiết bị này tải về dễ gây nên những tình trạng mất an toàn cao do không được Google kiểm soát.

B6: Phân tích tác động:

* Tác động VỪA: Thiết bị của Huawei không được bán ra nhiều tại Việt Nam nên mắc ảnh hưởng đến tình hình chống dịch chung là không cao.

B7: Xác định rủi ro:

* Độ ch chắn cao và tác động lớn: Đây là một vấn đềớn đối với tổ chức sản xuất ứng dụng. Đặt ra nhiều bài toán khác nhau để đối phó với các mối đe dọa

B8: Khuyễn nghị các biện pháp kiểm soát

* Khuyến khích chuyển đổi thiết bị Huawei không được Google hỗ trợ sang những thiết bị được hỗ trợ và đáp ứng với mức tương thích ứng dụng
* Thực hiện phổ cập smartphone toàn dân để nâng cao độ phủ sóng của những thiết bị thông minh

1. Người dùng cố tình sửa, thay đổi dữ liệu, cấu trúc chương trình

B1: Đặc điểm hệ thống :

* Dữ liệu thống ứng dụng Bluezone trên máy người dùng

B2: Xác định mối đe dọa :

* Thiết Người dùng cố tình sửa, thay đổi dữ liệu, cấu trúc chương trình.

B3: Xác định lỗ hổng :

* Quyền truy cập ứng dụng, máy ảnh bộ sưu tập vẫn được yêu cầu cả khi bluezone không cần đến.

B4: Phân tích kiểm soát :

- Hiện thời:

- Không sử dụng các quyền nhằm thu thập thông tin cá nhân

- Sắp tới:

- Kiểm soát chặt chẽ mã nguồn ứng dụng

- Hạn chế những tác động kích hoạt quyền ko cần thiết

B5: Xác định mức độ chắc chắn:

* Mức độ chắc chắn VỪA:
* Tuy theo công bố của BKAV rằng họ không dùng đến các quyền này nhưng khi phát hiện F0 thì dữ liệu tự động gửi lên mà ko cần yêu cầu chấp nhận từ phía người dùng.

B6: Phân tích tác động:

* Tác động CAO: Quyền riêng tư cá nhân trên không gian mạng đòi hỏi những ứng dụng này cần có một cơ chế cấp quyền minh bạch và những lời giải thích rõ ràng. Nếu không sẽ gây ảnh hưởng đến tâm lý người dân cũng như ảnh hưởng đến công tác phòng dịch chung.

B7: Xác định rủi ro:

* Độ chắc chắn cao và tác động cao, điều này chỉ ra trách nhiệm lớn thuộc về đội ngũ phát triển. Đề ra bài toán phân quyền ứng dụng sao cho không tồn tại những nghi ngờ tác động đến dữ liệu nhạy cảm.

B8: Khuyễn nghị các biện pháp kiểm soát

* Sửa đổi các quyền không cần thiết
* Quản lí tốt cũng như đặt ra những cơ chế cấp quyền phù hợp
* Rà soát những lỗi tồn đọng trong ứng dụng, cập nhật thường xuyên từ những phản hồi của người dùng.

1. Sử dụng một mã ID duy nhất

B1: Đặc điểm hệ thống

* Dữ liệu hệ thống bluezone

B2: Xác định đe dọa

* Rủi ro: Người sử dụng không thể thay đổi mã số này, trừ khi xóa và cài lại ứng dụng. Cách làm không giống ai này khiến **người sử dụng có thể bị theo dõi, bị lộ thông tin vị trí, hành trình, đã gặp ai, có bị nhiễm hay phơi nhiễm hay không**.
* Nguyên nhân : Bluezone sử dụng sóng Bluetooth để phát và thu mã số ngẫu nhiên. Thay vì liên tục thay đổi mã số ngẫu nhiên như các giải pháp của Singapore, Châu Âu hay Google/Apple, mỗi người sử dụng Bluezone chỉ có một mã số duy nhất, gọi là mã ID Bluezone
* Nguồn đe dọa : Tất cả những người dùng bluezone

B3: Xác định lỗ hổng:

* Sử dụng một mã ID duy nhất, cách làm của Bluezone khiến người dùng có nguy cơ bị theo dõi, bị lộ thông tin về danh tính, địa điểm, hành trình duy chuyển, đã gặp ai, vào lúc nào, ở đâu và có nhiễm bệnh hay không

B4: Phân tích kiểm soát:

* Tạm dừng ứng dụng bluezone, sửa chữa lỗ hổng sau đó mới cho tiếp tục phát hành lại
* Thay đổi việc sử dụng một mã ID duy nhất bằng cách cho tự động thay đổi mã ID một vài phút.

B5: Xác định mức độ chắc chắn

* Cao
* Vì mã số Bluezone ID chỉ có 6 chữ số và được hiển thị ngay trên màn hình ứng dụng, nó có thể bị nhìn trộm.
* Vì mã số được tạo dựa vào thời gian, nếu ai biết khoảng thời gian anh A cài ứng dụng (vì họ mời anh A cài) họ sẽ có thể khoanh vùng mã số của anh ấy. Đó là chưa kể đa số người dùng sẽ không hiểu mã số này có ý nghĩa gì, họ có thể vô tình chia sẻ hoặc bị người khác lừa tiết lộ mã số.

B6: Phân tích tác động

* Cao
* Việc Bluezone ID rơi vào tay kẻ xấu là vô cùng nguy hiểm bởi chúng có thể thực hiện được rất nhiều hành vi gây tổn đến cả bản thân người sử dụng hay thậm chí các cơ quan tổ chức có liên quan, và cao hơn nữa là đất nước nên đây có thể coi là một trong những lỗ hổng nguy hiểm bậc nhất của Bluezone nên nó gây tác động không hể nhỏ
* Giải pháp của Bluezone khiến điện thoại của bạn liên tục phát đi một mã số cố định, thông báo cho thế giới xung quanh biết bạn đang ở đâu, làm gì, vào lúc nào, với ai. Đây là những thông tin cá nhân cực kỳ nhạy cảm. Để bảo vệ những thông tin này, các giải pháp trên thế giới phát ra nhiều mã số. Bluezone không thể làm khác.

B7: Xác định rủi ro

* CAO
* Người sử dụng có thể bị theo dõi, bị lộ thông tin vị trí, hành trình, đã gặp ai, có bị nhiễm hay phơi nhiễm hay không.
* Bluezone nói rằng mã số không tiết lộ danh tính người dùng, điều này chỉ đúng khi mã số được thay đổi liên tục. Khi chỉ có một mã số duy nhất, danh tính rất dễ bị lộ
* Bluezone đã không còn sử dụng một ID duy nhất, mà đã tự động thay đổi ID mỗi vài phút. Ngoài ra, Bluezone cũng đã không còn thu thập địa chỉ Bluetooth Classic nữa
* Nhưng chúng mình khuyến cáo những người dừng trước đây còn đang sử dụng phần mềm cũ, hay xóa đi và tải lahi ngay bản cập nhật mới nhất từ phía bluzone công bố

B8: Khuyến nghị các biện pháp kiểm soát

* Sử dụng phương pháp thay đổi id liên tục là điều mà bluezone không thể làm khác
* Thay đổi mã id mỗi phút là cách làm mà nhiều nước trên thế giới áp dụng để bảo vệ thông tin người dùng

1. Tập trung dữ liệu một chỗ dẫn đến có được đồ thị tiếp xúc xã hội

B1: Đặc điểm hệ thống

* Các dữ liệu sau khi lấy về và xử lí phía bên bluezone.

B2: Xác định mối đe dọa

* Rủi ro: kẻ xấu có được đồ thị tiếp xúc xã hội
* Nguyên nhân: Tập trung tất cả dữ liệu ở một chỗ để xử lí
* Đối tượng bị đe dọa: Tất cả nhưng người dùng bluezone, nguy hiểm hơn là các quan trức cấp cao,…

B3: Xác định lỗ hổng

* Đây là một lỗ hổng bên phía có thể là nhà nước, tổ chức y tế, hay phía bluezone, bất kể cơ quan, tổ chức nào đứng ra tập trung và xử lí giữ liệu đều có thể gặp phải

B4: Phân tích kiểm soát

* Hiện thời: Hiện tại chưa có giải pháp cụ thể nào được bluezone đưa ra cho việc này
* Mới đây Bluezone đã đưa ra nhiều cam kết để trấn an người dùng, như “Úng dụng chỉ lưu dữ liệu trên máy của bạn, không chuyển lên hệ thống”, hoặc “Mọi người tham gia cộng đồng ẩn danh với những người khác. Chỉ cơ quan Y tế có thẩm quyền mới có thể biết những người nhiễm và nghi nhiễm do tiếp xúc gần với người nhiễm COVID-19”. Tuy nhiên, vẫn chưa có một cơ chế nào để giám sát việc thực hiện các cam kết đó.
* Nên để đảm bảo kiểm soát được phần nào việc này cần có những cơ chế, chế tài xử lí rõ ràng với những đối tượng sử dụng trái phép thông tin dữ liệu thu thập được vào mục đích xấu, cũng như thành lập cơ quan, tổ chức đủ tín nhiệm giám sát việc này
* Nhưng mình biết đây nằm nhiều ở phần con người nên việc này khó mà có thể giải quyết một cách hoàn toàn, triệt để mà chỉ phần nào

B5: Xác định mức độ chắc chắn

* Thấp
* Cũng như mình đã nói ở trên điều này nằm ở khâu xử lí thông tin của bluzone, và phần nhiều là cách mà bluezone bảo vệ dữ liệu ra sao và làm sao để đảm bảo không bị lạm quyền

B6: Phân tích tác đông

* Tuy mức độ chắc chắn là thấp nhưng mức độ tác động của nó thì không hề nhỏ
* Vì đồ thị tiếp xúc sẽ cho biết biết được ai đã gặp ai, trong bao lâu, vào lúc nào. Từ thông tin này có thể suy ra được ai quen ai, tức đồ thị tiếp xúc xã hội của phần lớn quan chức và dân chúng. Đây là thông tin rất nhạy cảm.Từ đó kẻ xấu sẽ lợi dụng điều đó và dễ dàng thực hiện hành vi xấu crua mình như tống tiền, lạm quyền, sử dụng những thông tin nạy cảm để ép buộc ai đó phải làm gì theo ý mình nếu không chúng sẽ được phát tán, nếu điều đó xảy ra với một quan chức cấp cap của nhà nước không phải sẽ rất nguy hiểm sao.

B7: Xác định rủi ro

* Thấp
* Bluezone là một phần mềm thuộc quyền sở hữa Bộ TT&TT nên việc dữ liệu được đảm bảo, và bảo vệ cũng sẽ được đảm bảo phần nào .

B8: Khuyến nghị các biện pháp kiểm soát

* Chính phủ có thể ban hành nghị định ghi rõ dữ liệu Bluezone chỉ dùng để chống dịch, sẽ được xóa trong bao nhiêu ngày kể từ khi Việt Nam tuyên bố hết dịch, rồi thuê hoặc chỉ định một cơ quan giám sát độc lập. Dân càng tin tưởng thì Chính phủ phải càng minh bạch, có vậy mới bền lâu được

1. Nguy cơ bị chơi xấu bằng việc thu thập tín hiệu BLE

B1: Đặc điểm hệ thống

* Dữ liệu cá nhân của người sử dụng

B2: Xác định mối đe dọa

* Rủi ro: Chơi xấu, giả mạo
* Nguyên nhân: Các ứng dụng truy vết tiếp xúc như Bluezone hoạt động bằng cách thu phát tín hiệu Bluetooth. Mỗi tín hiệu có chứa hai thông số: mã số người dùng và địa chỉ Bluetooth. Bất kỳ điện thoại hay thiết bị thu sóng Bluetooth nào cũng có thể nhìn thấy hai thông số này khi đứng gần điện thoại của người khác.
* Đối tượng bị đe dọa: những nơi công cộng hoặc công ty đối thủ

B3: Xác định lỗ hổng

* Truy vết sử dụng tín hiệu Bluetooth BLE

B4: Phân tích kiểm soát

* Nếu có phát hiện nghi vấn bị chơi xấu, gửi ngay thông tin về lịch sử tiếp xúc lên hệ thống để so sánh với lịch sử tiếp xúc của F0 đã được cơ quan y tế cập nhật . Nếu không giống với kết quả mà cơ quan y tế cập nhật, thì tín hiệu là giả mạo

B5: Xác định độ chắc chắn

* Cao
* Đây hoàn toàn là một nguy cơ có thể xảy ra bởi kẻ tấn công có thể dễ dàng thu được tín hiệu BlE, sau đó phát tín hiệu Bluetooth đặt tại bơi mà hắn muốn. Thiết bị sẽ phát đi tín hiệu Bluezone giả mạo các bluezone ID đã thu thập được trước đó.

B6: Phân tích tác động

* Lớn
* Việc phát đi tín hiệu Bluetooth giả mạo các Bluzone ID sẽ có thể tạo ra các báo động ra như tạo ra các F0 giả mạo mặc dù không có sự tiếp xúc của F0 đó với những người tại nơi bị kẻ tấn công đặt thiết bị phát
* Kẻ tấn công có thể đặt thiết bị phát tại các nơi công cộng gây ra nhiều người sẽ nhận được kết quả tiếp xúc giả, sau khi khối lượng thông báo giả này được gửi lên hệ thống sẽ làm rác hệ thống gây khó khan cho cơ quan y tế trong việc truy vết
* Kẻ tấn công đặt thiết bị tại nơi làm việc của đối thủ, tạo tín hiệu giả làm công việc bị đình trệ ảnh hưởng tới hiệu quả công việc , doanh thu, khách hàng và kinh tế

B7: Xác định rủi ro

* Cao
* Như mình đã nói ở trên việc thu và phát song tín hiệu BLE là rất dễ dàng với thiết bị thu, phát nên chúng hoàn toàn có thể xảy ra

B8: Khuyến nghị các biện pháp kiểm soát

* Giải pháp được đưa ra như sau: Cho phép 1 Bluezoner giả định có phát hiện tiếp xúc F0 (Nhận được thông tin qua broadcast ), Bluezoner này sẽ có tùy chọn xác minh F0 mình đã tiếp xúc có đúng là F0 thật hay không, bằng cách gửi lịch sử tiếp xúc F0 của mình lên hệ thống để so sánh với lịch sử tiếp xúc của F0 đã được cơ quan Y tế cập nhật. Nếu không có sự tương đồng, Bluzoner không phải F1

1. Số lượng người cài đặt ứng dụng không đủ để phát huy hiệu quả của ứng dụng.
2. Xác định đe dọa:

* Số lượng người cần đủ để ứng dụng phát huy hiệu quả tùy thuộc vào:
  + - 1. Người dùng có hiểu được chức năng chính của ứng dụng hay không?
      2. Niềm tin vào nhà sản xuất (chính phủ) có đủ để người dân cài đặt hay không?
      3. Có hiểu được những lỗ hổng mà ứng dụng đang tồn tại hay không?
      4. Có dễ dàng để tải và cài đặt và sử dụng ứng dụng không?.
      5. Người dùng có dễ tin vào các bài viết truyên truyền, bôi nhọ hình ảnh của ứng dụng trên các phương tiện truyền thông của những kẻ chống đối và phá hoại nhà nước hay không ?
      6. Có điều kiện để sở hữu smart phone để sử dụng ứng dụng hay không?

1. Phân tích kiểm soát

* Biện pháp hiện thời:
  + - 1. Đẩy mạnh truyền thông tới người dùng.
      2. Giao trách nhiệm tới các cán bộ gần dân nhất tới từng nhà khuyến cáo người dân.

1. Xác định ức độ chắc chắn

* Mức độ chắc chắn là VỪA: vì điều nước ta có tới 90 triệu dân nên để hiệu quả thì số người dùng ít nhất phải là 60 triệu. Điều này đặt ra bài toán lớn với chính phủ để ứng dụng tới với người dân. Nhưng do hoàn cảnh và đặc điểm con người nước ta: hoàn cảnh gấp rút và nguy cấp; đặc điểm người dân thì không nhiều người quan tâm tới vấn đê kỹ thuật mà chỉ quan tâm tới công dụng ứng dựng. Điện thoại smartphone đã phủ cập hết tới người dân nên khá dễ dàng trong việc tiếp cận. Dân ta có niềm tin lớn đối với Đảng.

1. Phân tích tác động

* Khả năng xảy ra lớn: Chi phí làm ra ứng dụng trong thời gian ngắn là rất lớn về tài sản và công sức tâm huyết của bao người. Khi ứng dụng không phát huy hiệu quả thì tất cả quá trình làm ra nó đều trở nên vô nghĩa hoặc không mang lại giá trị tương xứng.

1. Xác định rủi ro

* Mức độ thiệt hại là vừa nhưng tác động lại lớn, điều này đặt ra bài toán khó cho công tác truyền thông đề tránh tổn thất nặng nề

1. Khuyến nghị các biện pháp kiểm soát:

* Xây dựng phương án truyền thông trước khi ứng dụng ra mắt để người dân có thời gian tìm hiểu về ứng dụng. Giúp khi ra mắt ứng dụng nhanh chóng phát huy quả.

1. F0,F1,F2 có thể bị làm giả
   * + 1. Xác định đe dọa

* F0, F1, F2 có thể bị làm giả: đây là lỗ hổng khá nghiêm trọng vì điều này ảnh hưởng trực tiếp tới cuộc sống, tài sản của của đất nước khi F0, F1, F2 bị nhầm. Dưới sức ảnh hưởng của ứng dụng và hoàn cảnh thực tiễn thì đây là một vấn đề mà nhiều hacker sẽ quan tâm và sẽ không có ít phần tử lợi dụng lỗ hổng này.
  + - 1. Phân tích kiểm soát

Đặc biệt lưu ý và kiếm soát khâu tạo F0, F1, F2 trong quá trình sau thiết kế:

* Tham khảo các thuật toán, các cách trên thế giới đang sử dụng, các chuyên gia để có một cách an toàn và tối ưu nh.
* Thường xuyên báo cáo và pentest để kiểm tra các trường hợp có thể xảy ra để từ đó lập kịch bản phòng chống.
* Sẵn sàng thay đổi các khâu trước đó khi xảy ra nh mâu thuẫn khiến cho lỗ hổng trên có thể bị đe dọa.
* Lắng nghe cầu thị các ý kiến từ các chuyên gia khi public mã nguồn.
  + - 1. Xác định độ chắc chắn

Mức độ chắc chắn là CAO:

* Do ứng dựng có tính public lớn (vì phát tín hiệu Bluetooth liên tục.)
* Do tính mới và quan trọng của ứng dụng nên các Hacker hay kẻ phá hoại sẽ khá hứng thú với vi hack và phá hoại môi trường ứng dụng.
  + - 1. Phân tích tác động
* khả năng xảy ra lớn: Khi F0, F1, F2 được phát hiện thì cơ quan nhà nước sẽ thực hiện cách ly khoanh vùng nên nếu F0, F1, F2 giá mạo thì việc cách ly là vô nghĩa và tiền của và công sức trong 14 ngày đó sẽ vô nghĩa. Ngoài ra, gây hoang mang trong lòng dân, ảnh hướng tới cục diện của cuộc chiến chống dịch Covid. Khi đó, hệ quả kéo theo là niềm tin của người dân vào ứng dụng mất đi.
  + - 1. Xác định rủi ro
* Mức độ thiệt hại cao và tác động lớn: Đây là một vấn đề lớn đối với tổ chức sản xuất ứng dụng. Đặt ra nhiều bài toán khác nhau để đối phó với các mối đe dọa.
  + - 1. Khuyến khích các biện pháp kiểm soát
* Lập tổ chuyên trách xây dựng cách thức hiệu quả trong phần xác định F0, F1, F2.
* Lập tổ liên lạc phản ứng nhanh với các cơ quan chức năng trong việc xác định F0.
* Lập đội thử nghiệm ngay với khâu này đề tránh những sai xót k đáng có mà dẫn tới hậu quả lớn.

1. Cung cấp quyền Camera cho ứng dụng BZ
2. Xác định đe dọa

* Việc ứng dụng BZ được cung cấp quyền camera là một vấn đề khá nghiêm trọng khi mà gần đây các vấn đề về lộ thông tin hay những hình ảnh qua camera đang là các vấn đề gây rất nhiều bức bối và sẽ có không ít những thành phần có chủ đích xấu sẽ lợi dụng những lỗ hổng tương tự như này

1. Phân tích kiểm soát

* Kiểm soát khâu cấp quyền cho ứng dụng, chỉ cung cấp những quyền cần thiết và loạI bỏ những quyền không sử dụng đến.

1. Xác định độ chắc chắn

* Mức độ chắc chắn là cao vì hầu hết các thiết bị có thể càI đặt bluezone đều có camera, điều này có thể gây ra lộ hình ảnh thông tin cá nhân.

1. Phân tích tác động

* Khả năng xảy ra thấp

1. Xác định rủi ro

* Mức độ thiệt hại cao và khả năng xảy ra thấp. Đây là vấn đề mà khi bị tấn công vào lỗ hổng sẽ gây ra tổn thất lớn đến người dùng dẫn đến ứng dụng không còn mức tin tưởng cao.

1. Khuyến nghị các biện pháp kiểm soát

* Vì chưa rõ BZ cấp quyền camera cho ứng dụng để làm gì nên chưa thể đưa ra được cách khắc phục. Nếu trong trường hợp không sử dụng để làm gì thì cách khắc phục chỉ có thể là ngừng cung cấp quyền camera cho ứng dụng.
  + Qua quá trình phân tích trên thì ta thấy được những yếu tố tác động đến vấn đề an toàn của ứng dụng gồm có:
    1. Người dùng.
    2. Nhà phát triển ứng dụng
    3. Hacker mũ trắng hoặc đen.
    4. Đội quản lý thông tin.

->> Chính vì vậy Xây dựng khung pháp lý để sẵn sàng phản ứng:

* Luật an ninh mạng quy định về hoạt động bảo vệ an ning quốc gia và bảo đảm trặt tự, an toàn xã hội trên không gian mạng; trách nhiện của cơ quan, tổ chức, cá nhân có liên quan. Luật chỉ ra những phạm vi mà luật bảo vệ, hành vi bị cấm, các hệ thống vật chất phần mềm; chính sách Nhà nước; Nguyên tắc bảo vê; Biện pháp bảo vệ để bám sắt vào từng khâu của quy trình phát triển ứng dụng BLUEZONE. Để từ đó quy kết trách nhiệm một cách rõ ràng và cụ thể. Tóm lại: nhấn mạnh về tấn công mạng và các giải pháp phòng chống
* Luật an toàn thông tin được đưa ra để giải quyết vấn đề phát tán, rao bán thông tin cá nhân trên môi trường mạng: quy trách nhiệm về cơ quan, tổ chức, cá nhân. Đưa ra những quy định đối với các sản phẩn dịch vụ trong việc quản lý thông tin. Tóm lại: nhấn mạnh về quản lý an toàn thông tin.
* Nâng cao ý thức của mỗi người để kiểm soát dữ lệu tốt, từ đó nâng cao hiệu quả của ứng dụng và xa hơn là công tác chống dịch toàn dân

KẾT LUẬN

Các quốc gia khi phát triển giải pháp truy vết tiếp xúc đều tham khảo ý kiến của các chuyên gia. Bluezone có rất nhiều lỗ hổng sơ đẳng, chứng tỏ việc thiết kế và triển khai không có sự tham gia của những chuyên gia về an ninh mạng và riêng tư.

Bluezone white paper nên sử dụng tiếng Anh để biết thêm được các ý kiến từ các chuyên gia trên thế giới hoặc trong khu vực những ngườI quan tâm đến các application kiểu Contact tracing như BlueZone.