# BẢN TIN NỘI BỘ
# CẬP NHẬT VỀ AN TOÀN THÔNG TIN VÀ CẢNH BÁO LỖ HỔNG BẢO MẬT

## 1. 80% rò rỉ dữ liệu do người dùng tự làm lộ thông tin khi truy cập các ứng dụng trực tuyến

Trong tham luận "Rò rỉ dữ liệu và một số biện pháp giảm thiểu nguy cơ rò rỉ dữ liệu trong hệ thống thông tin quan trọng" trình bày tại chương trình diễn tập quốc gia về ứng cứu sự cố an toàn thông tin mạng năm 2019 được tổ chức ngày 31/7, ông Lương Xuân Thắng, Cục CNTT – Bộ Công an cho biết, những năm gần đây, thế giới đã xảy ra rất nhiều vụ rò rỉ dữ liệu, trong đó có những dữ liệu mật gây chấn động toàn cầu, liên quan đến nhiều quốc gia, nhiều quan chức của các nước. Riêng trong năm ngoái, hàng loạt vụ rò rỉ dữ liệu với quy mô lớn đã xảy ra, nguyên nhân có thể do bị tin tặc tấn công hoặc bị bán cho bên thứ ba.

Đại diện Cục CNTT - Bộ Công an cũng dẫn ra số liệu từ báo cáo của InfoWatch Analytical Center, theo đó trong nửa đầu năm ngoái, hệ thống của hãng này đã ghi nhận được 1.039 vụ thất thoát, rò rỉ dữ liệu được các tổ chức, cá nhân công bố, tăng 12% so với cùng kỳ năm 2017. Với 1.039 vụ lộ lọt dữ liệu này, đã có tới 2,39 tỷ hồ sơ bị rò rỉ gồm các thông tin cá nhân, số bảo hiểm xã hội, thẻ tín dụng và một số thông tin khác.

Nghiên cứu của InfoWatch cũng chỉ ra rằng, có tới 64,5% vụ rò rỉ dữ liệu xuất phát từ bên trong nội bộ tổ chức và 35,5% gây ra bởi các cuộc tấn công từ bên ngoài vào các hệ thống thông tin của các tổ chức.

Đáng chú ý, tham luận của đại diện Cục CNTT – Bộ Công an cho thấy, có cùng mối lo chung với các nước khác trên thế giới, Việt Nam đang phải đối mặt với các nguy cơ về lộ lọt, rò rỉ thông tin dữ liệu rất lớn.

Cụ thể, dẫn ra kết quả khảo sát của hãng Symantec đối với các doanh nghiệp Việt Nam cho thấy có tới 94% doanh nghiệp bị rò rỉ dữ liệu. Tháng 10/2018, hacker Sogo Nakamoto đã tấn công vào hệ thống của Ngân hàng Hợp tác xã Việt Nam và để lại thông báo bán 275.000 thông tin khách hàng… Ngoài ra, trong năm 2018 có nhiều doanh nghiệp lớn về công nghệ bị rò rỉ thông tin khách hàng.

Trung tâm Ứng cứu khẩn cấp máy tính Việt Nam - VNCERT hồi cuối năm 2017 cũng đã có văn bản khẩn cấp số 442 về việc lộ 1,4 tỷ tài khoản và mật khẩu từ các trang mạng xã hội, dịch vụ trực tuyến (dữ liệu bị lộ lọt lên tới 41 GB). Trong đó, có 437.644 tài khoản email (930 tài khoản email của cơ quan nhà nước ".gov.vn").

"Tình trạng rò rỉ, lộ lọt bí mật nhà nước qua Internet đã và đang diễn ra khá phổ biến, nhiều vụ việc rất nghiêm trọng. Nhiều tài liệu có độ mật cao xếp loại "Tối mật", "Mật" đã bị lộ lọt trên mạng Internet", ông Lương Xuân Thắng nhấn mạnh.

Đề cập đến nguyên nhân của tình trạng trên, vị đại diện Cục CNTT Bộ Công an nhận định, có tới 80% rò rỉ dữ liệu do người dùng: tự làm lộ thông tin cá nhân khi sử dụng các thiết bị thông minh truy cập vào các ứng dụng trực tuyến; và 20% rò rỉ dữ liệu thông qua tấn công khai thác điểm yếu an toàn thông tin.

Cũng theo phân tích của đại diện Cục CNTT, Bộ Công an, các nguy cơ dẫn đến rò rỉ thông tin, dữ liệu của các cơ quan, tổ chức có thể kể đến như: soạn thảo văn bản có nội dung bí mật trên các máy tính có kết nối mạng Internet; sao chép dữ liệu có nội dung bí mật vào các USB không bảo mật; gửi tài liệu có nội dung bí mật qua thư điện tử; in ấn, sao chụp phát tán các tài liệu có nội dung bí mật; tải các tài liệu có nội dung bí mật lên các trang web rao bán tài liệu; máy tính tồn tại lỗ hổng bảo mật, tồn tại nhiều virus, phần mềm độc hại đánh cắp dữ liệu và phát tán trên mạng; truy cập dữ liệu nhạy cảm từ người dùng không xác định.

Đại diện Cục CNTT, Bộ Công an cũng chỉ rõ: "Để giảm thiểu nguy cơ mất an toàn thông tin, loại bỏ cơ bản nguyên nhân rò rỉ dữ liệu trong các hệ thống thông tin quan trọng, các biện pháp đề xuất phải hội tụ đủ 4 yếu tố: Con người; Quy trình chính sách; Công nghệ; và Tài chính".

Đặc biệt, nhấn mạnh yếu tố "Con người", đại diện Cục CNTT, Bộ Công an đề xuất, với người dùng trong hệ thống, cần tuyên truyền, nâng cao nhận thức về vấn đề bảo đảm an toàn thông tin; nâng cao kỹ năng, tuân thủ quy trình sử dụng các thiết bị CNTT trong hệ thống, nhận biết các nguy cơ, hình thức tấn công mạng.

Bên cạnh đó, cũng cần xây dựng đội ngũ chuyên trách về an toàn thông tin có đủ trình độ để thực hiện nhiệm vụ của đơn vị chuyên trách về an toàn thông tin; tổ chức và tham gia gia ứng cứu các sự cố về mạng và an toàn thông tin. Các cán bộ quản lý, chủ quản hệ thống thông tin phải được đào tạo, nâng cao trình độ quản lý các hệ thống thông tin.

***Khuyến nghị:***

Phòng ATTT khuyến nghị: Người dùng cần luôn đề cao cảnh giác tránh để lộ lọt thông tin đồng thời tuân thủ các quy trình, quy định bảo đảm an toàn thông tin đã ban hành.

Link tham khảo: https://ictnews.vn/cntt/bao-mat/80-ro-ri-du-lieu-do-nguoi-dung-tu-lam-lo-thong-tin-khi-truy-cap-cac-ung-dung-truc-tuyen-187160.ict

## 2. Dọa người dùng lộ ảnh sex, hacker phát tán mã độc tống tiền

Theo Công ty an ninh mạng Slovakia ESET, nếu đang sử dụng điện thoại Android, bạn có thể trở thành nạn nhân của một loại virus mới phát tán qua tin nhắn SMS.

Mã độc có tên gọi Android/Filecoder.C được kích hoạt từ ngày 12/7. Nó sử dụng danh bạ của nạn nhân để gửi đi tin nhắn SMS chứa các liên kết xấu. Loại virus này phát tán đầu tiên thông qua những bài đăng khiêu dâm trên diễn đàn Reddit và XDA-Developers.

Đoạn tin nhắn cho thấy một đường link, với nội dung kiểu: "Tôi thấy hình ảnh của bạn xuất hiện trên web khiêu dâm này!". Để chân thực hơn, tên miền liên kết đôi khi được rút gọn bằng các công cụ như bit.ly hay Google URL Shortener.

Các tin nhắn cũng được gửi đến bằng một trong 42 ngôn ngữ tùy thuộc vào cài đặt trên thiết bị.

Khi liên kết được mở, mã độc bắt đầu kiểm soát máy chủ để truy cập danh bạ, đồng thời mã hóa các tệp. Nạn nhân có thể mất quyền truy cập dữ liệu trong thiết bị. Tuy nhiên, những file có dung lượng lớn hơn 50 MB lại không bị ảnh hưởng.

Virus này mã hóa dữ liệu bằng thuật toán RSA. Nếu chấp nhận trả khoản tiền chuộc, kẻ tấn công sẽ giải mã và gửi khóa riêng cho nạn nhân để lấy lại dữ liệu.

Các nhà nghiên cứu của ESET cho biết mọi tập tin được mã hóa đều có thể phục hồi. "Nhưng nếu mã độc này được cải tiến, nó có thể trở thành mối đe dọa nghiêm trọng".

ESET không tiết lộ có bao nhiêu thiết bị đã dính mã độc Filecoder. Khi kiểm tra đường dẫn, các nhà nghiên cứu phát hiện nó được mở 59 lần, chủ yếu từ người dùng Trung Quốc, Mỹ và Hongkong.

Trong thời điểm Android tiếp tục đối mặt với những mối đe dọa bảo mật, Google khuyên người dùng thường xuyên kiểm tra và tải về các bản cập nhật, cũng như thận trọng khi cấp quyền truy cập thiết bị cho nhà phát triển ứng dụng.

***Khuyến nghị:***

Phòng ATTT khuyến nghị: Người dùng cần thường xuyên kiểm tra và tải về các bản cập nhật, cần đọc kỹ các điều khoản khi cài đặt ứng dụng, không mở các đường dẫn lạ trong SMS để đảm bảo an toàn thông tin.

Link tham khảo: https://vietnamnet.vn/vn/cong-nghe/bao-mat/doa-nguoi-dung-lo-anh-sex-hacker-phat-tan-ma-doc-tong-tien-555075.html

### 3. Google tiết lộ PoC cho 4 lỗ hổng có thể khai thác từ xa trên iOS

Các nhà nghiên cứu an ninh mạng của Google cuối cùng đã tiết lộ chi tiết và PoC cho 4 trong số 5 lỗ hổng an ninh có thể cho phép kẻ tấn công từ xa nhắm mục tiêu vào các thiết bị iOS của Apple chỉ bằng cách gửi tin nhắn độc hại qua iMessage.

Tất cả các lỗ hổng, đều không yêu cầu tương tác người dùng, đã được Samuel Groß và Natalie Silvanovich của Google Project Zero báo với Apple. Tuần trước, Apple đã vá các lỗ hổng này bằng việc phát hành bản cập nhật iOS 12.4 mới nhất.

Bốn trong số các lỗ hổng này là các vấn đề lỗi bộ nhớ và use-after-free không cần tương tác có thể cho phép kẻ tấn công từ xa thực hiện mã tùy ý trên các thiết bị iOS bị ảnh hưởng.

Tuy nhiên, các nhà nghiên cứu mới chỉ công bố chi tiết và PoC cho ba trong bốn lỗ hổng RCE quan trọng này và giữ bí mật về lỗ hổng thứ tư (CVE-2019-8641) vì bản cập nhật mới nhất không hoàn toàn giải quyết vấn đề này.

Lỗ hổng thứ năm (CVE-2019-8646), lỗi đọc ngoài giới hạn (out-of-bounds), cũng có thể được thực thi từ xa bằng cách gửi một tin nhắn không đúng định dạng qua iMessage. Nhưng thay vì thực thi mã, lỗi này cho phép kẻ tấn công đọc nội dung của các tệp được lưu trữ trên thiết bị iOS của nạn nhân thông qua bộ nhớ bị rò rỉ.

Dưới đây là chi tiết ngắn gọn về bốn lỗ hổng:

• CVE-2019-8647 (RCE qua iMessage) – Đây là lỗi use-after-free nằm trong framework Core Data (khung Dữ liệu lõi) của iOS có thể dẫn tới thực thi mã tùy ý

do quá trình deserialization (chuyển đổi chuỗi byte thành đối tượng) không an toàn khi sử dụng phương thức NSArray initWithCoder.

• CVE-2019-8662 (RCE qua iMessage) - Lỗ hổng này cũng tương tự như lỗi use-after-free ở trên và nằm trong thành phần QuickLook của iOS, cũng có thể được kích hoạt từ xa thông qua iMessage.

• CVE-2019-8660 (RCE qua iMessage) - Đây là vấn đề lỗi bộ nhớ nằm trong khung Dữ liệu lõi và thành phần Siri, nếu bị khai thác thành công, có thể cho phép kẻ tấn công từ xa bất ngờ dừng ứng dụng hoặc thực thi mã tùy ý.

• CVE-2019-8646 (Đọc tệp qua iMessage) - Lỗ hổng này, cũng nằm trong các thành phần Siri và Core Data của iOS, có thể cho phép kẻ tấn công đọc nội dung của các tệp được lưu trữ trên thiết bị iOS mà không cần tương tác của người dùng, như người dùng di động không có sandbox.

Bên cạnh 5 lỗ hổng này, tuần trước, Silvanovich cũng đã công bố thông tin chi tiết và PoC cho một lỗ hổng đọc ngoài giới hạn khác cũng cho phép kẻ tấn công từ xa rò rỉ bộ nhớ và đọc tệp từ một thiết bị từ xa.

Lỗ hổng, CVE-2019-8624, nằm trong thành phần Digital Touch của watchOS và ảnh hưởng đến Apple Watch Series 1 trở lên. Vấn đề đã được Apple vá trong tháng này với việc phát hành watchOS 5.3.

Do PoC cho tất cả sáu lỗ hổng này hiện đã được công khai, người dùng được khuyến cáo nên nâng cấp các thiết bị Apple lên phiên bản phần mềm mới nhất càng sớm càng tốt.

***Khuyến nghị:***

Phòng ATTT khuyến nghị: Người dùng các thiết bị Apple nên cập nhật lên các phiên bản phần mềm mới nhất để đảm bảo an toàn thông tin.

Link tham khảo: https://whitehat.vn/threads/google-tiet-lo-poc-cho-4-lo-hong-co-the-khai-thac-tu-xa-tren-ios.12526/

## TECHNICAL PAGES:

1. Chi tiết về thông tin một số lỗ hổng trên các sản phẩm/dịch vụ phổ biến tại Việt Nam trong tuần, cụ thể như sau:

| STT | Sản phẩm/ dịch vụ | Mã lỗi quốc tế | Mô tả ngắn | Ghi chú |
|---|---|---|---|---|
| 1 | Foxit | CVE-2019-14209<br>CVE-2019-14208<br>CVE-2019-14210<br>... | Nhóm 09 lỗ hổng trên phần mềm FoxitPhantomPDF phiên bản trước 8.3.10 làm lộ bộ nhớ Heap…<br>01 lỗ hổng ở mức nghiêm trọng, có điểm CVSS Base là 9.8/10 và nhiều lỗ hổng ở mức cao. | Đã có thông tin xác nhận và bản vá. |
| 2 | Mozilla | CVE-2019-11691<br>CVE-2019-11692<br>CVE-2019-11693<br>….. | Nhóm 48 lỗ hổng trên một số chức năng, thành phần (XMLHttpRequest, Listeners, WebGL, HTTP/2) của trình duyệt Firefox và Thunderbird cho phép đối tượng tấn công khai thác lỗi tràn bộ đệm, chèn và thực thi mã lệnh Ảnh hưởng tới nhiều phiên bản Firefox và Thunderbird | Đã có thông tin xác nhận và bản vá |
| 3 | Oracle | CVE-2019-2764<br>CVE-2019-2792<br>CVE-2019-2835<br>... | Nhóm 157 lỗ hổng trên một số sản phẩm, ứng dụng (Oracle Enterprise Manager Products Suite, Oracle Retail Applications, Oracle Fusion Middleware...) của Oracle cho phép đối tượng tấn công thực hiện tấn công từ chối dịch vụ, truy cập trái phép vào ứng dụng và thực hiện hành động nguy hại (cập nhập, chèn, xóa) Nhiều lỗ hổng có điểm CVSS Base ở mức cao. | Chưa có thông tin xác nhận và bản vá. |
| 4 | Qualcomm | CVE-2019-2263<br>CVE-2019-2299<br>CVE-2019-2301<br>… | Nhóm 50 lỗ hổng trên một số firmware của Qualcomm- sử dụng nhiều trong các sản phẩm công nghệ (từ thiết bị IoT điều khiển công nghiệp, điều khiển tự động, Mobile, và cả thiết bị mạng...) cho phép đối tượng tấn công khai thác lỗi tràn bộ đệm, lỗi cấp phát bộ nhớ từ đó có thể | Đã có thông tin xác nhận và bản vá |

| | | | | |
|---|---|---|---|---|
| | | | thực hiện tấn công sâu hơn | |
| 5 | IBM | CVE-2019-4415<br>CVE-2019-4439<br>CVE-2018-2024<br>... | Nhóm 07 lỗ hổng trong sản phẩm, dịch vụ của IBM (Cloud Private, QRadar SIEM, Spectrum Protect) cho phép đối tượng tấn công khai thác lỗi tràn bộ đệm để chèn và thực thi mã lệnh trong Spectrum Protect, truy cập trái phép vào tài nguyên trên hệ thống đặc biệt là dữ liệu giám sát của sản phẩm Qradar. | Đã có thông tin xác nhận và bản vá. |
| 6 | Exim | CVE-2019-13917 | 01 lỗ hổng trong Exim phiên bản 4.85 đến 4.92 cho phép đối tượng tấn công thực thi mã lệnh như quyền Root. Có 4,855,461 máy chủ trên thế giới đang sử dụng Exim công khai trên Internet, trong đó có 30.942 máy chủ của Việt Nam | Đã có thông tin xác nhận và bản vá |

2. Danh sách IP/tên miền độc hại có nhiều kết nối từ Việt Nam

| **STT** | **Tên miền/IP** |
|---|---|
| 1 | disorderstatus.ru |
| 2 | differentia.ru |
| 3 | www.iuqerfsodp9ifjaposdfjhgosurijfaewrwergwea.com |
| 4 | atomictrivia.ru |
| 5 | soplifan.ru |
| 6 | somicrososoft.ru |
| 7 | morphed.ru |
| 8 | awjapmnak.info |
| 9 | www.cityofangelsmagazine.com |
| 10 | a.deltaheavy.ru |

3. Các cán bộ kỹ thuật đầu mối về ATTT cần thực hiện:

- Xử lý các lỗ hổng phát hiện tại bảng 1 (nếu có).
- Chặn, xử lý các truy nhập tới các tên miền độc hại tại bảng 2.