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: **35**/BC-CATTT

Hà Nội, ngày 07 tháng 08 năm 2018

TÓM TẮT
Tình hình an toàn thông tin đáng chú ý trong tuần 31/2018
(từ ngày 30/7/2018 đến ngày 05/8/2018)

BẢNG TỔNG HỢP

1. Ngày 31/7/2018, tại Hà Nội diễn ra Lễ họp báo công bố tổ chức cuộc thi An toàn không gian mạng toàn cầu WhiteHat Grand Prix 2018, chủ đề **Truyền thuyết Việt Nam - Legends of Vietnam**. Sau Vòng Sơ loại thi online, 10 đội thi quốc tế xuất sắc nhất sẽ quy tụ tại Hà Nội để tham gia vòng Chung kết theo hình thức đối kháng trực tiếp (Attack/Defence onsite).

2. Bộ trưởng Nội vụ Đức, ông Horst Seehofer cho rằng nước này cần phải có những hành động phản công trên không gian mạng. Hiện nay, Chính phủ Đức đang cân nhắc dự luật cho phép đáp trả một cách chủ động trước các cuộc tấn công mạng của nước ngoài vào các hệ thống thông tin của nước Đức.

3. Ngày 03/8/2018, qua hoạt động theo dõi và thu thập thông tin, Cục An toàn thông tin đã phát hiện ít nhất 171 địa chỉ IP của Việt Nam (tương ứng với 171 hệ thống thông tin đằng sau) có thể đã bị lây nhiễm mã độc Emotet. Đây là mã độc đang gây ảnh hưởng trên diện rộng, với trên 5.000 tổ chức ở 170 quốc gia đã bị ảnh hưởng (hơn 70.000 địa chỉ IP public và hơn 4000 ASN được phát hiện có hoạt động liên quan đến mã độc này).

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. Ngày 31/7/2018, tại Hà Nội diễn ra Lễ họp báo công bố tổ chức cuộc thi An toàn không gian mạng toàn cầu WhiteHat Grand Prix 2018, chủ đề

Truyền thuyết Việt Nam - Legends of Vietnam. Sau Vòng Sơ loại thi online, 10 đội thi quốc tế xuất sắc nhất sẽ quy tụ tại Hà Nội để tham gia vòng Chung kết theo hình thức đối kháng trực tiếp (Attack/Defence onsite). Ban Tổ chức cho biết đây là lần đầu tiên một cuộc thi an toàn không gian mạng quy mô toàn cầu được tổ chức thi đấu trực tiếp tại Việt Nam.

WhiteHat Grand Prix 2018 do Cục An toàn thông tin, Bộ Thông tin và Truyền thông phối hợp cùng Diễn đàn WhiteHat.vn tổ chức. Điểm thú vị so với các cuộc thi an toàn thông tin mạng khác là WhiteHat Grand Prix qua từng năm đều mang một thông điệp về đất nước, con người Việt Nam. Chủ đề cuộc thi năm 2015 là ***"Hello Vietnam"*** với nhưng danh lam, thắng cảnh của Việt Nam, năm 2016 là ***"Discovering Vietnam"*** với những món ngon trong Ẩm thực Việt, năm 2017 là ***"Vietnam Heritages"*** giới thiệu những di sản văn hóa đậm đà bản sắc dân tộc. Năm 2018 là "legends of Vietnam" sẽ khám phá những truyền thuyết của đất nước Việt Nam từ Con Rồng, Cháu Tiên thời dựng nước, đến Bánh Chưng, Bánh Dày truyền thống hay sự tích Dưa Hấu .v.v...

Đặc biệt, từ năm 2015, đây là cuộc thi duy nhất do Việt Nam tổ chức thu hút được sự tham gia của nhiều đội trên phạm vi toàn cầu. Bên cạnh ý nghĩa về mặt chuyên môn, đây cũng là cơ hội để quảng bá một Việt Nam mến khách, giàu văn hóa đến bạn bè khắp năm châu.

1.2. Bộ trưởng Nội vụ Đức, ông Horst Seehofer cho rằng nước này cần phải có những hành động phản công trên không gian mạng. Hiện nay, Chính phủ Đức đang cân nhắc dự luật cho phép đáp trả một cách chủ động trước các cuộc tấn công mạng của nước ngoài vào các hệ thống thông tin của nước Đức.

Theo báo cáo của cơ quan chức năng Đức, các vụ tấn công mạng từ nước ngoài có chiều hướng gia tăng từ năm 2014 và tăng cao vào năm ngoái (2017), các cuộc tấn công mạng từ nước ngoài chủ yếu nhằm vào các tổ chức chính phủ, nhân quyền, các trung tâm nghiên cứu và ngành công nghiệp vũ trụ, quốc phòng, hóa dầu của Đức, vì vậy cơ quan này không chỉ cần phải có năng lực để theo dõi, giám sát, phát hiện, xử lý các cuộc tấn công mạng mà cần phải có sức mạnh để thực hiện các biện pháp phản ứng, chủ động đáp trả.

Báo cáo cũng cho biết, đã có nhưng chiến dịch trên không gian mạng nhằm tuyên truyền và làm sai lệch thông tin, tác động lên ý kiến xã hội của nước Đức với mục tiêu làm bất ổn và suy yếu chính quyền nước này.

1.3. Theo một thống kê gần đây, đã có ít nhất 170 quốc gia bị ảnh hưởng bởi mã độc Emotet trong đó có Việt Nam.

Emotet đã và đang là một trong những mã độc gây thiệt hại lớn nhất ảnh hưởng lên các tổ chức chính phủ và tài chính. Nó có khả năng lây nhiễm nhanh trên các hệ thống mạng, khiến cho việc phòng, chống mã độc này rất khó khăn.

Chức năng chính của Emotet là tải về và cài đặt các Trojan khác. Thêm vào đó, Emotet có thể biến đổi để vượt qua các chức năng phát hiện dựa trên dấu hiệu (signature-based) của các giải pháp phòng, chống mã độc. Emotet có một vài phương pháp để duy trì tồn tại trong hệ thống, bao gồm việc tự khởi động các dịch vụ và khóa registry. Emotet sử dụng các thư viện DLL để liên tục cải tiến và cập nhật các chức năng. Ngoài ra, Emotet có khả năng phát hiện máy ảo và có thể tạo ra các dấu hiệu giả khi thực thi trong môi trường ảo.

Emotet được phát tán qua thư rác sử dụng các phương pháp của kỹ thuật tấn công lừa đảo (phishing) để lừa người dùng mở tập tin đính kèm hoặc truy cập vào các đường dẫn độc hại.

Ngày 03/8/2018, qua hoạt động theo dõi và thu thập thông tin, Cục An toàn thông tin đã phát hiện ít nhất 171 địa chỉ IP của Việt Nam (tương ứng với 171 hệ thống thông tin đằng sau) có thể đã bị lây nhiễm mã độc này. Hiện tại theo đánh giá của một số tổ chức quốc tế về an toàn thông tin đây là mã độc đang gây ảnh hưởng trên diện rộng, với trên 5.000 tổ chức ở 170 quốc gia đã bị ảnh hưởng (hơn 70.000 địa chỉ IP public và hơn 4000 ASN được phát hiện có hoạt động liên quan đến mã độc này).

Nhằm bảo đảm an toàn không gian mạng Việt Nam, Cục An toàn thông tin khuyến nghị các cơ quan, tổ chức, đơn vị thực hiện:

- Giới hạn và kiểm soát kết nối SMB giữa các máy client (có thể sử dụng tường lửa trên từng máy);

- Sử dụng và thường xuyên cập nhật dấu hiệu cho các giải pháp phòng, chống mã độc;

- Cập nhật các bản vá cho hệ điều hành;

- Theo dõi và cập nhật các biện pháp lọc thư điện tử rác và chặn địa chỉ IP nghi ngờ trên tường lửa.

Danh sách một số IP/Domain/Mã hash độc hại liên quan đến hoạt động của Emotet

SHA256

009d0f05d3c9b922ce82afb58c469e6d3f77e83c13be22e17bd42747ef985399

29048a6ac31caecd0423b604e8fb1fc72e666c083591cbf69c5dbd99ce46195c

3b3f16739d7842cbc9d6f39abce32f3cdf53794d330a8f8ad2230f0978d496a8

5e19c03d8558a9d1cc02b767afce7e55522aeb889fc91dccf9c3a8b270c2b45d

808a2fd9434cbc1b45d299440e1c82f0b2748eb3dbb67a5963afe9eb504c088f

ba1c140fd0ab10e978ea7e0c1d49a49b54271586c5434c8f2e95d07b1f72af13

Domain/URL

abovecreative.com

barocatch.com

bemnyc.com

http://shunji.org/logsite/INFO/AUK3980227455NVW/8441288/UNO-PRQRU

http://johnnipe.com/PAY/EFO64780OZCVYE/1869341089/LDY-YKBY

http://e3dai.com/NG/

http://belief-systems.com/QP2iE/

http://abakus-biuro.net//Y9pUQqBB/

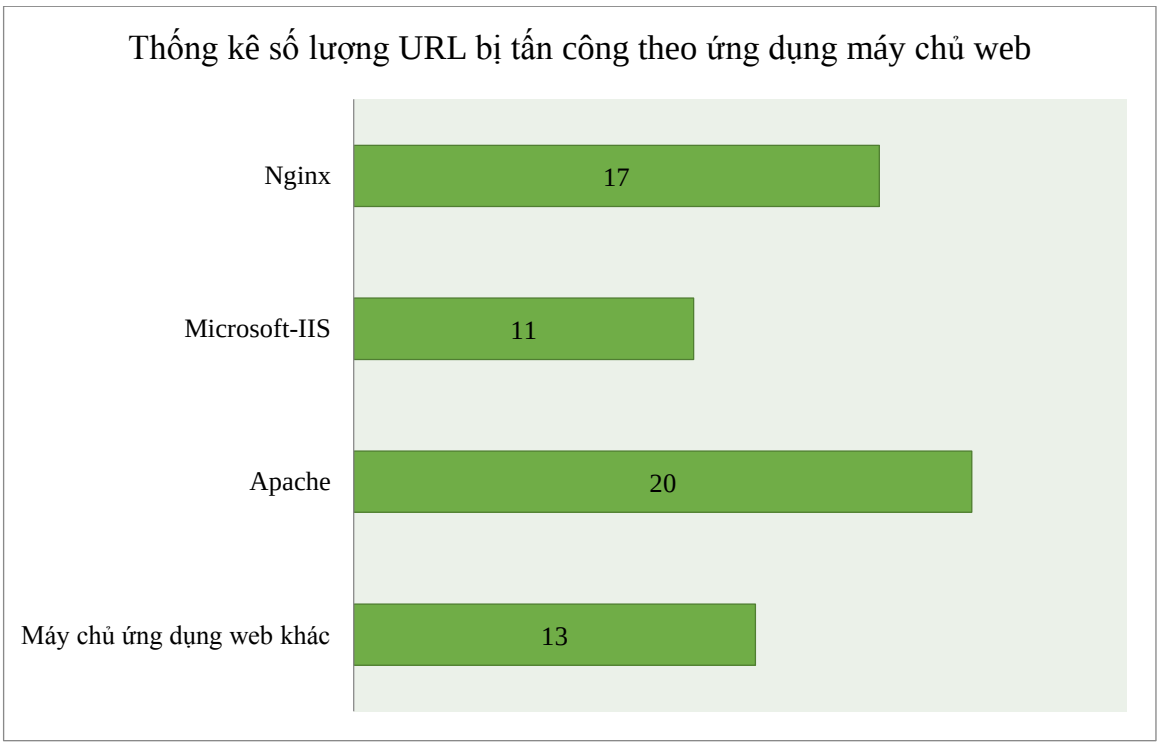
http://3music.net/iHIs/

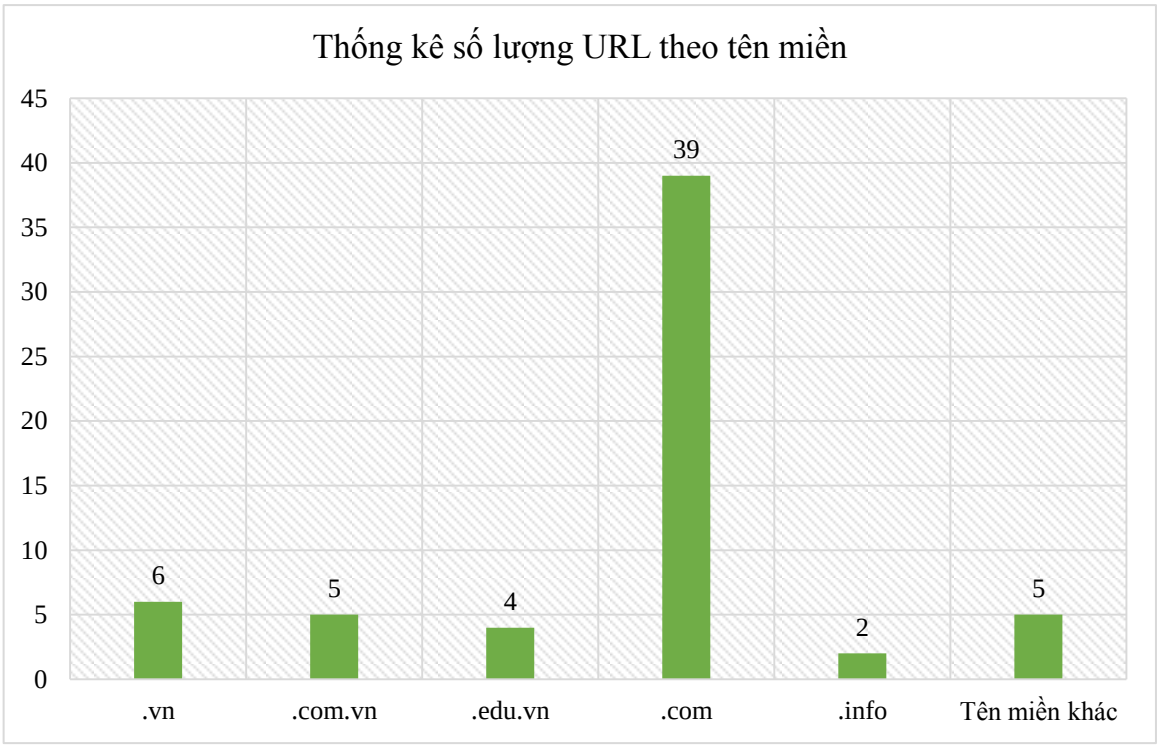
http://jobarba.com/wp-content/y3FG/

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…).

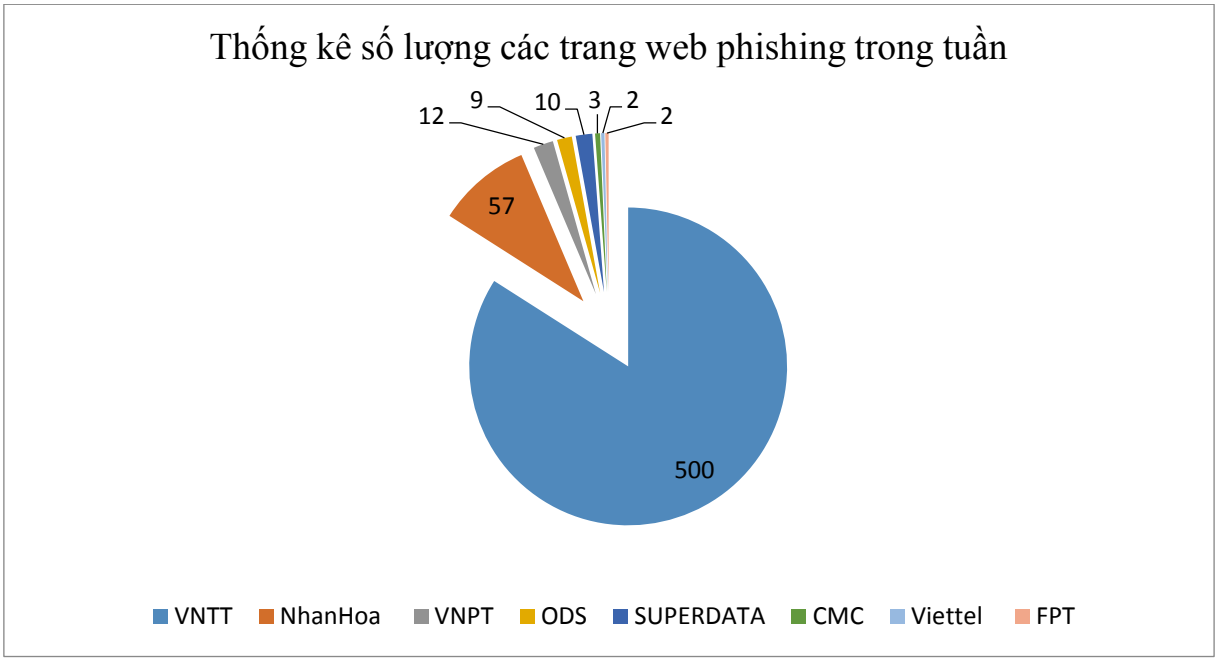
Trong tuần, Cục ATTT ghi nhận có ít nhất **61** đường dẫn (URL) trên các trang web tại Việt Nam bị tấn công, lợi dụng để thực hiện các hành vi gây mất an toàn thông tin. Trong đó, thống kê, phân loại các đường dẫn này theo loại ứng dụng máy chủ web (IIS, Apache …) và nhà cung cấp cụ thể như sau:



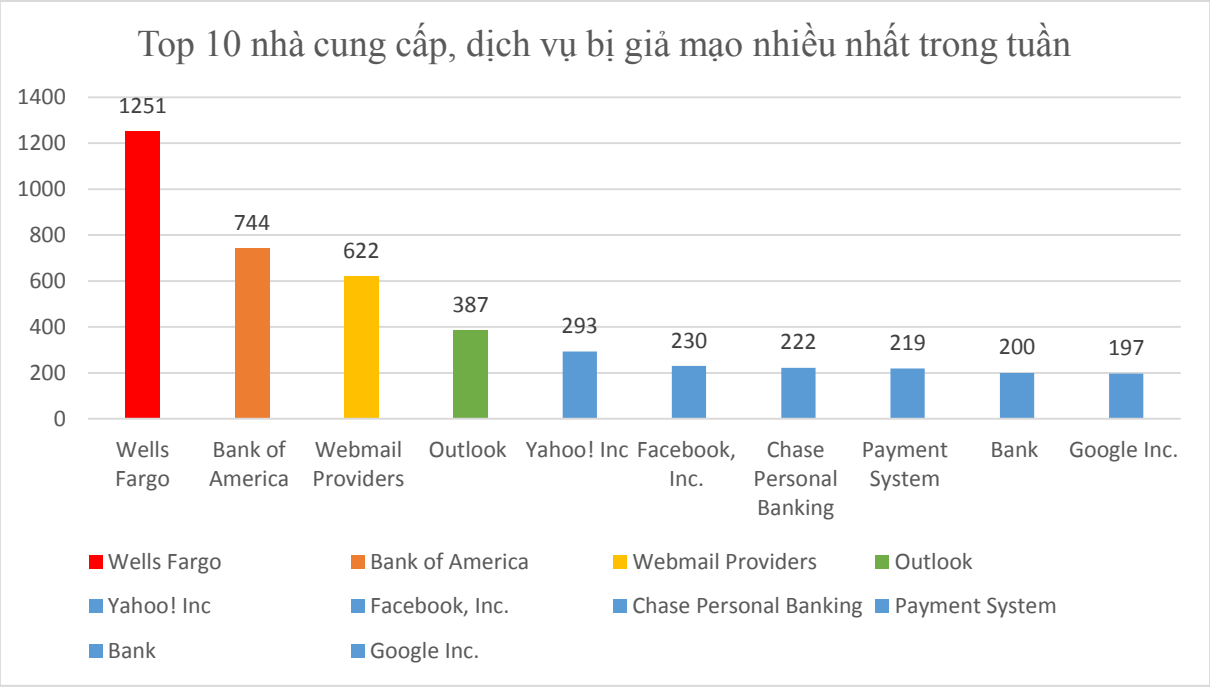


3. Tình hình tấn công lừa đảo (Phishing) trong tuần

3.1. Qua thu thập, theo dõi, trích xuất từ hệ thống kỹ thuật, Cục ATTT còn ghi nhận có ít nhất **606** 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, tài chính .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, outlook, yahoo .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 ít nhất 342 lỗ hổng, trong đó có ít nhất 13 lỗ hổng RCE (cho phép chèn và thực thi mã lệnh) và 8 lỗ hổng đã có mã khai thác.

4.2. Hệ thống kỹ thuật của Cục An toàn thông tin chủ động rà quét trên không gian mạng Việt Nam, đánh giá, thống kê cho thấy có **06** 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 85 lỗ hổng trên phần mềm đọc tài liệu được sử dụng phổ biến tại Việt Nam Foxit PDF reader; Nhóm 9 lỗ hổng trên các sản phẩm của Intel..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	Cisco	CVE-2018-0397 CVE-2018-0413 CVE-2018-0391 CVE-2018-0408 CVE-2018-0407 …	Nhóm 07 lỗ hổng trên các sản phẩm/dịch vụ của Cisco (Endpoints Mac Connector, Identity Service Engine, Prime Collaboration Provisioning, Small Business Managed Switches, Unified Communications Manager, Web Security Appliance) cho phép đối tượng tấn công thực hiện nhiều hình thức tấn công như: tấn công từ chối dịch vụ, CSRF, XSS, chèn và thực thi mã lệnh.	Đã có thông tin xác nhận
2	Foxit	CVE-2018-14268 CVE-2018-14270 CVE-2018-14271 CVE-2018-14272 CVE-2018-14256 …	Nhóm 85 lỗ hổng trên phần mềm đọc tài liệu phổ biến tại Việt Nam, Foxit PDF reader phiên bản 9.0.1.1049 cho phép đối tượng tấn công chèn và thực thi mã lệnh từ đó có thể cài cắm mã độc và thực hiện nhiều hình thức , cuộc tấn công nguy hiểm hơn	Đã có thông tin xác nhận và bản vá

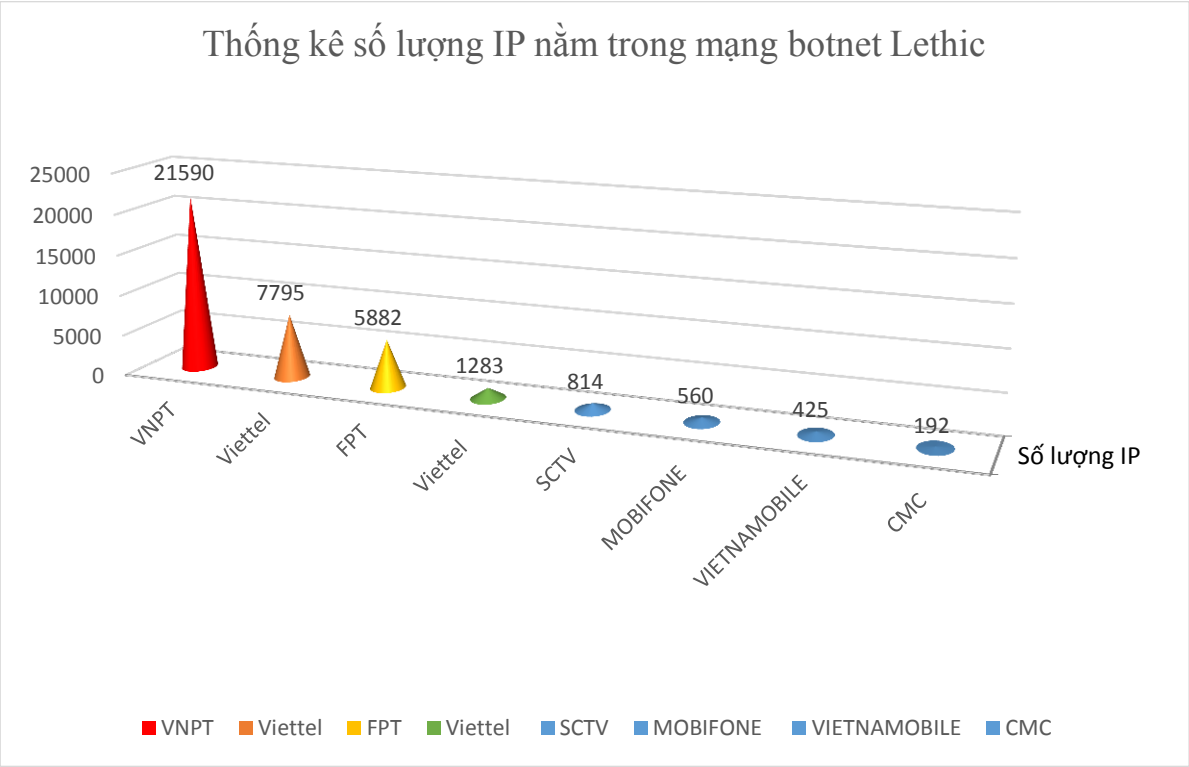
3	Huawei	CVE-2018-7792 CVE-2018-7794 CVE-2018-17174 CVE-2018-7947 CVE-2018-7957 …	Nhóm 07 lỗ hổng trên nhiều sản phẩm của Huawei (Mate 10, Mate 9 Pro, Emily-AL00A 8.1.0.153, Victoria-AL00 8.0.0.336a, BLA-L29 8.0.0.145,…) cho phép đối tượng tấn công thực hiện chèn và thực thi mã lệnh, tấn công từ chối dịch vụ và đánh cắp thông tin.	Đã có thông tin xác nhận và bản vá
4	Intel	CVE-2018-3605 CVE-2017-5692 CVE-2017-5693 CVE-2018-3671 CVE-2018-3663 …	Nhóm 09 lỗ hổng trên các sản phẩm của Intel (INTEL Distribution for Python, Graphics Driver for Windows, Saffron, Smart Sound Technology) cho phép đối tượng tấn công thực hiện tấn công từ chối dịch vụ, chèn và thực thi mã lệnh.	Chưa có thông tin xác nhận và bản vá
5	Paypal	CVE-2017-6213 CVE-2017-6215	Nhóm 02 lỗ hổng trên dịch vụ của Paypal (paypal/invoice-sdk-php, permissions-sdk-php) cho phép đối tượng tấn công thực hiện tấn công XSS và thực thi mã lệnh	Đã có thông tin xác nhận
6	Samsung	CVE-2018-10904 CVE-2018-10908	Nhóm 02 lỗ hổng trên Synthru Web Service của Samsung cho phép đối tượng thực hiện tấn công XSS và CSRF.	Chưa 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 Lethic

Mạng botnet Lethic được phát hiện lần đầu vào khoảng năm 2008, ban đầu gồm 210 000 - 310 000 máy cá nhân chủ yếu để gửi thư rác về các mảng dược phẩm. Thời kỳ phát triển mạnh, mạng botnet này chịu trách nhiệm cho 8-10% của tất cả các thư rác được gửi trên toàn thế giới. Tính đến tháng 4 năm 2010, botnet có khoảng 1,5% thị phần thư rác và gửi khoảng 2 tỷ thư rác mỗi ngày.

Theo thống kê về mạng botnet Lethic của Cục An toàn thông tin trong tuần có nhiều IP tại Việt Nam vẫn nằm trong mạng botnet này.



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

TT	Tên miền/IP
1	ew87fhzx.ru
2	1ffsxvw5df.ru
3	kukutrustnet777.info
4	88r771r2.ru
5	kh56fuav.ru
6	104.244.14.252
7	kukutrustnet888.info
8	g.omlao.com
9	0-0-0-0-0-0-0-0-0-0-0-0-0-0-5-0-0-0-0-0-0-0-0-0-0-0-0-0.info
10	0-0-0-0-0-0-0-0-0-0-0-0-0-0-10-0-0-0-0-0-0-0-0-0-0-0-0-0.info

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 An toàn thông tin 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 An toàn 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 An toàn thông tin 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 An toàn thông tin đã chia sẻ, đặc biệt là các tên miền đã nêu trong *mục 5.2* 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, TTTV.

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.govvn | 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