BỘ THÔNG TIN VÀ TRUYỀN THÔNG
CỤC AN TOÀN THÔNG TIN

Số: **37**/BC-CATTT

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

Hà Nội, ngày 21 tháng 08 năm 2018

TÓM TẮT
Tình hình an toàn thông tin đáng chú ý trong tuần 33/2018
(từ ngày 13/8/2018 đến ngày 19/8/2018)

BẢNG TỔNG HỢP

1. Nhà chức trách Hồng Kông khởi động chiến dịch tuyên truyền, nâng cao nhận thức về an toàn thông tin cho người dùng điện thoại thông minh. Đây là lần thứ 2 của chiến dịch tuyên truyền về tầm quan trọng của bảo đảm an toàn thông tin mà Hồng Kông thực hiện. Mục tiêu của chiến dịch lần này là tăng cường nhận thức về bảo vệ dữ liệu cho điện thoại thông minh và các thiết bị di động khác.

2. Từ 09h00 thứ Bảy ngày 18/08/2018 đến 09h00 Chủ nhật ngày 19/08/2018, đã diễn ra vòng loại cuộc thi an toàn thông tin mạng toàn cầu WhiteHat Grand Prix 2018 với chủ đề Truyền thuyết Việt Nam (Legends of Vietnam) theo hình thức Online CTF - Jeopardy.

3. Đầu tháng 8 năm 2018 Cục An toàn thông tin nhận được một báo cáo về tấn công APT vào các quốc gia Đông Nam Á, trong đó có nhiều mẫu mã độc sử dụng các tài liệu bằng Tiếng Việt để cài đặt mã độc vào máy tính người dùng. Những mã độc này có tên ENFAL và ENDCMS (Hussarini, Sarhust), mã khai thác được đính kèm vào tập tin tài liệu tiếng Anh và Tiếng Việt để khai thác lỗ hổng CVE-2017-11882 và CVE-2012-0158.

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. Nhà chức trách Hồng Kông khởi động chiến dịch tuyên truyền, nâng cao nhận thức về an toàn thông tin cho người dùng điện thoại thông minh. Đây

là lần thứ 2 của chiến dịch tuyên truyền về tầm quan trọng của bảo đảm an toàn thông tin mà Hồng Kông thực hiện. Mục tiêu của chiến dịch lần này là tăng cường nhận thức về bảo vệ dữ liệu cho điện thoại thông minh và các thiết bị di động khác.

Với tên gọi "Chiến dịch An toàn Thông tin 2.0", hoạt động này được thực hiện sau sự thành công của một chương trình tương tự hướng tới người dùng máy tính cá nhân diễn ra vào năm ngoái.

Chiến dịch lần này có mục đích nhắc nhở cộng đồng rằng không chỉ máy tính để bàn mà cả điện thoại thông minh, máy tính bảng và các thiết bị di động khác có thể bị lây nhiễm mã độc và bị tấn công bởi các đối tượng có ý đồ xấu, và có thể dẫn tới hậu quả thiệt hại về tài chính lớn cho các nạn nhân.

Để nâng cao nhận thức và khuyến khích người dân sử dụng các biện pháp bảo vệ cho các thiết bị thông minh, cảnh sát đang phối hợp với nhiều doanh nghiệp cung cấp sản phẩm, dịch vụ phòng, chống phần mềm độc hại để cho phép tải miễn phí các ứng dụng của họ trên trang mạng của chiến dịch. Các ứng dụng đã có 230.000 lần tải về, giúp loại bỏ 236.000 phần mềm độc hại, gần gấp 02 lần so với chiến dịch năm ngoái.

Trang mạng của chiến dịch cũng cung cấp thông tin về việc bảo vệ an toàn thông tin thiết bị thông minh. Các khuyến nghị để bảo vệ điện thoại thông minh một cách hiệu quả bao gồm:

- Không mở các đường dẫn thông tin lạ, nghi ngờ;

- Không cài đặt các ứng dụng không rõ nguồn gốc;

- Không jailbreak/wipe các thiết bị thông minh;

- Không mở các email lạ, đáng ngờ;

- Không truy cập các trang mạng không tin cậy;

- Nên sử dụng ít nhất một phân mềm phòng, chống mã độc;

- Hệ điều hành, ứng dụng và phần mềm phòng, chống mã độc nên được cập nhật thường xuyên;

- Khi có nghi ngờ thiết bị của mình bị nhiễm mã độc, hãy tham khảo ý kiến của các chuyên gia công nghệ thông tin;

- Chủ sở hữu của các thiết bị di động nên cảnh giác trước các dấu hiệu của việc lây nhiễm mã độc như tiêu tốn điện năng nhiều bất thường, hiệu năng giảm một cách rõ rệt và các phần mềm lạ xuất hiện trên máy mà mình không hề hay biết.

1.2. Từ 09h00 thứ Bảy ngày 18/08/2018 đến 09h00 Chủ nhật ngày 19/08/2018, đã diễn ra vòng loại cuộc thi an toàn thông tin mạng toàn cầu WhiteHat Grand Prix 2018 với chủ đề Truyền thuyết Việt Nam (Legends of Vietnam) theo hình thức Online CTF - Jeopardy với các chủ đề:

(1) Reverse engineering (Dịch ngược mã nguồn phần mềm, unpack…);

(2) Web Security (Các kỹ thuật tấn công vào ứng dụng web);

(3) Cryptography (Lý thuyết mật mã và ứng dụng, phá mã)

(4) Pwnable (Khai thác lỗ hổng phần mềm);

(5) Miscellaneous (Hỗn hợp).

Tham gia vòng loại có 720 đội, đến từ 79 quốc gia, trong đó có nhiều đội quốc tế có thứ hạng cao trên thế giới tham dự (5/10 đội đứng đầu trên bảng xếp hạng các đội tham gia ctftime.org).

Vòng Chung kết đối kháng trực tiếp, sẽ diễn ra vào trung tuần tháng 10/2018 tại Hà Nội. Đây là cuộc đua kéo dài liên tục trong 8 tiếng giữa 10 đội thi xuất sắc nhất từ vòng loại.

Place	Team	Score	Challenges	Country	Last submit
1	coconutCoffee	3080	✓✓✓×✓✓×✓✓✓✓×✓✓✓××✓✓✓		19/08/2018 04:19:26
2	dcua	2930	✓✓✓✓✓✓✓✓✓✓✓×✓×××××✓✓✓		19/08/2018 08:33:38
3	pwndevils	2620	✓✓✓×✓✓×✓✓✓✓✓×✓×✓××✓✓✓		19/08/2018 08:01:34
4	ACEBEAR	2460	×✓×✓✓✓×✓✓✓✓✓×✓✓×××✓✓✓		19/08/2018 08:32:24
5	LC1BC	2450	✓✓✓✓×✓×✓✓✓✓×✓×✓×××××		19/08/2018 07:58:00
6	Injocker10K	2180	✓✓×✓✓✓✓×✓✓✓×✓✓××××✓✓		19/08/2018 06:50:04
7	r3s0L	2170	✓✓×✓✓✓✓×✓✓✓×✓✓××××✓✓		19/08/2018 08:19:55
8	perfectblue	2160	✓✓✓✓✓✓××✓✓✓×✓✓××××✓✓		19/08/2018 08:59:27
9	0daysober	2130	✓✓×××✓✓✓✓✓✓×✓×××✓×✓✓		19/08/2018 05:40:50
10	CLGTftMeePwn	2030	✓✓×✓✓×✓×✓✓✓×✓✓××××✓✓		19/08/2018 08:36:45

1.3. Cảnh báo chiến dịch tấn công APT và các quốc gia Đông Nam Á trong đó có Việt Nam

Đầu tháng 8 năm 2018 Cục An toàn thông tin nhận được một báo cáo về tấn công APT vào các quốc gia Đông Nam Á, trong đó có nhiều mẫu mã độc sử dụng các tài liệu bằng Tiếng Việt để cài đặt mã độc vào máy tính người dùng.

Những mã độc này có tên ENFAL và ENDCMS (Hussarini, Sarhust), mã khai thác được đính kèm vào tập tin tài liệu tiếng Anh và Tiếng Việt để khai thác lỗ hổng CVE-2017-11882 và CVE-2012-0158, sau đó sẽ tiếp tục tải về máy tính các mã độc khác. Tập tin bằng Tiếng Anh gồm những nội dung liên quan đến chính trị và ngoại giao của Việt Nam, Philippines và Myanmar; những tập tin bằng Tiếng Việt lợi dụng nội dung rất phổ biến; quen thuộc và đa dạng (như góp ý dự thảo văn bản từ Văn phòng Chính phủ, phiếu đăng ký, báo cáo thu chi Đảng phí, đặc biệt có cả văn bản sử dụng thông tin về cảnh báo mã độc GrandCrab của Trung tâm VNCERT). Một số hình ảnh về văn bản bị lợi dụng để cài cắm mã độc có thể tham thiếu theo thông tin bên dưới.

Theo đánh giá chiến dịch tấn công này tương tự như chiến dịch tấn công APT15 (bao gồm cả việc sử dụng những mẫu mã độc và các quốc gia mục tiêu hướng đến)

Qua kiểm tra sơ bộ của Cục An toàn thông tin, những mẫu mã độc này hầu hết đã được đưa lên các kho lưu trữ và phân tích mã độc (như Virustotal) và nhiều giải pháp anti-virus đã nhận dạng và lại khai thác những lỗ hổng cũ, đã có bản vá do vậy người dùng, các cơ quan tổ chức nếu đã cập nhật bản vá thường xuyên cho hệ điều hành, ứng dụng Microsoft Office và có sử dụng giải pháp phòng chống mã độc được cập nhật thường xuyên thì có thể không đáng lo ngại.

Đối với những trường hợp chưa thực hiện kịp thời việc cập nhật bản vá cho lỗ hổng bảo mật và giải pháp phòng chống mã độc cần kiểm tra, rà soát dựa trên những thông tin kỹ thuật bên dưới để tránh nguy cơ mất an toàn thông tin, và thiệt hại có thể xảy ra đối với cơ quan, tổ chức và không gian mạng Việt Nam.

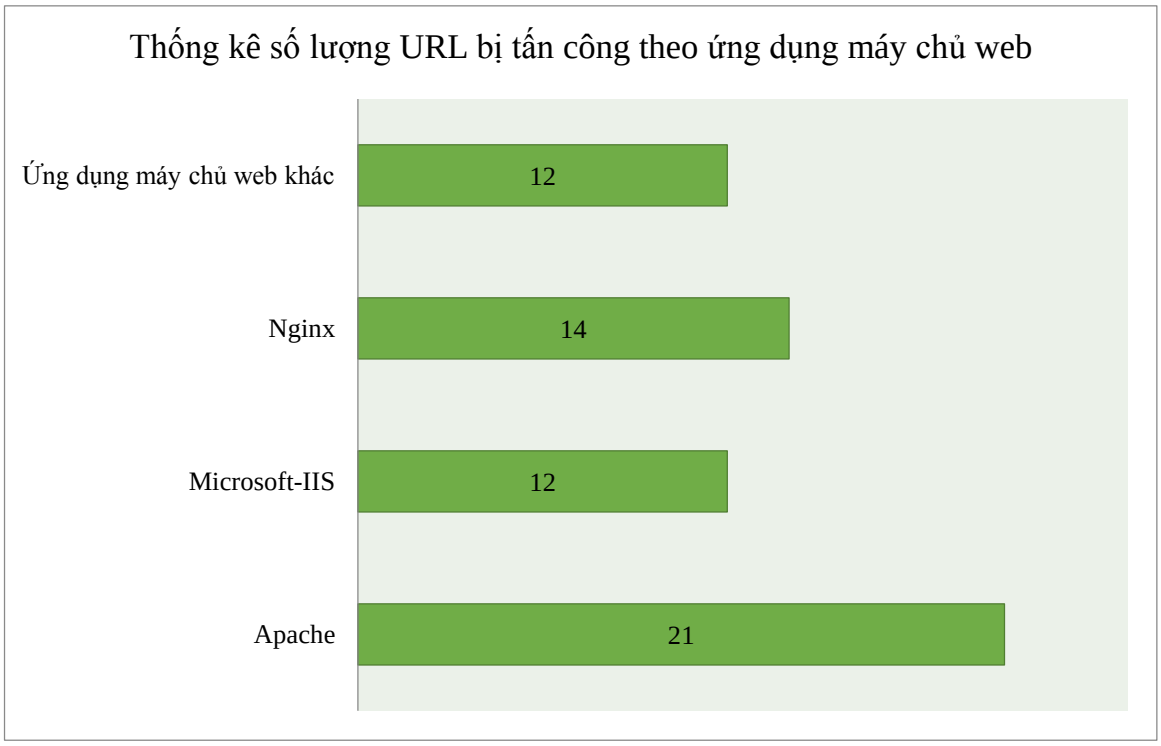
Thông tin về hình ảnh một số văn bản bị lợi dụng để khai thác điểm yếu và hạ tầng kỹ thuật của cuộc tấn công này có thể tham khảo tại đường dẫn sau:

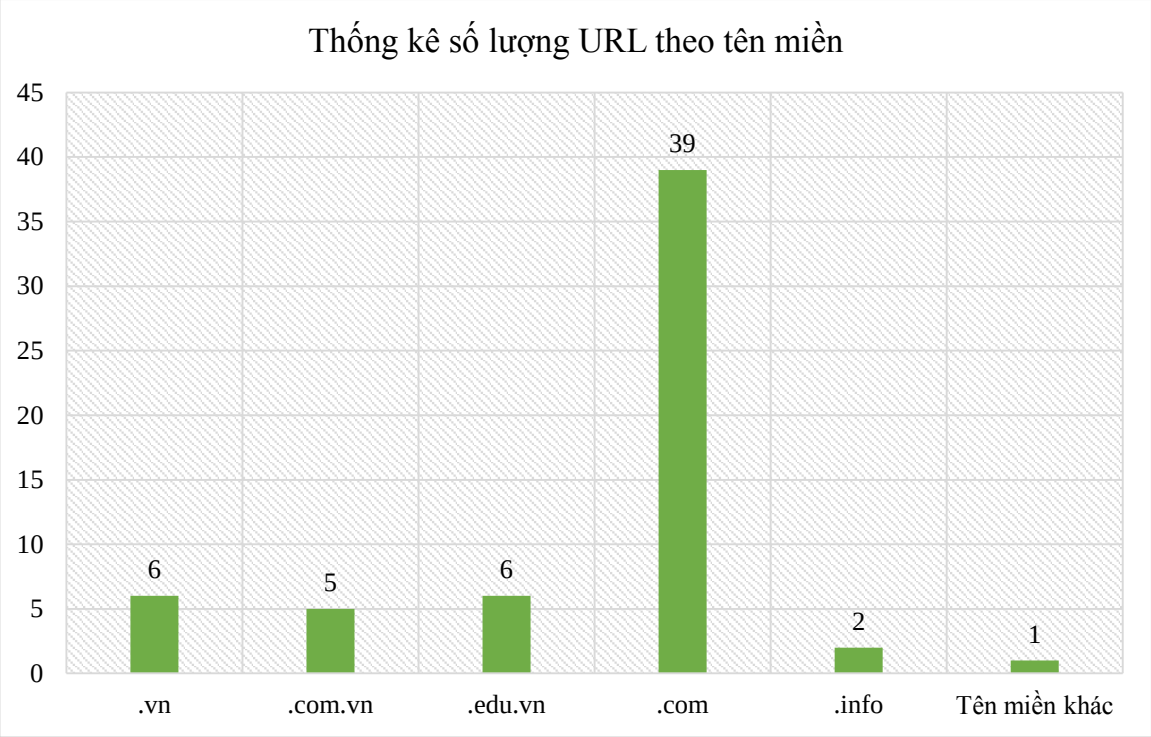
https://ti.khonggianmang.vn/dashboard/news/p/canh-bao-chien-dich-tan-cong-apt--vao-quoc-gia-dna/

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…).

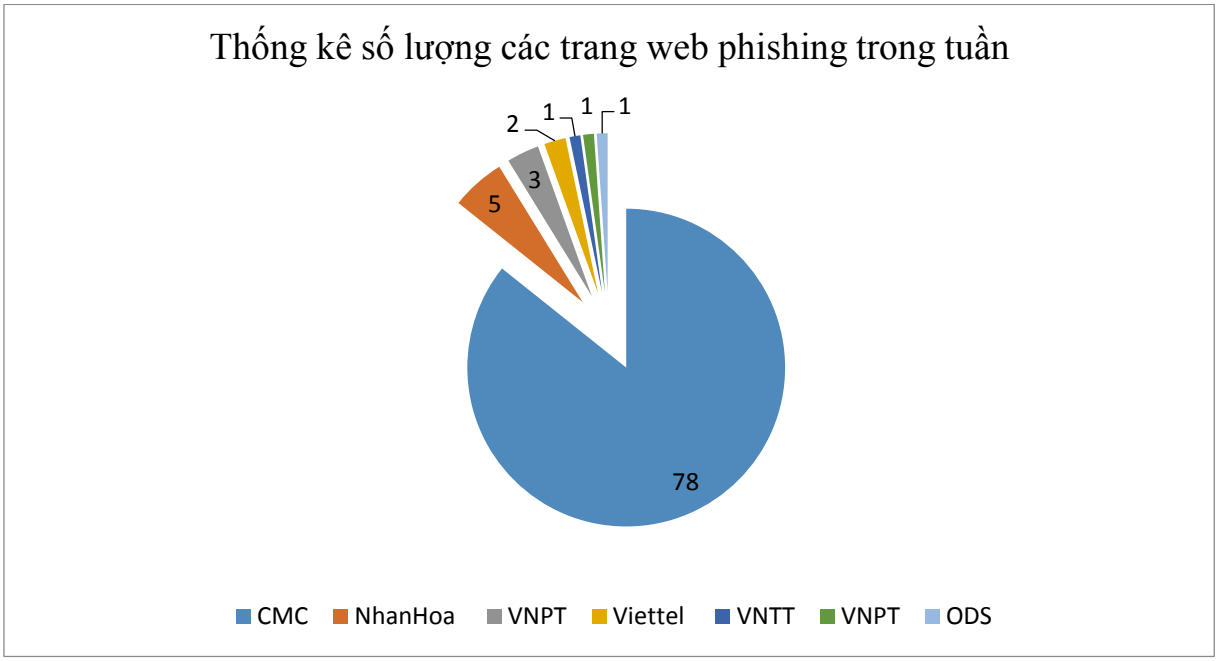
Trong tuần, Cục ATTT ghi nhận có ít nhất **59** đường dẫn (URL) trên các trang web tại Việt Nam bị tấn công, lợi dụng để thực hiện các hành vi gây mất an toàn thông tin. Trong đó, thống kê, phân loại các đường dẫn này theo loại ứng dụng máy chủ web (IIS, Apache …) và nhà cung cấp cụ thể như sau:



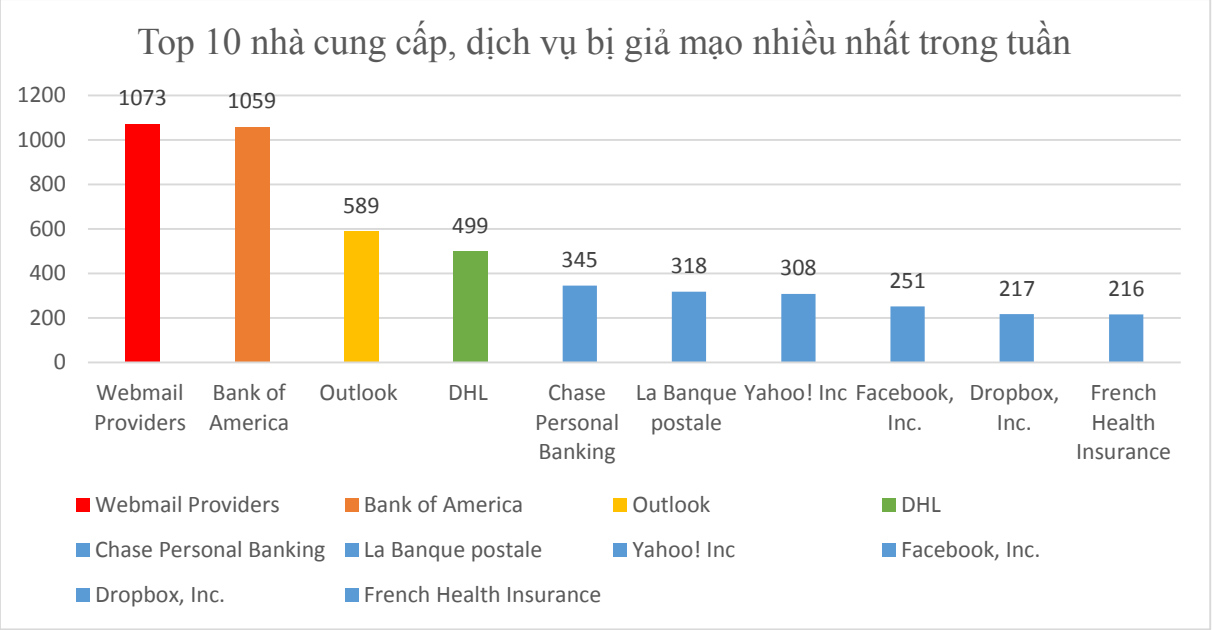


3. Tình hình tấn công lừa đảo (Phishing) trong tuần

3.1. Qua thu thập, theo dõi, trích xuất từ hệ thống kỹ thuật, Cục ATTT còn ghi nhận có ít nhất **93** 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, Dropbox, 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 ít nhất 241 lỗ hổng, trong đó có ít nhất 42 lỗ hổng RCE (cho phép chèn và thực thi mã lệnh) và 14 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 **05** 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: 3 lỗ hổng trên chip vi xử lý Core i3 của Intel cho phép đối tượng đánh cắp thông tin hệ thống; Nhóm 5 lỗ hổng trên một số sản phẩm của HP (các dòng máy in HP Inkjet, HPE iLO, OfficeConnect 1810 Switch Series, HPE XP P9000 CVAE) .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	Intel	CVE-2018-3615 CVE-2018-3620 CVE-2018-3646	Nhóm 3 lỗ hổng trên chip vi xử lý Core i3 của Intel cho phép đối tượng tấn công đánh cắp thông tin hệ thống	Đã có thông tin xác nhận

2	Cisco	CVE-2018-0418 CVE-2018-0410 CVE-2018-0409 CVE-2018-0367 CVE-2018-0415 …	Nhóm 11 lỗ hổng trên các sản phẩm phầm mềm của Cisco (Cisco ASR 9000 Series Aggregation Services Router Software, AsyncOS Software for Cisco Web Security Appliance) cho phép đối tượng tấn công thực hiện tấn công từ chối dịch vụ, tấn công XSS, đánh cắp thông tin, nhiều lỗ hổng cho phép chèn và thực thi mã lệnh.	Đã có thông tin xác nhận
3	Microsoft	CVE-2018-8360 CVE-2018-8390 CVE-2018-8355 CVE-2018-8379 CVE-2018-8382 …	Nhóm 60 lỗ hổng trên một số sản phẩm của Microsoft (.NET, Edge, Chakracore, Excel, Internet Explorer, DirextX Graphic Kernel, Windows…) cho phép thực hiện nhiều hình thức tấn công như đánh cắp thông tin, leo theo đặc quyền, chèn và thực thi mã lệnh.	Đã có thông tin xác nhận
4	HP	CVE-2018-5925 CVE-2018-5924 CVE-2018-7093 CVE-2018-7100 CVE-2018-7077	Nhóm 5 lỗ hổng trên một số sản phẩm của HP (các dòng máy in HP Inkjet, HPE iLO, OfficeConnect 1810 Switch Series, HPE XP P9000 CVAE) cho phép đối tượng thực hiện các hình thức tấn công từ chối dịch vụ, chèn và thực thi mã lệnh, đánh cắp thông tin.	Đã có thông tin xác nhận và bản vá
5	Netcomm Wireless	CVE-2018-14782 CVE-2018-14783 CVE-2018-14784 CVE-2018-14785	Nhóm 4 lỗ hổng trên dòng router Wireless G LTE Light Industrial M2M Router (NWL-25) với firmware phiên bản 2.0.29.11 trở về trước cho phép đối tượng tấn công truy cập vào tập tin hệ thống không cần xác thực, tấn công XSRF, chèn và thực thi mã lệnh.	Chưa có thông tin xác nhận

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

5.1. Mạng botnet Andromeda

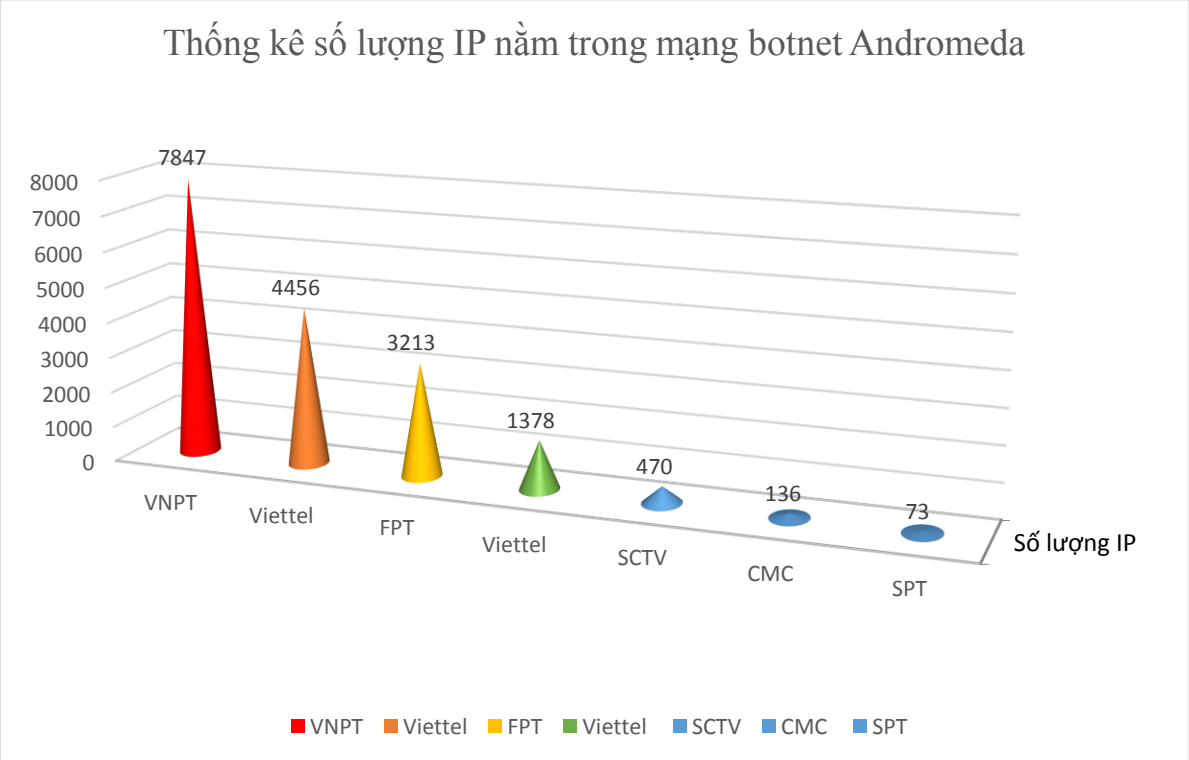
Botnet Andromeda, còn được gọi là Win32/Gamarue đã bắt đầu xuất hiện và lây nhiễm vào các máy tính từ năm 2011. Đối tượng chính của cuộc tấn công mã độc này là các doanh nghiệp sử dụng thẻ thanh toán.

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: Keyloogging; 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.

Tại Việt Nam, số lượng máy tính nằm trong mạng botnet Andromeda vẫn còn rất nhiều trong tuần mà Cục An toàn thông tin đang theo dõi.



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

TT	Tên miền/IP
1	fr4vkbdr.ru
2	1r69so6w16l.ru
3	kukutrustnet777.info
4	gd14hp0u6x.ru
5	104.244.14.252
6	qsqjeuno53.ru
7	kukutrustnet888.info
8	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
9	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
10	kukutrustnet987.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