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: **29**/BC-CATTT

Hà Nội, ngày 03 tháng 7 năm 2018

TÓM TẮT
Tình hình an toàn thông tin đáng chú ý trong tuần 26/2018
(từ ngày 25/6/2018 đến ngày 01/7/2018)

BẢNG TỔNG HỢP

1. Ngày 27/6/2018, Bộ TT&TT tổ chức chương trình diễn tập "Nâng cao năng lực xử lý tình huống tấn công mạng vào hệ thống công nghiệp và tài chính quan trọng".

2. Cơ quan chức năng của Chính phủ Ấn Độ yêu cầu các ngân hàng phải hoàn thành việc ngừng sử dụng hệ điều hành Windows XP trong các máy ATM trước tháng 6/2019.

3. Sau 6 năm tồn tại trên không gian mạng, botnet Necurs đã được liên tục nâng cấp thêm các tính năng mới trong vòng vài tháng trở lại đây. Nhóm các nhà nghiên cứu của Trend Micro đã phát hiện những thay đổi đáng lo ngại trong hoạt động của botnet này, nhiều khả năng Necurs đang được chuẩn bị để thực hiện những chiến dịch tấn công gây thiệt hại trên diện rộng.

1. Điểm tin đáng chú ý

1.1. Ngày 27/6/2018, Bộ TT&TT tổ chức chương trình diễn tập "Nâng cao năng lực xử lý tình huống tấn công mạng vào hệ thống công nghiệp và tài chính quan trọng".

Tham gia chương trình diễn tập lần này là các cán bộ lãnh đạo, cán bộ quản lý, cán bộ kỹ thuật của 17 cơ quan nhà nước, Tập đoàn kinh tế, Tổng công ty nhà nước, các tổ chức tài chính, ngân hàng TMCP và một số cơ quan có liên quan trong lĩnh vực điều khiển công nghiệp (SCADA/ICS và tài chính - ngân hàng.

17 đơn vị tham gia theo 2 lĩnh vực, trong đó 8 đơn vị diễn tập bảo đảm ATTT cho các hệ thống điều khiển công nghiệp và 9 đơn vị diễn tập về bảo đảm

ATTT cho các hệ thống tài chính, ngân hàng. Trực tiếp hướng dẫn các đội diễn tập là 2 chuyên gia quốc tế đến từ Nga và Mỹ với sự phối hợp của chuyên gia Cục ATTT, VNPT, Bkav, CMC…

Nội dung diễn tập "Nâng cao năng lực xử lý tình huống tấn công mạng vào hệ thống công nghiệp và tài chính quan trọng" tập trung vào các tình huống xử lý chỉ đạo, làm việc theo nhóm giúp các lãnh đạo, cán bộ quản lý, kỹ thuật viên chuyên trách về an toàn thông tin, CNTT của các cơ quan quản lý SCADA/ICS và hệ thống tài chính - ngân hàng quan trọng có thể thực hiện các biện pháp phòng chống, xử lý các tình huống tấn công mạng trong các kịch bản mô phỏng khi hệ thống vẫn được vận hành bình thường. Qua đó, giúp cán bộ có thêm nhận thức về các nguy cơ an toàn thông tin mới đối với hệ thống do mình quản lý và kinh nghiệm thực tế, nhanh nhạy, tự tin hơn khi xử lý các vấn đề an toàn thông tin chưa biết trước khi vận hành hệ thống thông tin quan trọng của tổ chức mình.

1.2. Cơ quan chức năng của Chính phủ Ấn Độ yêu cầu các ngân hàng phải hoàn thành việc ngừng sử dụng hệ điều hành Windows XP trong các máy ATM trước tháng 6/2019, trong bối cảnh các lỗ hổng bảo mật đang tăng lên do máy ATM của các ngân hàng sử dụng các phiên bản hệ điều hành không được hỗ trợ và không áp dụng các biện pháp bảo mật khác, điều này có khả năng gây ảnh hưởng tiêu cực đến lợi ích của khách hàng.

Mặc dù cơ quan này đã tư vấn, hướng dẫn các ngân hàng thực hiện các kế hoạch chuyển đổi nhưng tiến độ chuyển đổi diễn ra chậm và không hiệu quả. Ngân hàng và các nhà cung cấp dịch vụ ATM ủy quyền đã được yêu cầu thực hiện các biện pháp bảo mật theo thời hạn đưa ra như sau:

Biện pháp bảo mật	**Hạn cuối**
Bảo vệ ATM với mật khẩu BIOS, khóa chức năng autorun, cập nhật bản vá hệ điều hành và phần mềm, bảo vệ các thiết bị đầu cuối. truy cập quyền quản trị theo thời gian nhất định …	Tháng 8/2018
Áp dụng các biện pháp chống skimmer và lập danh sách whitelist các ứng dụng	Tháng 3/2018
Gỡ bỏ Windows XP	Tháng 6/2019

1.3. Sau 6 năm tồn tại trên không gian mạng, botnet Necurs đã được liên tục nâng cấp thêm các tính năng mới trong vòng vài tháng trở lại đây. Nhóm các

nhà nghiên cứu của Trend Micro đã phát hiện những thay đổi đáng lo ngại trong hoạt động của botnet này, nhiều khả năng Necurs đang được chuẩn bị để thực hiện những chiến dịch tấn công gây thiệt hại trên diện rộng. Ngoài các tính năng tương tự như bản gốc, mạng botnet này đã nâng cấp một số tính năng như đào tiền ảo, chiến thuật gửi thư rác..

Trong tháng 3, các chuyên gia bảo mật đã phát hiện Necurs đẩy một công cụ đào tiền mã hóa Monero - XMRig - vào các chương trình thực thi của mạng botnet này. Vào thời điểm phát hiện, khi kiểm tra nhật ký giao dịch của chủ sở hữu ví có thể kiếm được khoảng 1.200 đô la Mỹ trong vòng 24 giờ.

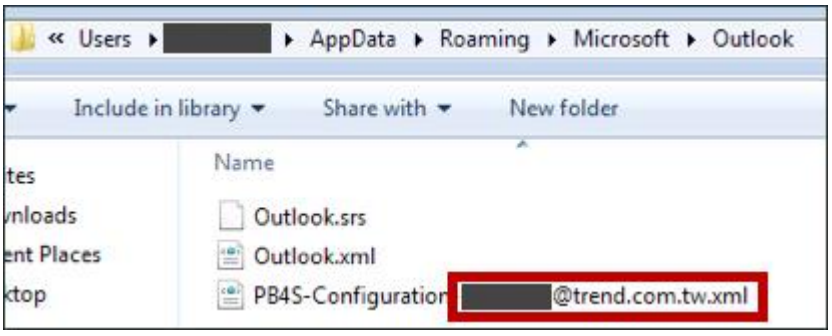
Màn hình hiển thị thông tin khai thác Monero bằng cách sử dụng XMRig

Trong tháng 4, mạng botnet này tiếp tục đẩy chương trình phần mềm FlawedAmmyy được phát triển từ một công cụ truy cập từ xa hợp pháp Ammyy Admin. Giống như công cụ máy tính để bàn từ xa, FlawedAmmyy có các chức năng của Quản trị viên Ammyy, bao gồm kiểm soát máy tính từ xa, quản lý hệ thống tệp, hỗ trợ proxy và khả năng trò chuyện, kiểm soát âm thanh…Một số thông tin mạng botnet này đánh cắp thu thập về: ID, OS, pcname, priv, domain, card..s

```
00000000  3d e3 55 4b f9 c1 71 05  5b e9 19 e9 ae d9 b3 85   =.UK..q. [.......
00000010  f0 74 3a 50 4c 73 38 5f  05 55 d6 a1 b6 16 a2 80   .t:PLs8_ .U......
00000020  e2 cb d2 4d                                       ...M
    00000000  2d 00                                          -.
00000024  38 8a 00 00 00 69 64 3d  35 33 34 35 32 37 39 36   8....id= 53452796
00000034  26 6f 73 3d 37 20 53 50  31 20 78 36 34 26 70 72   &os=7 SP 1 x64&pr
00000044  69 76 3d 55 73 65 72 2b  55 41 43 26 63 72 65 64   iv=User+ UAC&cred
00000054  3d 57 49 4e 2d 47 42 44  38 55 34 41 48 52 35 48   =WIN-GBD 8U4AHR5H
00000064  5c 76 69 72 75 73 26 70  63 6e 61 6d 65 3d 57 49   \virus&p cname=WI
00000074  4e 2d 47 42 44 38 55 34  41 48 52 35 48 26 61 76   N-GBD8U4 AHR5H&av
00000084  6e 61 6d 65 3d 26 62 75  69 6c 64 5f 74 69 6d 65   name=&bu ild_time
00000094  3d 33 31 2d 30 35 2d 32  30 31 38 20 31 35 3a 35   =31-05-2 018 15:5
000000A4  39 3a 35 36 20 50 4d 26  63 61 72 64 3d 30 26      9:56 PM& card=0&
000000B3  0b 00                                             ..
    00000002  0c                                             .
000000B5  0b 00                                             ..
    00000003  0c                                             .
000000B7  0b 00                                             ..
    00000004  0c                                             .
```

Các thông tin được FlawedAmmyy gửi về mạng botnet

Cuối tháng 5, Necurs thực hiện việc thu thập tài khoản email bằng cách tấn công các máy tính đã bị lây nhiễm có sử dụng Outlook. Khi một người dùng đăng nhập vào Outlook, phần mềm này sẽ tạo ra một thư mục có đường dẫn "%AppData%\Roaming\Microsoft\Outlook\" để lưu trữ một vài thông tin, trong đó có một file có địa chỉ e-mail của tài khoản viết trong tên. Necurs sẽ tìm kiếm những file như thế này rồi gửi về địa chỉ hxxp://185[.]176[.]221[.]24/l/s[.]php.



Thư mục lưu trữ dữ liệu của outlook có file với địa chỉ e-mail

Và vào tháng 6 vừa qua, mạng botnet Necurs lại tăng cường thêm một module spamming .NET. Module này có khả năng gửi e-mail và đánh cắp thông tin đăng nhập lưu trữ trong Internet Explorer, Chrome và Firefox. Điểm mới trong tính năng này là các e-mail spam có thể được gửi của qua các tài khoản e-mail đã được đăng nhập sẵn trên máy tính bị lây nhiễm khiến cho việc sử dụng danh sách đen để chống spam trở nên kém hiệu quả, cũng như module được lập trình để xóa ngay thư sau khi gửi để tránh việc bị người dùng phát hiện.

Để bảo vệ hệ thống thông tin chống lại mạng Necurs và các mối đe dọa liên tục phát tán khác, các cá nhân, tổ chức cần triển khai các giải pháp để có thể

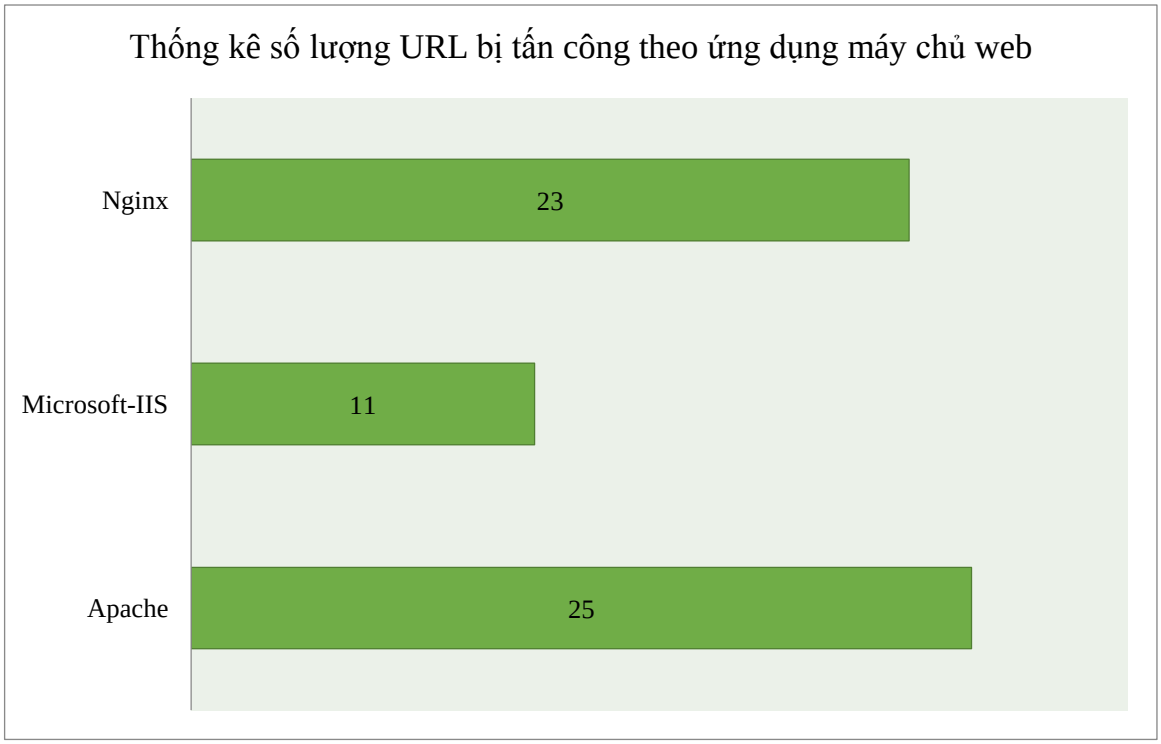
bảo vệ người dùng cuối (endpoint) khỏi các mối đe dọa bằng cách phát hiện các tệp độc hại và thư spam cũng như chặn tất cả các URL độc hại có liên quan.

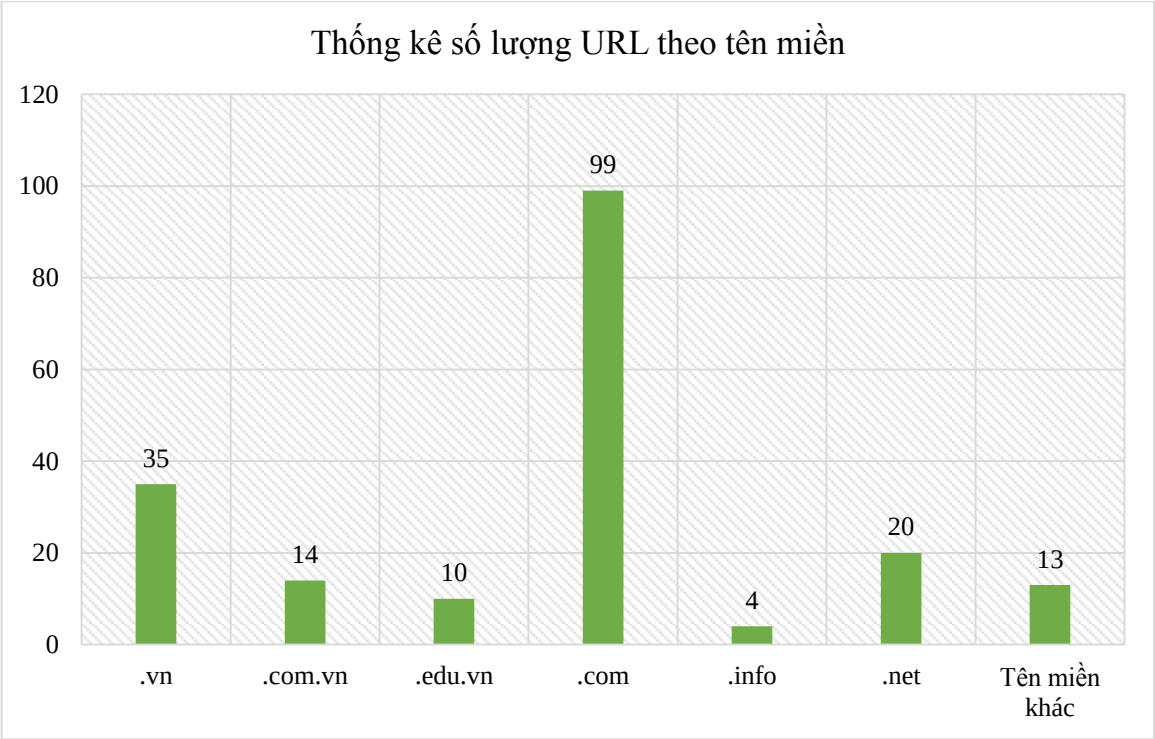
Mạng botnet Necurs cũng là một trong những mạng botnet được Cục An toàn thông tin theo dõi thường xuyên. Trong tuần có ít nhất 136 địa chỉ IP của Việt Nam (có thể coil à 136 hệ thống thong tin đang công khai trên Internet) đang nằm trong mạng botnet này.

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…).

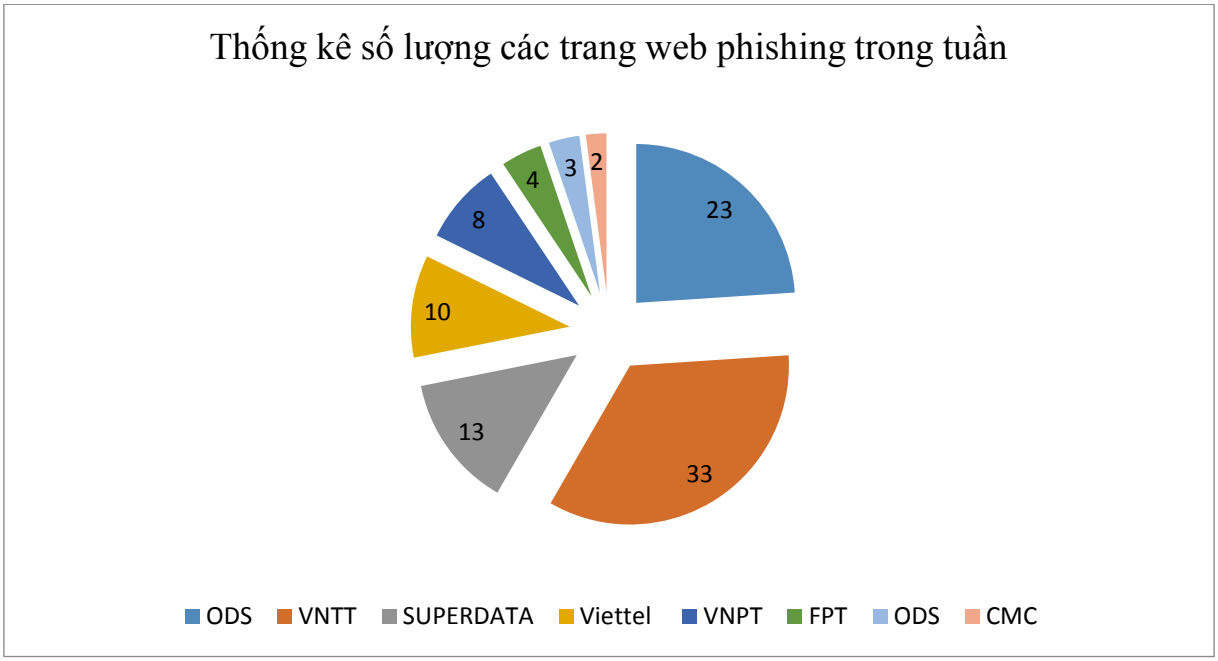
Trong tuần, Cục ATTT ghi nhận có ít nhất **195** đường dẫn (URL) trên các trang web tại Việt Nam bị tấn công, lợi dụng để thực hiện các hành vi gây mất an toàn thông tin. Trong đó, thống kê, phân loại các đường dẫn này theo loại ứng dụng máy chủ web (IIS, Apache …) và nhà cung cấp cụ thể như sau:



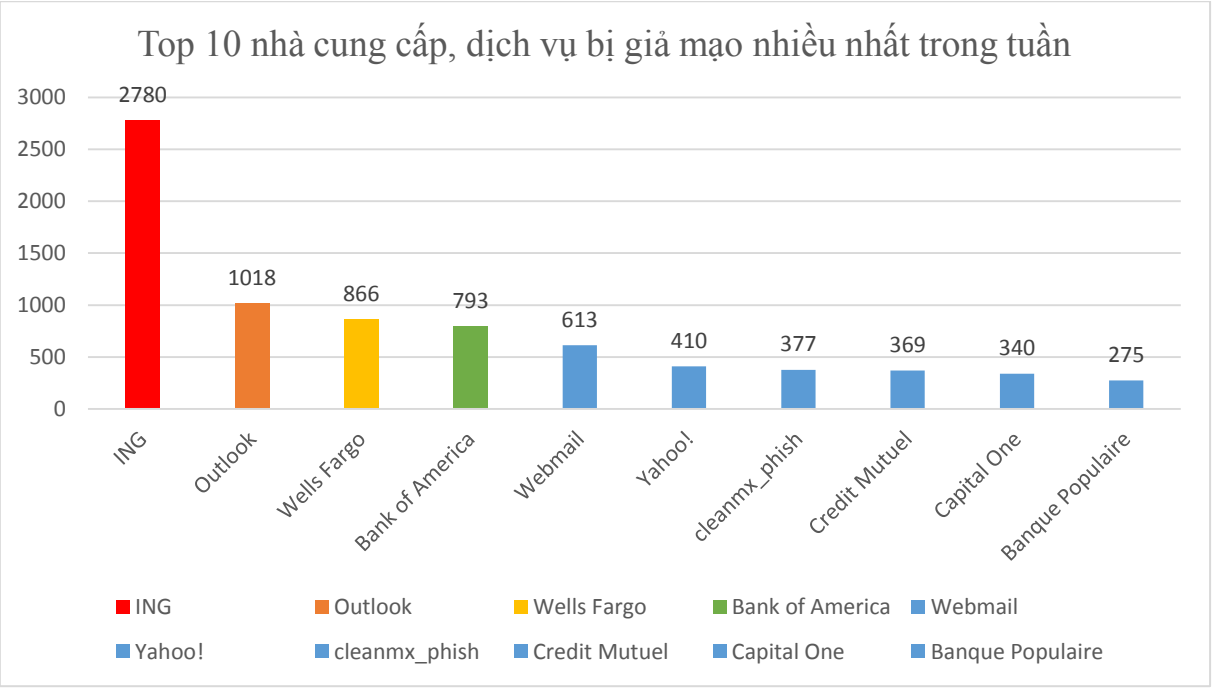


3. Tình hình tấn công lừa đảo (Phishing) trong tuần

3.1. Qua thu thập, theo dõi, trích xuất từ hệ thống kỹ thuật, Cục ATTT còn ghi nhận có ít nhất **363** 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, Outlook .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 302 lỗ hổng, trong đó có ít nhất 22 lỗ hổng RCE (cho phép chèn và thực thi mã lệnh) và 10 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 **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 15 lỗ hổng trên nền tảng và nhiều tiện ích của Wordpres; Nhóm 8 lỗ hổng trên nhiều sản phẩm của Siemens..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	Microsoft	CVE-2018-0599 CVE-2018-0593 CVE-2018-0592 CVE-2018-0600 CVE-2018-0595	Nhóm 09 lỗ hổng trên một số sản phẩm, dịch vụ của Microsoft (Visual C++ Redistributable, One Drive, Skype, Windows,…) cho	Chưa có thông tin xác nhận và bản vá

		…	phép đối tượng tấn công chiếm đặc quyền bằng cách sử dụng một Trojan DLL trên thư mục không xác định.	
2	Siemens	CVE-2018-4846 CVE-2018-4845 CVE-2018-11449 CVE-2018-11448 CVE-2018-4860 …	Nhóm 08 lỗ hổng trên nhiều sản phẩm của Siemens (RAPIDLab 1200 systems, RAPIDPoint 400 system, RAPIDPoint 500 systems, Scalance,…) cho phép đối tượng tấn công chèn và thực thi mã lênh, đánh cắp thông tin, chiếm quyền quản trị…	Đã có thông tin xác nhận
3	TP-link	CVE-2018-12692 CVE-2018-12693 CVE-2018-12694	Nhóm 03 lỗ hổng trên thiết bị mở rộng sóng wifi TL-WA850RE cho phép đối tượng tấn công thực hiện tấn công từ chối dịch vụ và thực thi mã lệnh. CVE-2018-12692 đã có mã khai thác Nhóm lỗ hổng này đã được đề cập trong Cảnh báo tuần trước, hiện vẫn chưa có bản vá	Chưa có thông tin xác nhận và bản vá.
4	Wordpress	CVE-2018-1000510 CVE-2018-1000512 CVE-2018-11506 CVE-2018-10505 CVE-2018-12636 …	Nhóm 15 lỗ hổng trên nền tảng và nhiều tiện ích của Wordpres cho phép đối tượng thực hiện tấn công XSS, CSRF, chỉnh sửa dữ liệu người dùng, chèn và thực thi mã lệnh, chiếm quyền quản trị. CVE-2018-12636 đã có mã khai thác.	Đã có thông tin xác nhận và bản vá

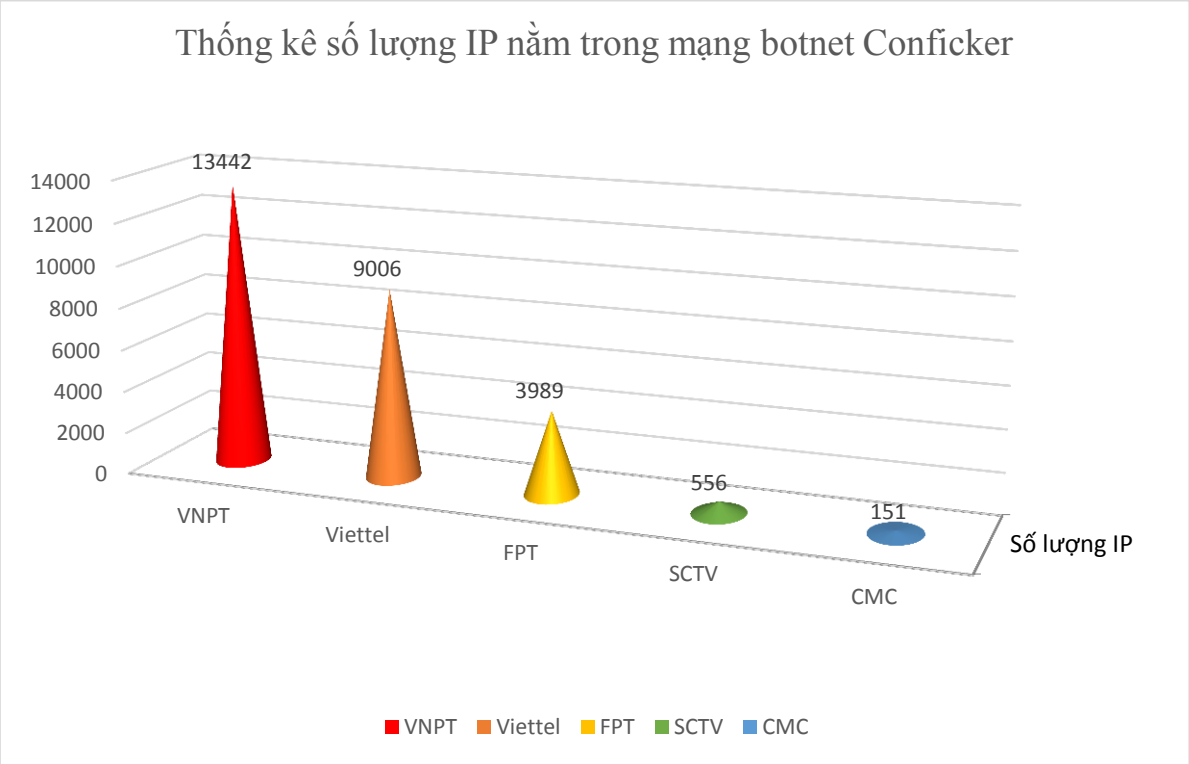
5. Hoạt động một số mạng botnet, APT, mã độc tại Việt Nam

5.1. Mạng botnet Conficker

Mạng botnet Conficker được phát hiện từ tháng 10/2008. Mã độc này được thiết kế nhằm vào hệ điều hành Microsoft Windows. Khi mã độc này lây nhiễm vào một máy tính, thì máy tính này tham gia vào mạng botnet và có thể bị điều khiển để gửi thư rác (spam) và tấn công các hệ thống khác. Những máy tính

bị lây nhiễm đều không truy cập được các website liên quan đến phần mềm diệt virus hay dịch vụ cập nhật của hệ Windows (Windows Update).

Mặc dù mạng botnet Conficker xuất hiện từ năm 2008, lợi dụng lỗ hổng cũ (MS 08-067), đã có bản vá bảo mật, tuy nhiên tại Việt Nam, số lượng máy tính nằm trong mạng botnet Conficker 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	w42f4ctqv4.ru
2	kukutrustnet777.info
3	104.244.14.252
4	g.omlao.com
5	v2k1j0t1.ru
6	mk.omkol.com
7	kukutrustnet888.info
8	init.icloud-analysis.com
9	u.amobisc.com
10	p.omlao.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 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

Cơ quan, tổ chức có thể liên hệ để được tư vấn, hỗ trợ trong công tác bảo đảm ATTT, cụ thể như sau:

- **Đăng ký nhận thông tin cảnh báo chung về ATTT, liên hệ**: Ông Hà Văn Hiệp, số điện thoại: 0968689111, thư điện tử: hvhiep@mic.gov.vn;

- **Đăng ký theo dõi, giám sát trang/cổng thông tin điện tử, liên hệ:** Ông Nguyễn Sơn Tùng, số điện thoại: 0977325416, thư điện tử: nstung@mic.gov.vn;

- **Đăng ký theo dõi, giám sát, xử lý mã độc, lừa đảo qua mạng, liên hệ:** Bà Bùi Thị Huyền, số điện thoại:0932481987; thư điện tử: bt_huyen@mic.gov.vn;

- **Đăng ký hỗ trợ cài đặt cảm biến (sensor) để giám sát, phòng, chống tấn công mạng, liên hệ**: Ông Nguyễn Phú Dũng, số điện thoại: 01676611700, thư điện tử: npdung@mic.gov.vn