BẢN TIN NỘI BỘ

CẬP NHẬT VỀ AN TOÀN THÔNG TIN VÀ CẢNH BÁO LỖ HỔNG BẢO MẬT

1. Phiên bản mới của FinSpy đánh cắp thông tin trên iOS, Android

Theo thông tin từ Kaspersky, một phiên bản mới của bộ công cụ độc hại FinSpy được phát hiện đánh cắp thông tin từ các chính phủ, cơ quan thực thi pháp luật và tổ chức phi chính phủ trên toàn cầu.

FinSpy là bộ công cụ phần mềm độc hại nguy hiểm được sử dụng để giám sát mục tiêu. Nó được sử dụng bằng cách điều chỉnh hành vi của từng mã độc trong bộ công cụ để phù hợp với mục tiêu hoặc nhóm mục tiêu cụ thể, cho phép tin tặc đánh cắp thông tin từ các thiết bị trên toàn thế giới.

Theo thông cáo báo chí ngày 10/7 của Kaspersky, phiên bản mới của bộ công cụ độc hại này hoạt động trên cả thiết bị iOS và Android. Chúng cho phép tin tặc theo dõi hoạt động của hầu hết các dịch vụ nhắn tin phổ biến, bao gồm cả dịch vụ được mã hóa, đồng thời che giấu dấu vết tốt hơn phiên bản trước đó.

Bộ công cụ độc hại này có thể ẩn đi các dấu hiệu của việc bẻ khóa trên iOS và giành quyền root trên thiết bị Android. Mã độc trên Android có chức năng tương tự như trên iOS, nhưng cũng có khả năng giành quyền root trên một thiết bị chưa được root, bằng cách khai thác DirtyCow - tính năng sẵn có trong bộ công cụ. Các mẫu mã độc của FinSpy trên Android đã bị phát hiện trong một vài năm qua. Dựa trên dữ liệu chứng thư của phiên bản cuối cùng được tìm thấy, mẫu mã độc này đã bắt đầu hoạt động vào tháng 6/2018.

Alexey Firsh - nhà nghiên cứu bảo mật của Kaspersky cho biết, các nhà phát triển đứng sau bộ công cụ độc hại FinSpy liên tục theo dõi các bản cập nhật bảo mật cho các nền tảng di động và có xu hướng nhanh chóng sửa đổi mã độc để vô hiệu hóa các bản sửa lỗi.

Hơn nữa, các nhà phát triển này theo dõi các xu hướng và triển khai chức năng trích xuất dữ liệu từ các ứng dụng hiện đang phổ biến. Kaspersky cho biết, số lượng nạn nhân mới của bộ công cụ độc hại FinSpy gia tăng hàng ngày. Do đó, người dùng cần theo dõi và cài đặt các bản cập nhật nền tảng di động sớm nhất có thể. Cho dù, các ứng dụng có thể an toàn đến mức nào hay người dùng bảo vệ dữ liệu tốt đến đâu, một khi điện thoại đã được root hoặc bẻ khóa thì nguy cơ lây nhiễm mã độc là rất cao.

Khuyến nghị:

Phòng ATTT khuyến nghị: Người dùng thiết bị di động không root máy và cần cập nhật phiên bản mới nhất của hệ điều hành để đảm bảo an toàn thông tin.

Link tham khảo: http://www.antoanthongtin.vn/Detail.aspx?CatID=c74b5c11-1141-471b-95c8-a05fe6e7d3a6&NewsID=3167b35c-5ea5-4420-8514-9d71cb74bd20

2. Phát hiện ứng dụng FaceApp giả mạo "tiêm" mã độc vào thiết bị người dùng

Những ngày gần đây, ứng dụng chỉnh sửa hình ảnh FaceApp liên tục bị cảnh báo về vấn đề bảo mật. Theo ông Yeo Siang Tiong, Tổng giám đốc Kaspersky khu vực Đông Nam Á, hiện tại, việc một ứng dụng được bàn tán rất nhiều trên mạng xã hội và trở thành hiện tượng đang diễn ra rất thường xuyên.

"Ở thời đại mà người dùng dễ bị cuốn hút bởi một xu hướng có tính giải trí và hợp thời đại như hiện nay, trạng thái FOMO hoặc Fear of Missing Out (lo sợ bị bỏ lỡ) có thể làm xao lãng những thói quen bảo mật cơ bản - như cảnh giác trong việc cấp quyền cho ứng dụng", ông Yeo Siang Tiong chia sẻ.

Cũng theo thông tin từ Kaspersky, một nghiên cứu của hãng này cho thấy 63% người dùng không đọc thỏa thuận sử dụng và 43% người dùng đánh dấu vào tất cả yêu cầu truy cập dữ liệu khi cài đặt ứng dụng mới. Mặc dù cuộc khảo sát này đã được thực hiện 3 năm trước, nhưng các chuyên gia Kaspersky tin rằng những con số nêu trên vẫn có giá trị thể hiện thói quen kỹ thuật số của người dùng hiện nay.

Về cơ bản, việc tham gia các thử thách trực tuyến hay cài đặt ứng dụng mới sẽ không gây hại. Sự nguy hiểm nằm ở chỗ người dùng dễ dàng cấp quyền cho các ứng dụng được truy cập vô hạn vào danh bạ, hình ảnh, tin nhắn riêng tư… Việc này cho phép các đơn vị sản xuất ứng dụng có thể truy cập vào những dữ liệu nhạy cảm một cách hợp pháp. Khi dữ liệu nhạy cảm bị hack hoặc sử dụng sai mục đích, các ứng dụng có thể xuất hiện lỗ hổng mà tin tặc lợi dụng khai thác để phát tán mã độc.

Để không phải đối mặt với tình huống đáng lo ngại kể trên, chuyên gia Kaspersky khuyên người dùng cần luôn cẩn thận và đề cao cảnh giác khi trực tuyến. Nhằm giảm thiểu khả năng bị tấn công mạng, Kaspersky khuyến nghị người dùng áp dụng các cách như: chỉ tải xuống ứng dụng từ những nguồn đáng tin cậy, đọc đánh giá và xếp hạng của các ứng dụng trước khi tải về; xem xét và lựa chọn kỹ lưỡng những ứng dụng trước khi cài đặt lên thiết bị; đọc kỹ thỏa thuận sử dụng trước khi cấp phép quyền truy cập, chú ý đến những quyền mà ứng dụng của bạn yêu cầu truy cập; tránh việc nhấp chuột theo quán tính với các yêu cầu khi cài đặt ứng dụng.

Ngoài ra, người dùng cũng được khuyên nên cài đặt giải pháp bảo mật trên thiết bị của mình.

Cũng trong thông tin mới phát ra, Kaspersky cho biết, các chuyên gia của hãng đã phát hiện một ứng dụng FaceApp giả mạo được sử dụng để tiêm mã độc vào thiết bị của người dùng.

Cụ thể, Kaspersky đã xác định một ứng dụng giả mạo được tạo ra để đánh lừa người dùng, khiến họ nghĩ rằng đây là phiên bản chính thức của FaceApp. Trên thực tế, ứng dụng giả mạo này khiến thiết bị di động của nạn nhân bị nhiễm mã độc với mô-đun phần mềm quảng cáo mang tên MobiDash. Khi ứng dụng từ những nguồn không chính thức được tải xuống cài đặt, chúng sẽ báo lỗi giả và được gỡ bỏ ngay sau đó. Tiếp theo, một mô-đun độc hại trong ứng dụng sẽ được cài cắm kín đáo và bắt đầu hiển thị quảng cáo trên thiết bị của người dùng.

Theo dữ liệu của Kaspersky, khoảng 500 người dùng đã gặp sự cố này chỉ trong hai ngày, với phát hiện đầu tiên xuất hiện vào ngày 7/7/2019. Có gần 800 mô-đun khác nhau đã được xác định.

Ông Igor Golovin, nhà nghiên cứu bảo mật tại Kaspersky cho biết: "Những người đứng sau MobiDash thường ẩn mô-đun phần mềm quảng cáo của họ dưới vỏ bọc những ứng dụng và dịch vụ phổ biến. Điều này có nghĩa là các hoạt động của FaceApp giả mạo đang diễn ra mạnh mẽ, với hàng trăm mục tiêu tấn công chỉ trong vài ngày. Chúng tôi khuyên người dùng không nên tải xuống các ứng dụng từ những nguồn không chính thức, đồng thời nên cài đặt các giải pháp bảo mật trên thiết bị của mình để tránh mọi thiệt hại do mã độc gây ra".

Khuyến nghị:

Phòng ATTT khuyến nghị: Người dùng cần kiểm tra nguồn gốc nhà phát hành, đọc kỹ các chính sách của ứng dụng trước khi cài đặt để đảm bảo an toàn thông tin.

Link tham khảo: https://ictnews.vn/cntt/bao-mat/phat-hien-ung-dung-faceapp-gia-mao-tiem-ma-doc-vao-thiet-bi-nguoi-dung-185911.ict

3. Mở tài liệu bằng LibreOffice có thể khiến máy tính bị hack

LibreOffice tồn tại một lỗ hổng thực thi mã nguy hiểm và chưa có bản vá, có thể lén lút cài mã độc vào hệ thống của người dùng ngay khi họ mở file do hacker tạo ra.

LibreOffice là một trong những lựa chọn phần mềm mã nguồn mở và thay thế cho các bộ Microsoft Office phổ biến nhất hiện nay, dùng trên các hệ điều hành Windows, Linux và macOS.

Nhà nghiên cứu Alex Inführ, người phát hiện ra lỗ hổng cho biết, đầu tháng 07/2019, LibreOfffice đã phát hành phiên bản phần mềm mới nhất 6.2.5 để xử lý hai lỗ hổng nghiêm trọng (CVE-2019-9848 và CVE-2019-9849), nhưng bản vá cho lỗ hổng cũ hiện đã bị qua mặt.

Dù nhà nghiên cứu Inführ chưa tiết lộ chi tiết kỹ thuật cho phép mình qua mặt được bản vá, nhưng có giải thích về ảnh hưởng của lỗ hổng này như sau:

- **CVE-2019-9848**: Lỗ hổng vẫn tồn tại trên phiên bản mới nhất, nằm trong LibreLogo - môi trường lập trình Python được mặc định đi kèm LibreOffice.

Lỗ hổng có thể cho phép kẻ tấn công tạo một file tài liệu chứa mã độc, âm thầm thực thi lệnh python tùy ý mà không hiển thị bất kỳ cảnh báo nào đến người dùng mục tiêu.

Lỗi hổng này đã có PoC.

- **CVE-2019-9849**: Lỗ hổng cho phép đưa đoạn mã khai thác từ xa vào một tài liệu, kể cả khi chế độ "stealth mode" (chế độ tàng hình) được bật. Lỗi này có thể được khắc phục bằng cách cài đặt bản cập nhật mới nhất.

Lỗ hổng đã được báo cáo cho đội ngũ LibreOffice nhưng cho đến khi có bản vá, người dùng được khuyến cáo cập nhật hoặc cài đặt lại phần mềm mà không dùng đến macro hoặc ít nhất là tính năng LibreLogo, bằng cách thực hiện các bước sau:

Mở mục setup và bắt đầu quá trình cài đặt

Lựa chọn cài đặt “Custom”

Lựa chọn mở rộng “Optional Components”

Tick vào LibreLogo và lựa chọn “This Feature Will Not Be Available"

Chọn Next và sau đó cài đặt phần mềm

Khuyến nghị:

Phòng ATTT khuyến nghị: Người dùng LibreOffice nên cập nhật hoặc cài đặt lại phần mềm mà không dùng đến macro hoặc ít nhất là tắt tính năng LibreLogo theo hướng dẫn ở trên để đảm bảo an toàn thông tin.

Link tham khảo: https://whitehat.vn/threads/mo-tai-lieu-bang-libreoffice-co-the-khien-may-tinh-bi-hack.12513/

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	Microsoft	CVE-2019-1001 CVE-2019-1092 CVE-2019-1104 ...	Nhóm 77 lỗ hổng trên một số sản phẩm, phần mềm của Microsoft (Chakracore, Edge, Office, IE, Windows 10, Windows 7, Windows Server 2012...) cho phép đối tượng tấn công chèn và thực thi mã lệnh từ xa, tấn công leo thang.	Đã có thông tin xác nhận và bản vá.
2	Adobe	CVE-2019-7850 CVE-2019-7843 CVE-2019-7847 …..	Nhóm 11 lỗ hổng trên một số sản phẩm của Adobe (Campaign Classic, Bridge CC Dreamweaver, Experience Manager) cho phép đối tượng tấn công chèn và thực thi lệnh độc hại, thu thập thông tin nhạy cảm.	Đã có thông tin xác nhận và bản vá
3	Centos Webpanel	CVE-2019-13359 CVE-2019-13383 CVE-2019-13605 ...	Nhóm 08 lỗ hổng trên CentOS Web Panel cho phép nwgoiwf dùng tải tập tin tùy ý lên thư mục /tmp, truy cập trái phép vào hệ thống với quyền của người dùng thông thường mà không cần xác thực, tìm kiếm người dùng có trên hệ thống.	Chưa có thông tin xác nhận và bản vá.
4	IBM	CVE-2019-4194 CVE-2019-4430 CVE-2018-2021	Nhóm 07 lỗ hổng trên một số sản phẩm của IBM (IBM Campaign, QRadar SIEM, IBM Jazz, IBM Maximo Asset Management) cho phép đối tượng tấn công khai thác lỗi Path Traverse để truy cập trái phép vào tập tin trên hệ thống, lỗi XSS thực thi các đoạn mã Java, thu thập thông tin nhạy cảm	Đã có thông tin xác nhận và bản vá
5	Cisco	CVE-2019-1873 CVE-2019-1932	Nhóm 08 lỗ hổng trên một số sản phẩm, ứng dụng của Cisco	Đã có thông tin

		CVE-2019-1921 ...	(IOS Access Points, Small Business Switches, FindIT Network Management Software, Identity Services Engine, Industrial Network Director) cho phép đối tượng tấn công truy cập vào giao diện console của thiết bị với quyền Root, khai thác lỗi SQL InjectionCentOS Web Panel, XSS, chuyển hướng người dùng đến trang web độc hại, một số lỗi cho phép thực thi hàng động trái phép thông qua REST APT	xác nhận và bản vá.
6	Tp-link	CVE-2019-13613 CVE-2019-1010104 CVE-2019-13569 CVE-2019-12934	02 Lỗ hổng trên thiết bị TP-Link Wireless Router Archer Router và TP-Link Archer C1200 cho phép khai thác lỗi tràn bộ đệm để thực thi ma lệnh.	Chưa có thông tin xác nhận và bản vá
7	Wordpress	CVE-2019-1010104 CVE-2019-13569 CVE-2019-12934	Nhóm 03 lỗ hổng trên một số plugin của Wordpress (TechyTalk Quick Chat, Email Subscribers & Newsletters, wp-code-highlightjs) cho phép khai thác lỗi SQL Injection, XSS.	Chưa 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	n.hmiblgoja.ru
2	mokoaehaeihgiaheih.ru
3	produkktc.com
4	mel.cloudcontentsmak.com
5	and30.blabladomdom.com
6	ajkeahkcueafuiaeuf.ru
7	dghfhfgjfhjghj6699.net

8	and28.aviationdreamflightering1.com
9	https://realhotchickss.com/xefyzznumsa
10	bszotsjovih.com

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.