CẢNH BÁO

TUẦN 14 (30/03/2020 - 05/04/2020)

Hà Nội, ngày 07 tháng 04 năm 2020

Tin tức

- Các ứng dụng Android độc hại khai thác dịch Covid-19 để phát tán mã độc.
- Công cụ độc hại tấn công Zoom nhằm thu thập thông tin người dùng.

Điểm yếu, lỗ hổng

- 299 lỗ hổng được công bố và cập nhật
- 07 lỗ hổng/nhóm lỗ hổng trên các sản phẩm tại Việt Nam.
- Chi tiết 02 lỗ hổng: CVE-2020-7982, CVE-2020-0796

Số liệu, thống kê

- Tấn công DRDoS
- Tấn công Web
- Mạng botnet: Avalanche, Conficker, Necurs, Wannacry.
- IP/tên miền độc hại:10 địa chỉ

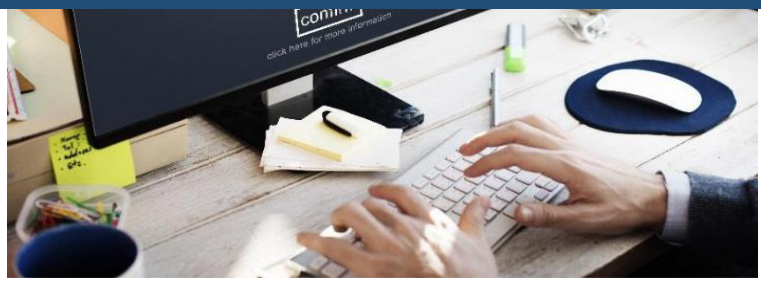
Khuyến nghị

Khuyến nghị đối với các cơ quan, đơn vị.

RSG

Cập nhật 05 báo cáo tài liệu chuyên ngành.

Các ứng dụng Android độc hại khai thác thông tin liên quan tới dịch Covid-19 để phát tán mã độc.



Ngày 26 tháng 3, các chuyên gia bảo mật đã phát hiện ra 11 ứng dụng Adroid giả mạo chứa mã độc tồn tại dưới dạng những ứng dụng hợp phát liên quan đến việc theo dõi đại dịch Covid-19. Tất cả các ứng dụng độc hại được phát hiện đều là các phiên bản của một ứng dụng hợp phát với tên gọi là **SM_Covid19.**

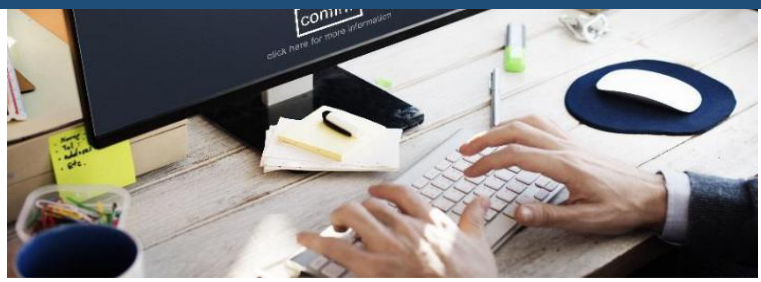
Các ứng dụng này được tạo ra sau ngày 20 tháng 3, thời điểm Covid-19 đang lan rộng, đặc biệt là ở châu Âu, nhằm mục tiêu đến nước Ý, nơi có các trường hợp được xác nhận nhiều nhất về Covid-19. Ngoài ra, các ứng dụng này còn được cài đặt trên các thiết bị ở Mỹ và Pháp.

Các ứng dụng độc hại có nhiều tính năng của ứng dụng hợp pháp như thu thập thông tin vị trí và thiết bị để theo dõi Covid-19. Tuy nhiên, ứng dụng có thể kết nối TCP ngược, cho phép đối tượng tấn công thu thập thông tin (tệp, tin nhắn SMS, danh bạ của thiết bị bị lây nhiễm, thậm chí có thể chụp ảnh màn hình về những gì thiết bị đang hiển thị) chèn và thực thi mã tùy ý.

Ngoài ra, phần mềm độc hại được sử dụng cũng có một mô-đun được thêm vào cho phép tải xuống bất kỳ payload nào từ máy chủ của đối tượng tấn công, nó hỗ trợ cho việc thực hiện cuộc tấn công vào tất cả người dùng trong cùng một lúc, tạo botnet, tấn công từ chối dịch vụ.

Source: https://symantec-blogs.broadcom.com/blogs/threat-intelligence/android-apps-coronavirus-covid19-malicious
https://otx.alienvault.com/pulse/5e87a59fc22c38919d9c9340

Cảnh báo công cụ độc hại tấn công ứng dụng phần mềm Zoom nhằm thu thập thông tin người dùng.



Trong thời gian vừa qua, nhu cầu phải làm việc từ xa trong mùa dịch Covid-19 nên số người sử dụng Zoom tăng đáng kể (tăng 67% kể từ đầu năm), làm nó trở thành mục tiêu của những cuộc tấn công mạng. Gần đây, đã phát hiện một công cụ tự động có khả năng tìm kiếm 100ID các cuộc họp mỗi giờ. Công cụ có thể tìm kiếm gần 2,400 cuộc họp trên Zoom chỉ sau một ngày quét dò tìm.

Công cụ có tên là zWarDial, có khả năng đoán được mã các cuộc họp Zoom, với độ dài từ 9 tới 11 ký tự, cho phép đối tượng tấn công thu thập thông tin trong cuộc họp (thời gian diễn ra, người tổ chức cuộc họp, chủ đề cuộc họp và có thể liên kết cuộc họp). zWarDial có thể xác định mã cuộc họp hợp lệ với khả năng thành công là 14%.

Vào tháng 1/2020, Zoom đã bổ sung thêm tính năng cho phép ngăn chặn các truy vấn quét ID cuộc họp, nhưng công cụ zWarDial đã vượt qua tính năng này bằng cách thực hiện truy vấn thông qua trình duyệt Tor.

Source: https://www.businessinsider.sg/protect-zoom-meetings-password-hackers-zoom-bombing-2020-4

https://www.popularmechanics.com/technology/security/a31982009/is-zoom-safe/

Ứng dụng Zoom cũng tồn tại nhiều lỗ hổng bảo mật, gần đây nhất là 3 lỗ hổng đã có mã khai thác. (Chi tiết mã khai thác được đề cập tại phần điểm yếu lỗ hổng của báo cáo).

Một số quốc gia trên thế giới (như Mỹ, Đài Loan…) cũng đã ngăn cấm hoặc khuyến nghị người dùng không sử dụng Zoom để họp trực tuyến vì lo ngại vấn đề bảo mật, quyền riêng tư.

Cơ quan, tổ chức, người dùng khi sử dụng các ứng dụng để họp trực tuyến cần hết sức lưu ý trong việc thiết lập các tính năng bảo mật của ứng dụng, cũng như lựa chọn những ứng dụng minh bạch, có độ đin cậy cao hơn.

Nguy cơ tấn công mạng từ điểm yếu lỗ hổng

Trong tuần, các tổ chức quốc tế đã công bố và cập nhật ít nhất 299 lỗ hổng, trong đó có 68 lỗ hổng mức cao, 145 lỗ hổng mức trung bình, 26 lỗ hổng mức thấp và 60 lỗ hổng chưa đánh giá. Trong đó có ít nhất 45 lỗ hổng cho phép chèn và thực thi mã lệnh.

Hệ thống kỹ thuật của Cục ATTT chủ động rà quét trên không gian mạng Việt Nam, đánh giá, thống kê cho thấy có 07 lỗ hổng/nhóm lỗ hổng trên các sản phẩm, dịch vụ CNTT phổ biến, có thể gây ảnh hưởng lớn đến người dùng ở Việt Nam, như: Nhóm 10 lỗ hổng trong một số thành phần của Apache , Nhóm 10 lỗ hổng trong phần mềm Wordpress , Nhóm 49 lỗ hổng trong các sản phẩm của Apple, Nhóm 08 lỗ hổng trong các thiết bị Lenovo, Nhóm 05 lỗ hổng trong Gitlab , Nhóm 03 lỗ hổng trong Zoom, Nhóm 03 lỗ hổng trong thiết bị của Dell,… Thông tin chi tiết về một số lỗ hổng trên các sản phẩm/dịch vụ phổ biến tại Việt Nam cụ thể như sau:

Một số lỗ hổng trên các sản phẩm/dịch vụ phổ biến tại Việt Nam:

- *Adobe: CVE-2020-3797, CVE-2020-3793,...*
- *Apple: CVE-2015-7334, CVE-2020-9769,...*
- *Gitlab: CVE-2020-10956, CVE-2020-10954,...*
- *Lenovo: CVE-2015-5684, CVE-2015-5684,...*
- *Wordpress: CVE-2020-7947, CVE-2019-6009,...*
- *Zoom: CVE-2020-11500, CVE-2020-11470,...*
- *Dell: CVE-2020-5344, CVE-2020-5347...*

Thông tin điểm yếu lỗ hổng

STT	Sản phẩm/ dịch vụ	Mã lỗi quốc tế	Mô tả ngắn	Ghi chú
1	Apache	CVE-2020-1934 CVE-2019-17564 CVE-2020-1927 …	Nhóm 10 lỗ hổng trong một số thành phần của Apache (HTTP Server, Dubbo NetBeans,…) cho phép đối tượng tấn công tấn công XSS.	Đã có thông tin xác nhận và bản vá
2	Wordpress	CVE-2020-7947 CVE-2020-6009 CVE-2020-6008 …	Nhóm 10 lỗ hổng trong phần mềm Wordpress (LearnDash plugin, Auth0 plugin,…) cho phép đối tượng tấn công chèn và thực thi mã từ xa, tấn công XSS, SQL Injection.	Đã có thông tin xác nhận và bản vá
3	Apple	CVE-2015-7334 CVE-2020-9769 CVE-2020-3847 …	Nhóm 49 lỗ hổng trong các sản phẩm của Apple (watchOS, macOS Catalina, Apple Safari, tvOS,…) cho phép đối tượng tấn công thu thập thông tin, chèn và thực thi mã từ xa.	Đã có thông tin xác nhận và bản vá
4	Lenovo	CVE-2015-5684 CVE-2015-5684 CVE-2015-7334 …	Nhóm 08 lỗ hổng trong một số thành phần và sản phẩm của Lenovo (Lenovo Solution Center,…) cho phép đối tượng bypassed, tấn công thực thi mã từ xa. 01 lỗ hổng có điểm CVSS: 10.0 (đặc biệt nghiêm trọng).	Đã có thông tin xác nhận và bản vá
5	Gitlab	CVE-2020-10956 CVE-2020-10954 CVE-2020-10952 …	Nhóm 05 lỗ hổng trong Gitlab (Gitlab EE/CE 8.11-12.9.1, Gitlab 8.1,…) cho phép đối tượng tấn công thu thập thông tin, tấn công từ chối dịch vụ, tấn công SSRF.	Đã có thông tin xác nhận và bản vá
6	Zoom	CVE-2020-11500 CVE-2020-11470 CVE-2020-11469	Nhóm 03 lỗ hổng trong Zoom (Zoom Client for Meetings <=4.6.9) cho phép đối tượng tấn công truy cập trái phép tài khoản người dùng, tấn công leo thang chiếm quyền cao nhất của hệ thống.	Chưa có thông tin xác nhận và bản vá
7	Dell	CVE-2020-5344 CVE-2020-5347 CVE-2020-5348	Nhóm 03 lỗ hổng trong thiết bị của Dell (Dell EMC, Dell Latitude 7202) cho phép đối tượng tấn công chèn và thực thi mã tùy ý, tấn công từ chối dịch vụ. 01 lỗ hổng có điểm CVSS: 10.0 (đặc biệt nghiêm trọng).	Đã có thông tin xác nhận và bản vá

Thông tin chi tiết lỗ hổng, điểm yếu lưu ý

CVE-2020-7982

CVE-2020-7982 là lỗ hổng trong trình quản lý gói opkg của OpenWRT, phát hiện ngày 16/03/2020, cho phép đối tượng tấn công vượt qua cơ chế kiểm tra tính toàn vẹn khi tải tập tin .ipk từ đó có thể lợi dụng để chèn và thực thi mã từ xa, tấn công giả mạo, kiểm soát thiết bị.

Lỗ hổng ảnh hưởng đến phiên bản OpenWRT 18.06 đến 18.06.6 và 19.07.0; LEDE 17.01.0 đến 17.01.7.

OpenWRT là một hệ điều hành miễn phí, được cài đặt trên hàng triệu thiết bị định tuyến (asus, dlink, linksys,tp-link...), cũng như các thiết bị như điện thoại di động, máy tính bảng,…

Hiện đã có cập nhật bản vá tại phiên bản OpenWRT 18.06.7 và 19.07.1 (phát hành vào tháng 2/2020), để cập nhật phiên bản mới nhất, người dùng truy cập tại:

https://openwrt.org/

.

Source: https://service.khonggianmang.vn/
https://openwrt.org/advisory/2020-01-31-1
https://blog.forallsecure.com/uncovering-openwrt-remote-code-execution-cve-2020-7982
https://nvd. nist.gov/vuln/detail/CVE-2020-7982

CVE-2020-0796

Là lỗ hổng trong giao thức Server Message Block 3.0 (SMBv3), cho phép đối tượng tấn công chèn và thực thi mã từ xa.

Lỗ hổng ảnh hưởng đến các phiên bản như Windows 10 Version 1903, Windows Server Ver 1903 (Server Core installation), Windows 10 Ver 1909, Windows Server Ver 1909 (Server Core installation).

Đối tượng tấn công đã khai thác lỗ hổng tràn bộ đệm trong máy chủ SMB của Microsoft, do lỗi trong cách SMBv3 xử lý các gói dữ liệu nén.

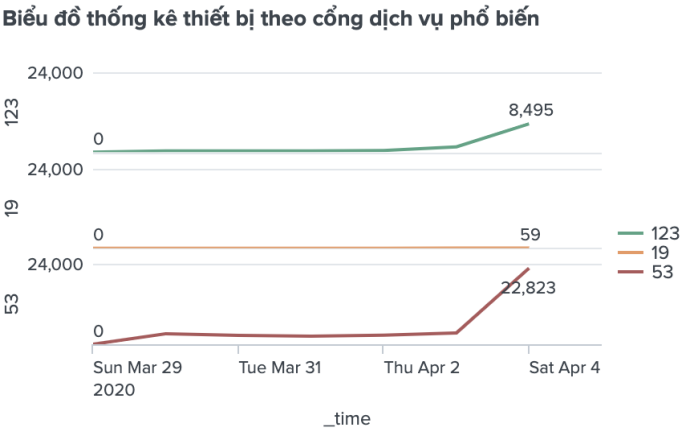
Microsoft đã phát hành bản cập nhật cho Windows 10 phiên bản 1903 và 1909, Windows Server 2019 phiên bản 1903 và 1909.

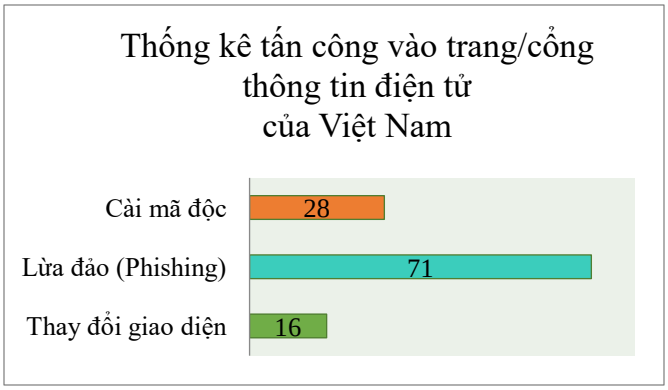
Source: https://service.khonggianmang.vn/
https://securityaffairs.co/wordpress/99507/security/cve-2020-0796-smbv3-bug-fix.html

Thống kê nguy cơ, các cuộc tấn công tại Việt Nam

Tấn công DRDoS

Tuần vừa qua tại Việt Nam, có rất nhiều máy chủ, thiết bị có thể trở thành nguồn phát tán tấn công DRDoS. Trong tuần có **48,939** (giảm so với tuần trước **50,676**) thiết bị có khả năng bị huy động và trở thành nguồn tấn công DRDoS. Các thiết bị này đang mở sử dụng các dịch vụ NTP (123), DNS (53), Chargen (19). Dưới đây là biểu đồ thống kê thiết bị theo cổng dịch vụ phổ biến trong tuần.



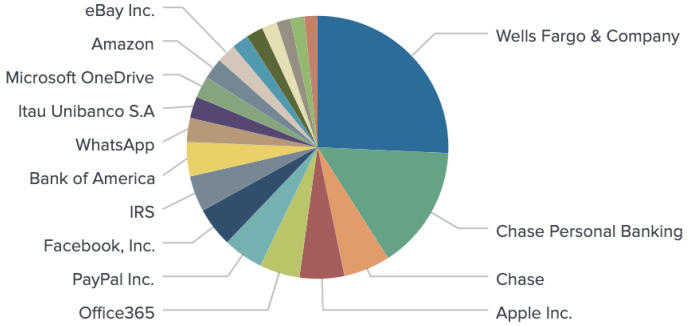


Tấn công Web

Trong tuần, có 115 trường hợp tấn công vào trang/cổng thông tin điện tử của Việt Nam: 16 trường hợp tấn công thay đổi giao diện, 71 trường hợp tấn công lừa đảo (Phishing), 28 trường hợp tấn công cài cắm mã độc.

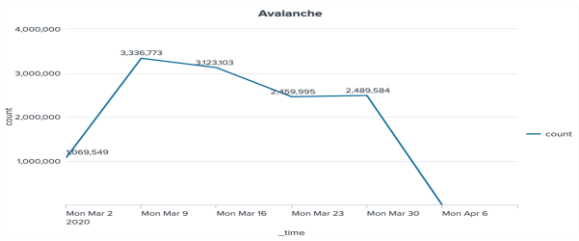
Tấn công Phishing

Trên thế giới có nhiều các trang web giả mạo các tổ chức, doanh nghiệp, nhà cung cấp, dịch vụ lớn như: Các mạng xã hội, ngân hàng, thư điện tử .v.v… Việt Nam có nhiều người dùng các dịch vụ, ứng dụng nước ngoài (cả miễn phí và có phí) như các mạng xã hội, Paypment, Apple, Paypal ..v.v… vì vậy người dùng cần phải hết sức cảnh giác với những trang web giả mạo để ăn trộm tài khoản.

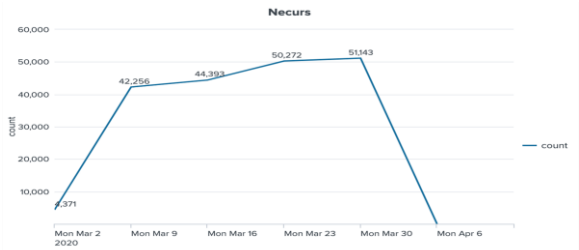


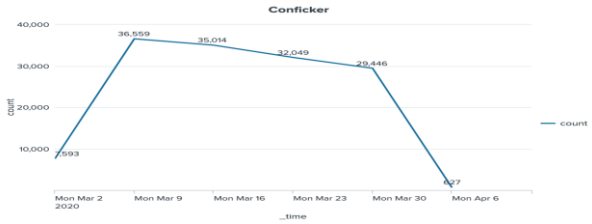
Thống kê nguy cơ, các cuộc tấn công tại Việt Nam

Trong tuần mạng botnet **Avalanche** có 2,489,584 lượt địa chỉ IP kết nối với máy chủ điều khiển tăng so với tuần 13 là 2,459,995.

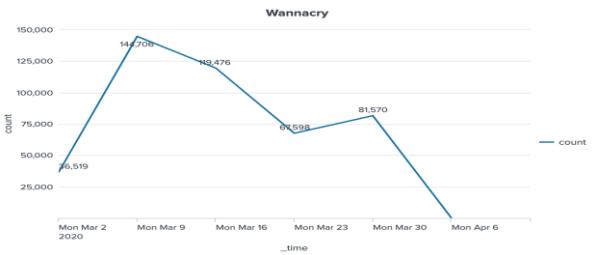


Trong tuần mạng botnet **Necurs** có 51,143 lượt địa chỉ IP kết nối với máy chủ điều khiển tăng so với tuần 13 là 50,272.





Trong tuần mạng botnet **Conficker** có 29,446 lượt địa chỉ IP kết nối với máy chủ điều khiển giảm so với tuần 13 là 32,049.



Trong tuần mạng botnet **Wannacry** có 81,570 lượt địa chỉ IP kết nối với máy chủ điều khiển tăng so với tuần 13 là 67,598.

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

disorderstatus.ru	xjpakmdcfuqe.in
differentia.ru	xjpakmdcfuqe.ru
atomictrivia.ru	amnsreiuojy.ru
iuqerfsodp9ifjaposdfjhgosurijfaewrwergwea.com	track.saygggggames.io
xdqzpbcgrvkj.ru	xjpakmdcfuqe.com
xjpakmdcfuqe.in	xjpakmdcfuqe.biz
disorderstatus.ru	xjpakmdcfuqe.in

Khuyến nghị đối với các cơ quan, đơn vị

HẠN CHẾ TẤN CÔNG TỪ CHỐI DỊCH VỤ

Đối với nguy cơ bị lợi dụng để thực hiện tấn công từ chối dịch vụ nêu tại mục 3: Kiểm tra các dịch vụ sử dụng giao thức UDP, hạn chế tối đa việc mở các cổng dịch vụ sử dụng giao thức UDP. Trong trường hợp sử dụng phải thường xuyên theo dõi và cập nhật bản vá lỗ hổng bảo mật cho dịch vụ, đồng thời cấu hình cứng hóa dịch vụ, hạn chế tối đa truy cập đến và đi liên quan đến địa chỉ/dải địa chỉ không cần thiết.

PHÒNG TRÁNH TẤN CÔNG WEB

Kiểm tra và xử lý các thiết bị trong toàn bộ hệ thống mạng nếu có dấu hiệu kết nối đến các tên miền độc hại Cục ATTT đã chia sẻ, đặc biệt là các tên miền đã nêu trong mục 5.2 báo cáo này.

CẬP NHẬT BẢN VÁ LỖ HỔNG

Theo dõi và cập nhật bản vá cho các lỗ hổng, đặc biệt là lỗ hổng nêu tại mục 2 báo cáo này.

LƯU Ý KIỂM TRA VÀ XỬ LÝ CÁC TÊN MIỀN ĐỘC HẠI

Nhằm tránh việc bị các đối tượng tấn công lợi dụng các trang web để thực hiện các hành vi gây mất an toàn thông tin như đã nêu trong mục 4, các cơ quan tổ chức cần phải thường xuyên kiểm tra, rà soát máy chủ web để kịp thời phát hiện và cập nhật.

CHỦ ĐỘNG KIỂM TRA, RÀ SOÁT, BÓC GỠ MÃ ĐỘC

Chủ động kiểm tra, rà soát, bóc gỡ mã độc ra khỏi hệ thống mạng. Cục ATTT sẵn sàng phối hợp với các cơ quan tổ chức tiến hành kiểm tra và bóc gỡ mã độc botnet trên hệ thống của cơ quan đơn vị. Để xác minh các máy tính bị nhiễm mã độc botnet, Quý đơn vị có thể liên hệ với Cục ATTT theo thông tin bên dưới để phối hợp thực hiện.

Thông tin liên hệ:
Trung tâm Giám sát an toàn không gian mạng quốc gia
024.3209.1616 - ais@mic.gov.vn
Tầng 16, số 115 Trần Duy Hưng, quận Cầu Giấy, Tp. Hà Nội

RSG – Báo cáo, tài liệu chuyên ngành

(1) Báo cáo cảnh báo lần thứ 3 trong 3 tháng liên tiếp của FBI về các cuộc tấn công vào chuỗi cung ứng và một số cuộc tấn công cũng đã nhắm vào ngành công nghiệp chăm sóc sức khỏe.

https://www.documentcloud.org/documents/6821581-FLASH-CP-000111-MW-Downgraded-Version.html

(2) Báo cáo chi tiết của của Guardicore, mã độc chiếm quyền điều khiển máy chủ cơ sở dữ liệu MSSQL vẫn đang hoạt động và lây nhiễm khoảng 3.000 cơ sở dữ liệu MSSQL mới mỗi ngày.

https://www.guardicore.com/2020/04/vollgar-ms-sql-servers-under-attack/

(3) Báo cáo của Europol chi tiết về cách mà tội phạm mạng đã phản ứng và phát triển kể từ khi bắt đầu đại dịch COVID-19! Theo báo cáo, ngoài tấn công hỗ trợ và mã độc ransomware và từ chối dịch vụ DDoS, kẻ tấn công còn tập trung khai thác tình dục trẻ em trên mạng thông qua các diễn đàn ngầm.

https://www.europol.europa.eu/sites/default/files/documents/catching_the_virus_cybercrime_disinformation_and_the_covid-19_pandemic_0.pdf

(4) Báo cáo của Google về dữ liệu di động của Việt Nam.

https://www.gstatic.com/covid19/mobility/2020-03-29_VN_Mobility_Report_en.pdf

(5) Các lỗ hổng cho phép khai thác máy ảnh trong safari của apple.

https://www.darkreading.com/vulnerabilities---threats/researcher-hijacks-ios-macos-camera-with-three-safari-zero-days/d/d-id/1337486

Tài liệu lưu trữ:

Chuyên mục **Báo cáo định kỳ** trên HỆ THỐNG CẢNH BÁO ĐIỂM YẾU VÀ RÀ SOÁT LỖ HỔNG BẢO MẬT TỰ ĐỘNG tại địa chỉ https://service.khonggianmang.vn/