BỘ THÔNG TIN VÀ TRUYỀN THÔNG
CỤC AN TOÀN THÔNG TIN

CỘNG HÒA XÃ HỘI CHỦ NGHĨA VIỆT NAM
Độc lập - Tự do - Hạnh phúc

Số: /BC-CATTT

Hà Nội, ngày tháng 4 năm 2019

TÓM TẮT
Tình hình an toàn thông tin đáng chú ý trong tuần 14/2019
(từ ngày 01/4/2019 đến ngày 07/4/2019)

BẢNG TỔNG HỢP

1. Cuối tháng 3/2019, Brunei quyết định sẽ thành lập một Trung tâm an toàn không gian mạng quốc gia để bảo vệ Brunei khỏi các mối đe dọa trên không gian mạng trước chiến lược của các chính phủ bên ngoài với mục tiêu khai thác công nghệ nhằm tìm kiếm các lợi ích kinh tế.

2. Để chuẩn bị ứng phó các cuộc tấn công mạng xuyên biên giới quy mô lớn, một Nghị định thư về ứng phó khẩn cấp thực thi pháp luật của EU đã được Hội đồng Liên minh châu Âu thông qua.

3. Phát hiện xu hướng tấn công mạng vào các máy chủ thư điện tử Zimbra của Việt Nam kết hợp khai thác các lỗ hổng bảo mật CVE-2016-9924, CVE-2018-20160, CVE-2019-9670. Việc kết hợp khai thác các lỗ hổng bảo mật này cho phép đối tượng tấn công đưa tập tin độc hại lên máy chủ và kiểm soát hệ thống thư điện tử..

4. Báo cáo được xây dựng dựa trên các nguồn thông tin thu thập được từ hệ thống phân tích và chia sẻ nguy cơ tấn công mạng Việt Nam (https://ti.khonggianmang.vn). Thông tin chi tiết về Hệ thống tại *Phụ lục kèm theo*.

1. Điểm tin đáng chú ý

1.1. Cuối tháng 3/2019, Brunei quyết định sẽ thành lập một Trung tâm an toàn không gian mạng quốc gia để bảo vệ Brunei khỏi các mối đe dọa trên không gian mạng trước chiến lược của các chính phủ bên ngoài với mục tiêu khai thác công nghệ nhằm tìm kiếm các lợi ích kinh tế.

Trong cuộc họp của Hội đồng lập pháp (LegCo), Bộ trưởng Giao thông và Truyền thông Brunei cho rằng một hệ sinh thái an toàn và bảo mật trên không gian mạng là cần thiết để nâng cao vị thế của Brunei, để Brunei trở thành một

"quốc gia thông minh". Brunei đang nỗ lực sử dụng công nghệ để cải thiện cuộc sống của người dân.

Việc thành lập Trung tâm an toàn không gian mạng quốc gia sẽ cho phép nước này giám sát và phối hợp các giải pháp ở cấp độ quốc gia để chống lại các mối đe dọa an toàn trên không gian mạng.

1.2. Để chuẩn bị ứng phó các cuộc tấn công mạng xuyên biên giới quy mô lớn, một Nghị định thư ứng phó khẩn cấp thực thi pháp luật của EU đã được Hội đồng Liên minh châu Âu thông qua. Nghị định thư là một phần của Kế hoạch chi tiết của EU về phối hợp ứng phó với các cuộc tấn công mạng và khủng hoảng an toàn thông tin mạng xuyên biên giới quy mô lớn. Nó có vai trò như một công cụ hỗ trợ các cơ quan thực thi pháp luật của EU trong việc đưa ra các phản ứng ngay lập tức trước các cuộc tấn công mạng xuyên biên giới thông qua đánh giá nhanh, chia sẻ các thông tin quan trọng một cách kịp thời và an toàn cùng với việc phối hợp hiệu quả với quốc tế.

Trong năm 2017, các cuộc tấn công mạng gây thiệt hại chưa từng có trên diện rộng của mã độc tống tiền WannaCry và NotPetya cho thấy khả năng phản ứng trước các cuộc tấn công mạng hiện nay là chưa đủ để giải quyết một cách hiệu quả trước sự phát triển nhanh chóng của các nhóm tấn công mạng.

Nghị định thư xác định quy trình, vai trò, trách nhiệm của các tổ chức trong EU và kênh liên lạc an toàn, liên tục 24/7 để trao đổi các thông tin quan trọng; cũng như sự phối hợp và cơ chế chống xung đột một cách tổng thể. Tổ chức này cố gắng bổ sung các cơ chế quản lý khủng hoảng bằng cách xây dựng các hoạt động xuyên quốc gia một cách hiệu quả và tạo điều kiện hợp tác với các bên liên quan của EU với quốc tế. Cùng với đó tạo điều kiện cho sự hợp tác với cộng đồng mạng và an toàn thông tin và đối tác khu vực tư nhân có liên quan.

1.3. Trong những tháng đầu năm 2019, tình hình an toàn thông tin (ATTT) trên thế giới cũng như tại Việt Nam diễn biến phức tạp, khó lường. Các lỗ hổng, điểm yếu ATTT bị đối tượng lợi dụng để tấn công mạng nguy hiểm, phát tán mã độc ngày càng phổ biến.

Qua công tác theo dõi, giám sát trên không gian mạng, Trung tâm Giám sát an toàn thông tin mạng quốc gia (NCSC) thuộc Cục An toàn thông tin (Cục ATTT) phát hiện xu hướng tấn công mạng vào các máy chủ thư điện tử Zimbra của Việt Nam kết hợp khai thác các lỗ hổng bảo mật CVE-2016-9924, CVE-2018-20160, CVE-2019-9670. Việc kết hợp khai thác các lỗ hổng bảo mật này cho phép đối tượng tấn công đưa tập tin độc hại lên máy chủ và kiểm soát hệ thống thư điện tử.

Hiện tại Zimbra đã phát hành bản vá cho các phiên bản Zimbra 8.7.11 và 8.8.x, chưa có bản vá cho các phiên bản khác.

Tại việt Nam qua kiểm tra sơ bộ NCSC phát hiện có **717** tên miền của máy chủ đang sử dụng phần mềm Zimbra. Trong đó có **35** tên miền của cơ quan nhà nước, **12** tên miền của ngân hàng và nhiều cơ quan tổ chức lớn khác.

Nhằm bảo đảm an toàn thông tin, phòng tránh các nguy cơ mất an toàn thông tin thông qua lỗ hổng này, Cục ATTT yêu cầu các cơ quan, tổ chức, doanh nghiệp đang sử dụng thư điện tử Zimbra thực hiện:

- Tăng cường các biện pháp bảo đảm an toàn thông tin cho toàn bộ hệ thống.

- Rà soát lại toàn bộ máy chủ thư điện tử Zimbra để phát hiện và loại bỏ các tập tin **.jsp** có dấu hiệu độc hại mà đối tượng tấn công đã đưa lên hệ thống. Đặc biệt thư mục .../webapps/zimbra/downloads/

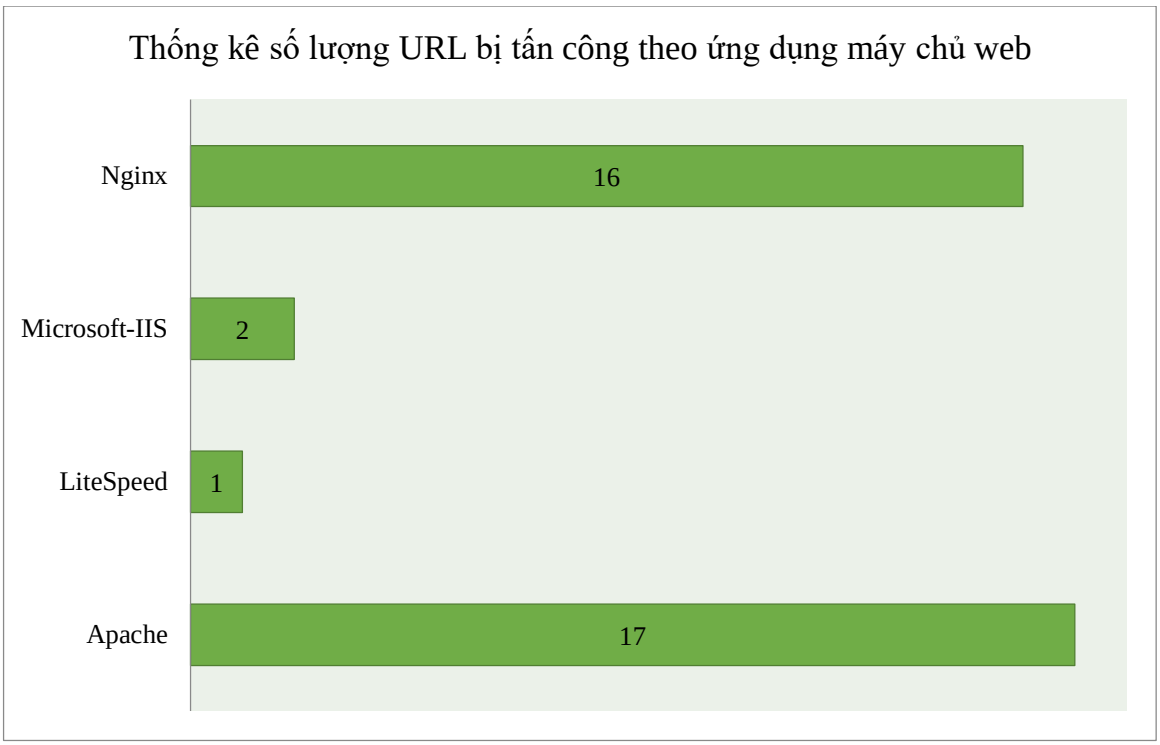
- Rà soát và kiểm tra phiên bản máy chủ thư điện tử đang sử dụng phần mềm Zimbra và cập nhật/nâng cấp lên phiên bản Zimbra mới nhất;

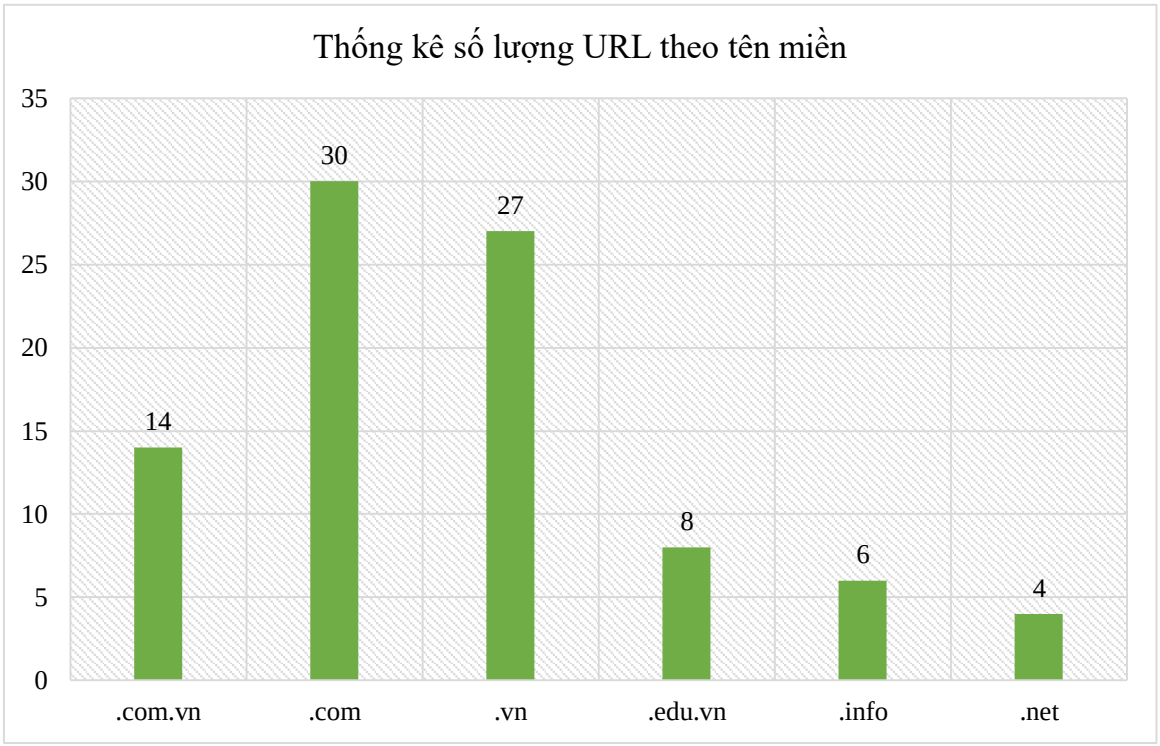
- Trong trường hợp chưa thể nâng cấp cần kiểm tra các phiên bản đang sử dụng và vá các điểm yếu, lỗ hổng đã biết để ngăn chặn việc khai thác kết hợp từ nhiều lỗ hổng đã biết này, và hạn chế việc truy cập vào cổng quản trị. Tham khảo tại: https://ti.khonggianmang.vn/dashboard/news/p/0day-zimbra-tu-nhieu-lo-hong-da-biet/.

2. Tình hình tấn công gây nguy hại trên các trang web tại Việt Nam

Qua theo dõi, trích xuất thông tin từ hệ thống kỹ thuật thời gian qua, Cục ATTT nhận thấy trên không gian mạng đang tồn tại nhiều trang web Việt Nam (bao gồm cả những trang web sử dụng dịch vụ máy chủ nước ngoài) bị tấn công, lợi dụng để thực hiện các hành vi gây mất an toàn thông tin như: phát tán thư rác; tấn công từ chối dịch vụ; cài đặt và phát tán các loại mã độc (gần đây nhất là cài đặt và phát tán mã độc để đào tiền ảo); lưu trữ các mã khai thác điểm yếu lỗ hổng một cách tự động (như lỗ hổng trên trình duyệt hay các thành phần mở rộng của trình duyệt mà người dùng sử dụng .v.v…).

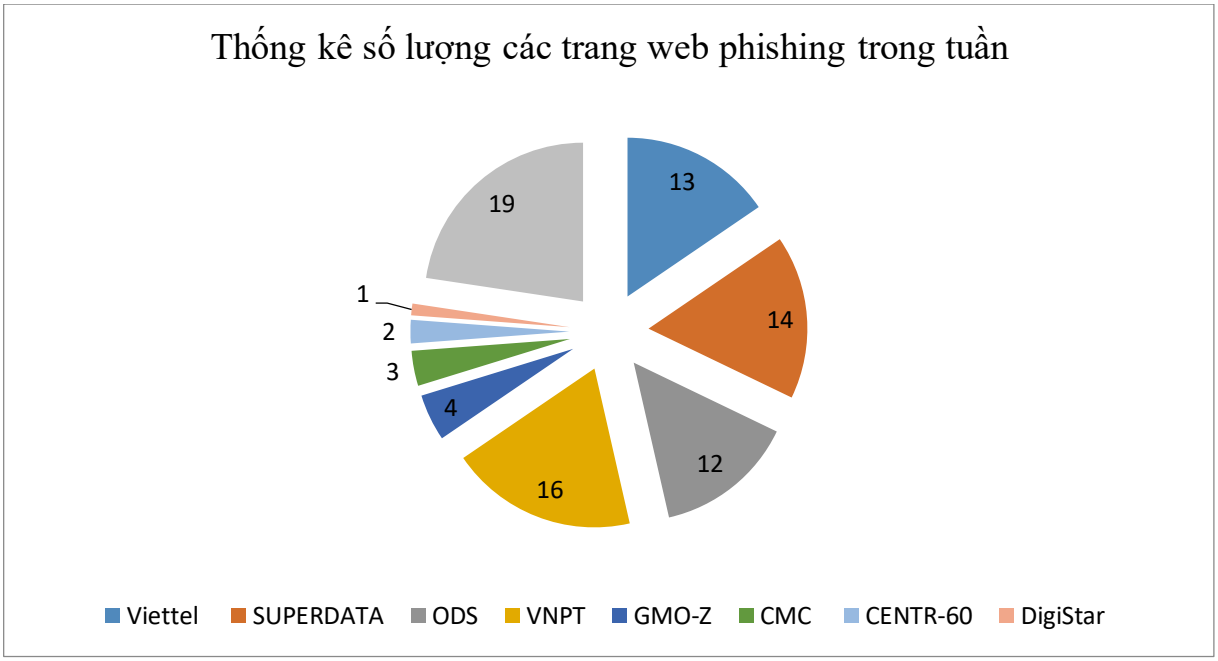
Trong tuần, Cục ATTT ghi nhận có ít nhất **89** đường dẫn (URL) trên các trang web tại Việt Nam bị tấn công, lợi dụng để thực hiện các hành vi gây mất an toàn thông tin. Trong đó, thống kê, phân loại các đường dẫn này theo loại ứng dụng máy chủ web (IIS, Apache …) và nhà cung cấp cụ thể như sau:



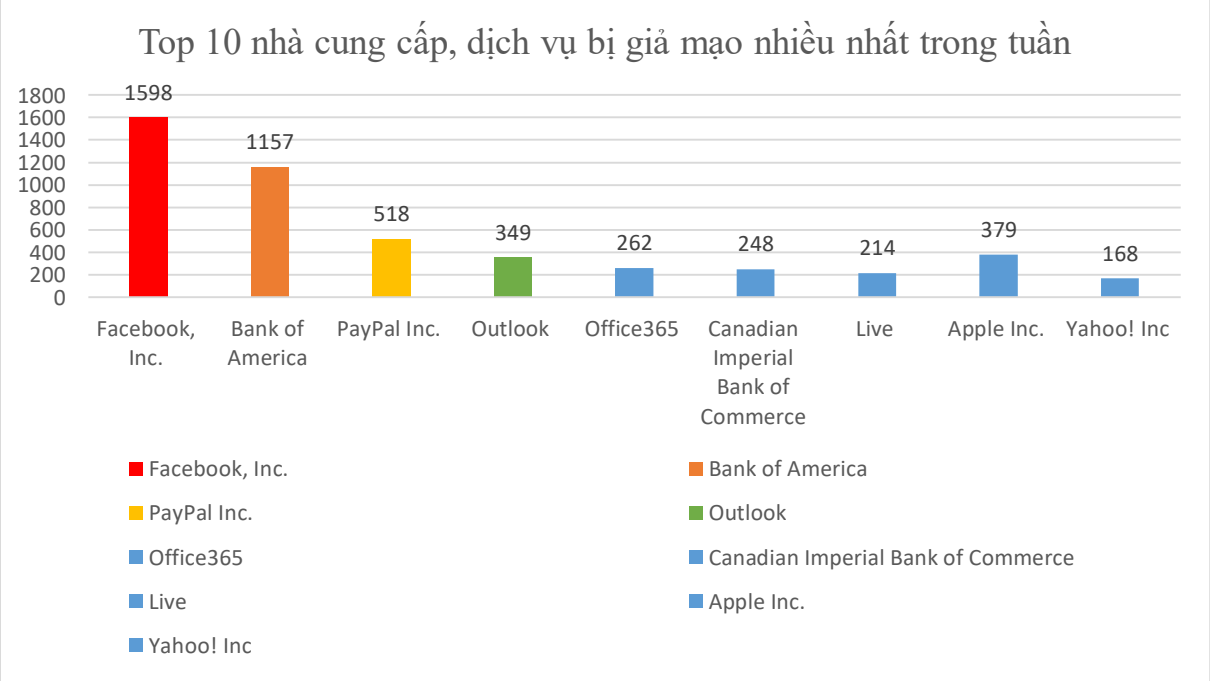


3. Tình hình tấn công lừa đảo (Phishing) trong tuần

3.1. Qua thu thập, theo dõi, trích xuất từ hệ thống kỹ thuật, Cục ATTT còn ghi nhận có ít nhất **84** trang web đặt tại Việt Nam bị lợi dụng để thực hiện tấn công Phishing trong tuần.



3.2. 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.

4. Lỗ hổng/điểm yếu an toàn thông tin trong tuần

4.1. Trong tuần, các tổ chức quốc tế đã công bố và cập nhật ít nhất 385 lỗ hổng, trong đó có 89 lỗ hổng mức cao, 108 lỗ hổng mức trung bình, 22 lỗ hổng mức thấp và 166 lỗ hổng chưa đánh giá; 1 lỗ hổng đã có mã khai thác.

4.2. Hệ thống kỹ thuật của Cục ATTT chủ động rà quét trên không gian mạng Việt Nam, đánh giá, thống kê cho thấy có 04 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 185 lỗ hổng trong một số sản phẩm của Apple; Nhóm 18 lỗ hổng trên phần mềm IBM; Nhóm 72 lỗ hổng trên phần mềm Jenkins ...v.v.

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

STT	Sản phẩm/ dịch vụ	Mã lỗi quốc tế	Mô tả ngắn	Ghi chú
1	IBM	CVE-2018-1936 CVE-2019-4014 CVE-2018-1640 CVE-2018-1906 CVE-2018-1917 CVE-2018-1618 CVE-2018-1622 ...	Nhóm 18 lỗ hổng trên một số sản phẩm, ứng dụng của IBM (API Connect, DB2 Linux/ Windows, Rational Engineering Lifecycle Manage, IBM SDK, WebSphere Application Server...) cho phép đối tượng tấn công thực hiện thu thập thông tin, khai thác các lỗi tràn bộ đệm để chèn và thực thi mã lệnh, tấn công leo thang.	Đã có thông tin xác nhận và bản vá
2	Apple	CVE-2018-4126 CVE-2018-4327 CVE-2018-4268 CVE-2018-4291 ...	Nhóm 185 lỗ hổng trong một số sản phẩm của Apple. Một ứng dụng độc hại truy cập tài khoản, tự động mở khóa AppleIDs của người dùng cục bộ và thực thi mã tùy ý với đặc quyền của hệ thống. Sự cố này ảnh hưởng đến các phiên bản trước IOS 12, macOS Mojave 10.14, tvOS 12, watchOS 5, Itunes 12.9	Đã có thông tin xác nhận và bản vá

			cho Windows, iCloud.	
3	Jenkins	CVE-2019-10298 CVE-2019-1003096 CVE-2019-1003098 CVE-2019-10294 CVE-2019-10289 …..	Nhóm 72 lỗ hổng trên phần mềm Jenkins (phần mềm sử dụng trong phát triển phần mềm) cho phép đối tượng tấn công thu thập thông tin xác thực lưu trữ trong cấu hình của Plugin, một số lỗ hổng cho phép chèn và thực thi mã lệnh.	Chưa có thông tin xác nhận và bản vá
4	Cisco	CVE-2019-1827 CVE-2019-1828 ……	Nhóm 02 lỗ hổng trên một số sản phẩm của Cisco (các dòng switch Nexus, NX-OS, FXOS Software,) cho phép truy cập và thông tin nhạy cảm lưu trữ trên hệ thống, chèn và thực thi mã lệnh để chiếm quyền kiểm soát thiết bị.	Đã có thông tin xác nhận và bản vá

5. Hoạt động một số mạng botnet, APT, mã độc tại Việt Nam

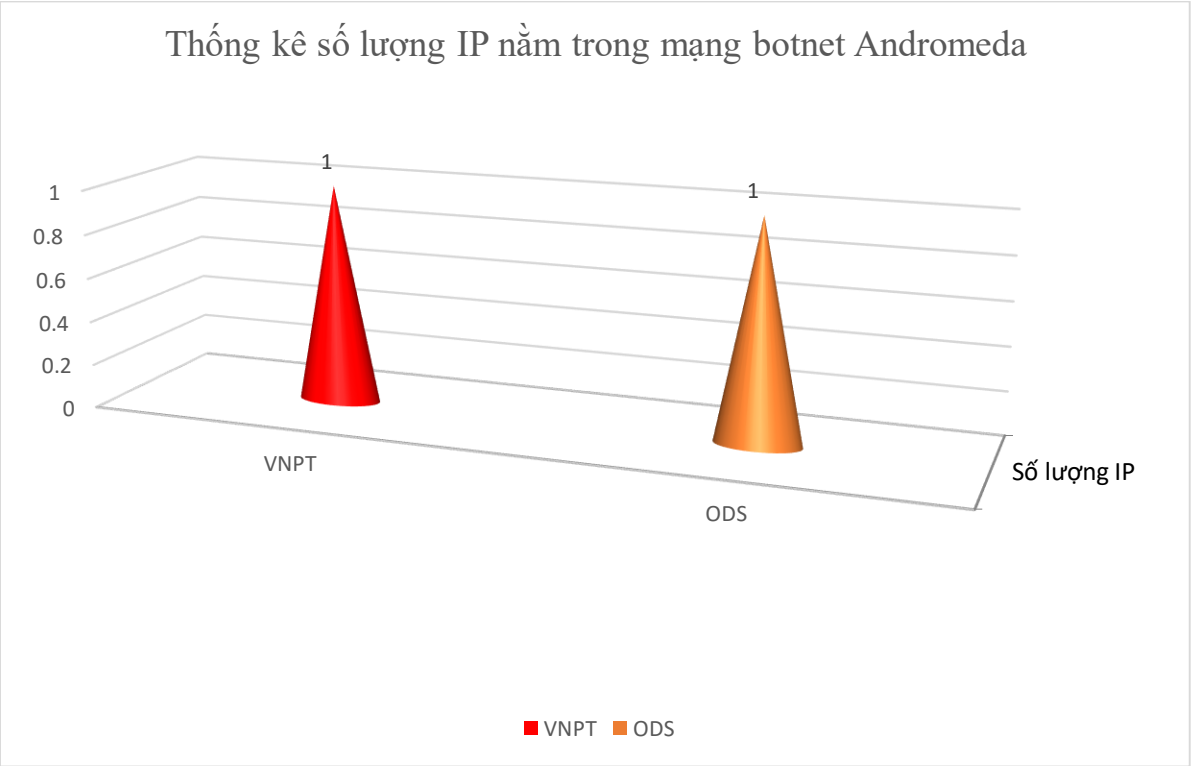
5.1. Mạng botnet Andromeda

Botnet Andromeda, còn được gọi là Win32/Gamarue đã bắt đầu xuất hiện và lây nhiễm vào các máy tính từ năm 2011. Đối tượng chính của cuộc tấn công mã độc này là các doanh nghiệp sử dụng thẻ thanh toán.

Mục đích chính của Andromeda botnet là để phát tán các dòng mã độc khác nhằm phục vụ các cuộc tấn công phần mềm độc hại toàn cầu. Mạng botnet Andromeda bao gồm và có liên quan đến ít nhất 80 họ phần mềm độc hại, trong đó chủ yếu là họ mã độc Point of Sale (POS), ví dụ như GamaPOS. Trong sáu tháng cuối năm 2017, nó đã bị phát hiện lây nhiễm khoảng hơn 1 triệu máy tính mỗi tháng.

Mã độc Andromeda có các chức năng chính như: Keylogging; Rootkit; Truy cập từ xa ẩn; Thu thập thông tin đăng nhập từ trình duyệt.

Các tổ chức quốc tế cũng đã hợp tác với nhau để ngăn chặn các máy chủ và khoảng 1500 tên miền độc hại được sử dụng để phát tán và kiểm soát mạng botnet này.



5.2. Danh sách IP/tên miền máy chủ điều khiển của mạng botnet Andromeda

TT	Tên miền/IP
1	bklfhppldrsh.org
2	ebvonryncldr.com

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

TT	Tên miền/IP
1	plpanaifheaighai.com
2	n.hmiblgoja.ru
3	ajkeahkcueafuiaeuf.ru
4	iuefgauiaiduihgs.com
5	mokoaehaeihgiaheih.ru
6	43trfdsds.com
7	bszotsjovih.com
8	https://kisscherrygirls.com/xefyzznumsa
9	mel.cloudcontentsmak.com
10	strikotunrev.top
11	2344t554ddfr.com
12	dnshkjashsdk3d11144d.ru
13	pudloxan.com

6. Khuyến nghị đối với các cơ quan, đơn vị

Nhằm bảo đảm an toàn thông tin trong hệ thống mạng của các cơ quan, tổ chức, Cục ATTT khuyến nghị:

- 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 2,* các cơ quan tổ chức cần phải thường xuyên kiểm tra, rà soát máy chủ web để kịp thời phát hiện và cập nhật các điểm yếu, lỗ hổng trên các máy chủ web thuộc cơ quan, tổ chức mình

- Người dùng cần phải hết sức cảnh giác với những trang web giả mạo để ăn trộm tài khoản, đặc biệt là các trang web giả mạo các ứng dụng, dịch vụ phổ biến như đã nêu trong *mục 3.2* báo cáo này.

- Theo dõi và cập nhật bản vá cho các lỗ hổng, đặc biệt là lỗ hổng nêu tại *mục 4.3* báo cáo này.

- 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.

- 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* báo cáo này.

Thông tin liên hệ Cục An toàn thông tin, tầng 8, số 115 Trần Duy Hưng, quận Cầu Giấy, TP. Hà Nội; số điện thoại: 024.3943.6684; thư điện tử ais@mic.gov.vn.

Trân trọng./.

Nơi nhận:
- Bộ trưởng và các Thứ trưởng (để b/c);
- Thư ký Lãnh đạo Bộ;
- Đơn vị chuyên trách về CNTT các bộ, ngành;
- Sở TT&TT các tỉnh, thành phố trực thuộc TW;
- Cục KSTTHC, Văn phòng Chính phủ;
- Vụ Khoa giáo - Văn xã, Văn phòng Chính phủ;
- Trung tâm CNTT, Văn phòng Trung ương Đảng;
- Trung tâm CNTT, Văn phòng Quốc Hội; (email)
- Trung tâm CNTT, Văn phòng Chủ tịch nước;
- Các Tập đoàn kinh tế; Tổng công ty nhà nước; Tổ chức tài chính và Ngân hàng;
- Cơ quan, đơn vị thuộc Bộ;
- Lãnh đạo Cục;
- Lưu: VT, NCSC.

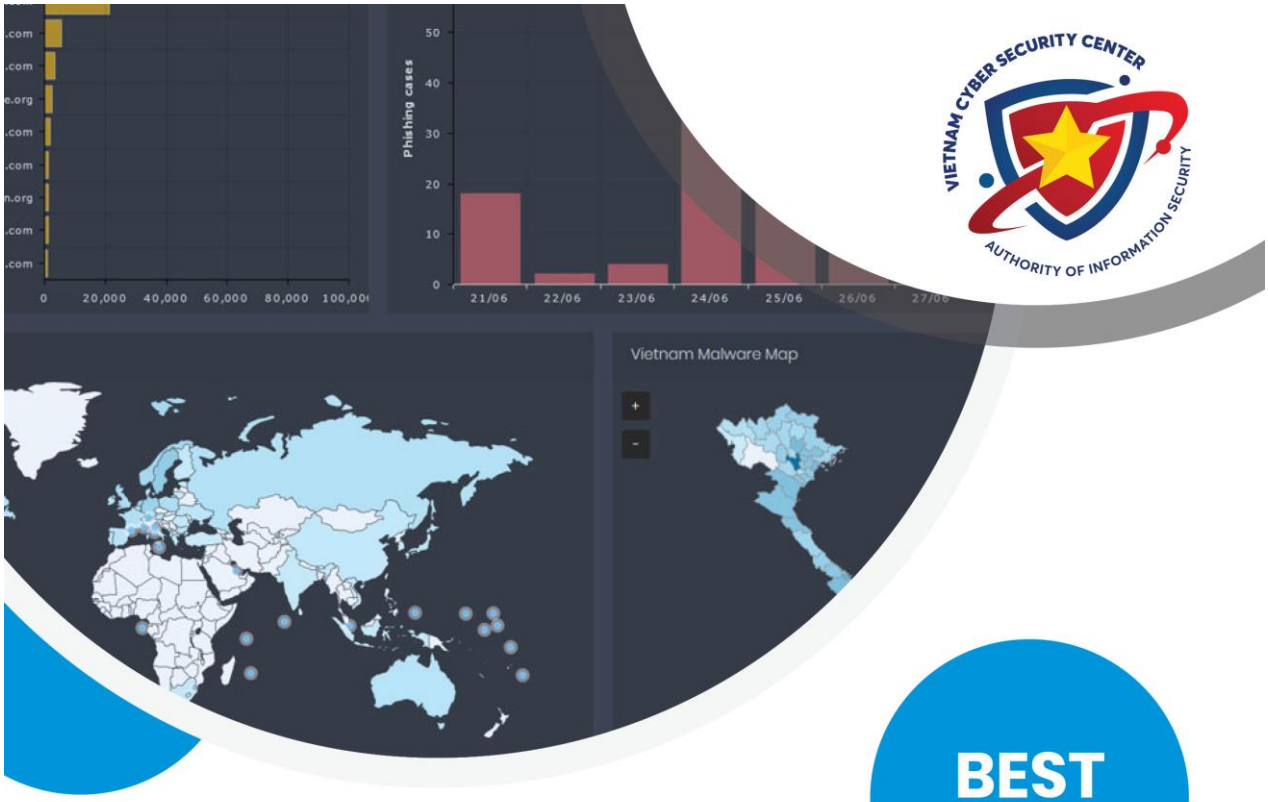
KT. CỤC TRƯỞNG
PHÓ CỤC TRƯỞNG

Nguyễn Huy Dũng

PHỤ LỤC

Hệ thống phân tích và chia sẻ nguy cơ tấn công mạng Việt Nam

https://ti.khonggianmang.vn



HỆ THỐNG PHÂN TÍCH VÀ CHIA SẺ NGUY CƠ TẤN CÔNG MẠNG VIỆT NAM

Vietnam Threat Intelligence Portal

GIỚI THIỆU VỀ HỆ THỐNG

Hệ thống phân tích và chia sẻ nguy cơ tấn công mạng Việt Nam là hệ thống cho phép thu thập, phân tích và chia sẻ thông tin trực tiếp về dấu hiệu, nguy cơ và cuộc tấn công mạng đang xảy ra trên hệ thống của các cơ quan, đơn vị. Mục tiêu của hệ thống nhằm tăng cường việc kết nối chia sẻ thông tin giữa các cơ quan, đơn vị, tổ chức.

ĐIỂM NỔI BẬT CỦA HỆ THỐNG

Khi truy cập vào hệ thống, các cơ quan, đơn vị sẽ được chia sẻ các thông tin theo thời gian thực về: các dấu hiệu, hình thức tấn công mạng trên hệ thống thông tin của mình được Cục An toàn thông tin tổng hợp, phân tích và xử lý từ nhiều tổ chức trên thế giới.

- **Cập nhật liên tục nguy cơ tấn công mạng:** Cập nhật danh sách các máy chủ điều khiển C&C, IP, Hash độc hại (APT, Botnet, Phishing, Ransomeware...) thường được sử dụng để tấn công vào Việt Nam.
- **Giám sát và cảnh báo sớm tấn công mạng:** Giám sát và cảnh báo sớm các tấn công vào hệ thống của tổ chức và các kết nối bất thường từ hệ thống mạng ra ngoài. Đánh giá định kỳ mức độ an toàn thông tin của hệ thống.

THÔNG TIN LIÊN HỆ

Email: ais@mic.gov.vn | Website: Khonggianmang.vn
Phone: +84 24 3209 6789 | Fax: +84 24 3209 6789
Address: Tầng 8 - 115 Trần Duy Hưng - Cầu Giấy - Hà Nội

BEST SERVICES

THÔNG TIN CẬP NHẬT

Hệ thống liên tục cập nhật và chia sẻ các thông tin về nguy cơ tấn công mạng đối với Việt Nam.

DỮ LIỆU ĐA DẠNG

Dữ liệu được tổng hợp từ các tổ chức Quốc tế, Việt Nam, từ các sensor, honeypot,...

CẢNH BÁO TỨC THÌ

Hệ thống cảnh báo sớm các tấn công và cảnh báo các kết nối bất thường từ hệ thống mạng tổ chức.

CÁC NỘI DUNG CỦA DỊCH VỤ

HOẠT ĐỘNG CỦA CHÚNG TÔI

Cảnh báo sớm ATTT

Hỗ trợ các tổ chức cảnh báo sớm các nguy cơ tấn công mạng.

Giám sát ATTT

Thực hiện cung cấp dịch vụ giám sát ATTT từ xa và tổng thể.

Đánh giá ATTT

Cung cấp dịch vụ đánh giá ATTT từ Ứng dụng, Hạ tầng, Kiến trúc...

Xử lý tấn công mạng

Hỗ trợ xử lý tấn công mạng cục bộ và trên diện rộng cho các tổ chức.

ORGANIZATION
Dành cho Tổ chức

- Danh sách máy chủ điều khiển độc hại.
- Danh sách IP độc hại.
- Danh sách mã hash độc hại.
- Danh sách website lừa đảo.
- Thông tin ATTT cập nhật.
- Báo cáo tổng hợp hàng tuần.

GOVERMENT
Dành cho cơ quan Chính phủ

- Đầy đủ thông tin của tài khoản Organization.
- Cập nhật điểm yếu, lỗ hổng nguy hiểm và phổ biến đối với Việt Nam.
- Giám sát tình trạng Up/Down của hệ thống.
- Giám sát và cảnh báo về mã độc/ backlink trên Website.
- Cảnh báo các tấn công mạng vào hệ thống công khai của tổ chức.
- Cảnh báo các kết nối bất thường, đáng ngờ từ hệ thống của tổ chức.
- Cảnh báo tức thì qua Email.
- Hỗ trợ kỹ thuật qua Email

ENTERPRISE
Dành cho Doanh nghiệp

- Đầy đủ thông tin của tài khoản Goverment.
- Danh sách domain độc hại C&C được sử dụng tấn công APT vào Việt Nam.
- Danh sách IP, Hash sử dụng tấn công có chủ đích APT vào Việt Nam.
- Cập nhật các thông tin có liên quan đến tổ chức, website giả mạo tổ chức...nếu có.
- Cập nhật các tin tức, phân tích kỹ thuật mới nhất về tấn công có chủ đích APT.
- Đánh giá các điểm yếu, lỗ hổng bảo mật định kỳ đối với các hệ thống công khai (IP và Domain) của tổ chức.
- Cảnh báo tức thì qua SMS.
- Hỗ trợ kỹ thuật qua Email.
- Hỗ trợ kỹ thuật Hotline.

LIÊN HỆ ĐĂNG KÝ SỬ DỤNG:

Email: ais@mic.gov.vn | **Website:** Khonggianmang.vn | **Phone:** +84 24 3209 6789
Address: 115 - Trần Duy Hưng - Cầu Giấy - Hà Nội