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: **46**/BC-CATTT

*Hà Nội, ngày 16 tháng 10 năm 2018*

# TÓM TẮT
## Tình hình an toàn thông tin đáng chú ý trong tuần 41/2018
## (từ ngày 08/10/2018 đến ngày 14/10/2018)

**BẢNG TỔNG HỢP**

1 Một đạo Luật của bang California, Hoa Kỳ dự kiến có hiệu lực vào ngày 01/01/2020 sẽ bắt buộc nhà sản xuất thiết bị kết nối internet không được trang bị mật khẩu duy nhất trên tất cả các sản phẩm của mình, và trên các sản phẩm này phải có tính năng bắt buộc người dùng phải đặt lại mật khẩu khi sử dụng thiết bị lần đầu tiên.

2. Một báo cáo gần đây của Cơ quan thẩm định trách nhiệm của chính phủ Hoa Kỳ (Government Accountability Office - GAO) cho biết khả năng chống tấn công mạng của các hệ thống vũ khí quân đội Hoa Kỳ là kém.

3. Theo phân tích của PaloAlto một trong những hình thức được đối tượng tấn công sử dụng để phát tán mã độc đào tiền ảo, mã độc mã hóa tư liệu và mã độc ăn trộm thông tin gần đây là yêu cầu người dùng cập nhật phiên bản Flash. Theo đó khi người dùng chấp nhận cập nhật thì bản cập nhật Flash giả mạo này sẽ cài đặt mã độc có tên XMRig.

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. Các thiết bị kết nối Internet như các bộ định tuyến và các tiện ích thông minh dành cho gia đình thường là những mục tiêu hấp dẫn của đối tượng tấn công. Bởi vì hầu hết các thiết bị này không có cơ chế bảo mật hoặc chỉ có cơ chế bảo mật đơn giản (ví dụ như tất cả các thiết bị khi xuất xưởng đều có cùng một mật khẩu mặc định).

Các thiết bị định tuyến và thiết bị IoT không an toàn thường xuyên bị truy cập trái phép và kiểm soát bởi đối tượng tấn công và bị lợi dụng để thực hiện các cuộc tấn công từ chối dịch vụ lớn.

Một đạo Luật của bang California, Hoa Kỳ dự kiến có hiệu lực vào ngày 01/01/2020 sẽ bắt buộc nhà sản xuất thiết bị kết nối internet không được trang bị mật khẩu duy nhất trên tất cả các sản phẩm của mình, và trên các sản phẩm này phải có tính năng bắt buộc người dùng phải đặt lại mật khẩu khi sử dụng thiết bị lần đầu tiên. Các loại thiết bị chịu điều chỉnh của Luật này là rất nhiều, bao gồm tất cả các thiết bị kết nối Internet (trực tiếp hoặc gián tiếp).

1.2. Một báo cáo gần đây của Cơ quan thẩm định trách nhiệm của chính phủ Hoa Kỳ (Government Accountability Office - GAO) cho biết khả năng chống tấn công mạng của các hệ thống vũ khí quân đội Hoa Kỳ là kém.

Báo cáo lưu ý rằng các khía cạnh công nghệ thông tin được áp dụng nhằm tăng cường hiệu quả của các loại vũ khí chiến lược quốc gia đồng thời cũng tạo ra nguy cơ các loại vũ khí này bị tấn công bởi các đối tượng trên mạng. Ví dụ những điểm yếu, lỗ hổng trong các tính năng tự động kết nối cho phép tàu chiến và máy bay chiến đấu tiên tiến thu thập và truyền tải lượng dữ liệu khổng lồ nhằm tăng khả năng của chúng trong chiến đấu.

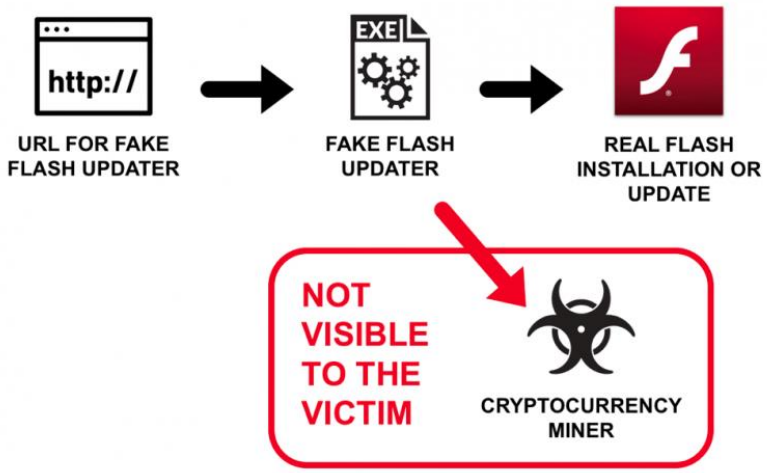
Trong các hoạt động thử nghiệm, Bộ Quốc phòng Hoa Kỳ (DoD) thường xuyên tìm thấy những lỗ hổng quan trọng trong các hệ thống. Trên thực tế, GAO đã tìm thấy gần như tất cả các chương trình thử nghiệm từ năm 2012 đến năm 2017 đều tồn tại lỗ hổng bảo mật. Báo cáo ghi nhận, DoD đã được cảnh báo nhiều lần trong 20 năm qua về việc cần phải tăng cường bảo vệ các hệ thống chống lại các cuộc tấn công mạng, tuy nhiên các tiêu chí bảo mật lại không phải là trọng tâm được lưu ý trong quá trình mua bán vũ khí.

1.3. Phát tán mã độc đào tiền ảo thông qua bản cập nhật Flash giả mạo

Trong những năm gần đây, đối tượng tấn công thường phát tán phần mềm độc hại thông qua những tập tin thực thi hoặc các tập tin Downloader trong đó cho phép cài đặt mã độc. Khi người dùng thực thi tập tin này trên máy tính (có khả năng bị khai thác lỗ hổng) thì không thấy có bất kỳ dấu hiệu bất thường nào.

Theo phân tích của PaloAlto, một trong những hình thức được đối tượng tấn công sử dụng để phát tán mã độc đào tiền ảo, mã độc mã hóa tư liệu và mã độc ăn trộm thông tin gần đây là yêu cầu người dùng cập nhật phiên bản Flash. Theo đó khi người dùng chấp nhận cập nhật thì bản cập nhật Flash giả mạo này sẽ cài đặt mã độc có tên XMRig, đồng thời cũng cập nhật cả phiên bản Flash có xác nhận và thông báo từ trình cài đặt Adobe (cải tiến so với những hình thức

giả mạo trước đây), do đó người dùng không thể nhận ra những hoạt động bất thường, trong khi đó mã độc XMRig vẫn đang chạy như tiến trình nền trên máy tính người dùng và thực hiện nhiều chức năng độc hại mà người dùng không biết.




Đường dẫn các bản cập nhật Flash giả mạo thường có chứa chuỗi ký tự "*flashplayer_down.php?clickid=*". Đã có ít nhất 113 mẫu khác nhau có đính kèm mã độc đã được tìm thấy, trong đó có tới 77 mã độc là CoinMiner.

Danh sách chi tiết các mẫu mã độc và URL phát tán bản cập nhật Flash giả mạo:

hxxps://raw.githubusercontent.com/pan-unit42/iocs/master/fake_Flash_updates/2018-09-fake-Flash-updates-APPENDIX-A.txt

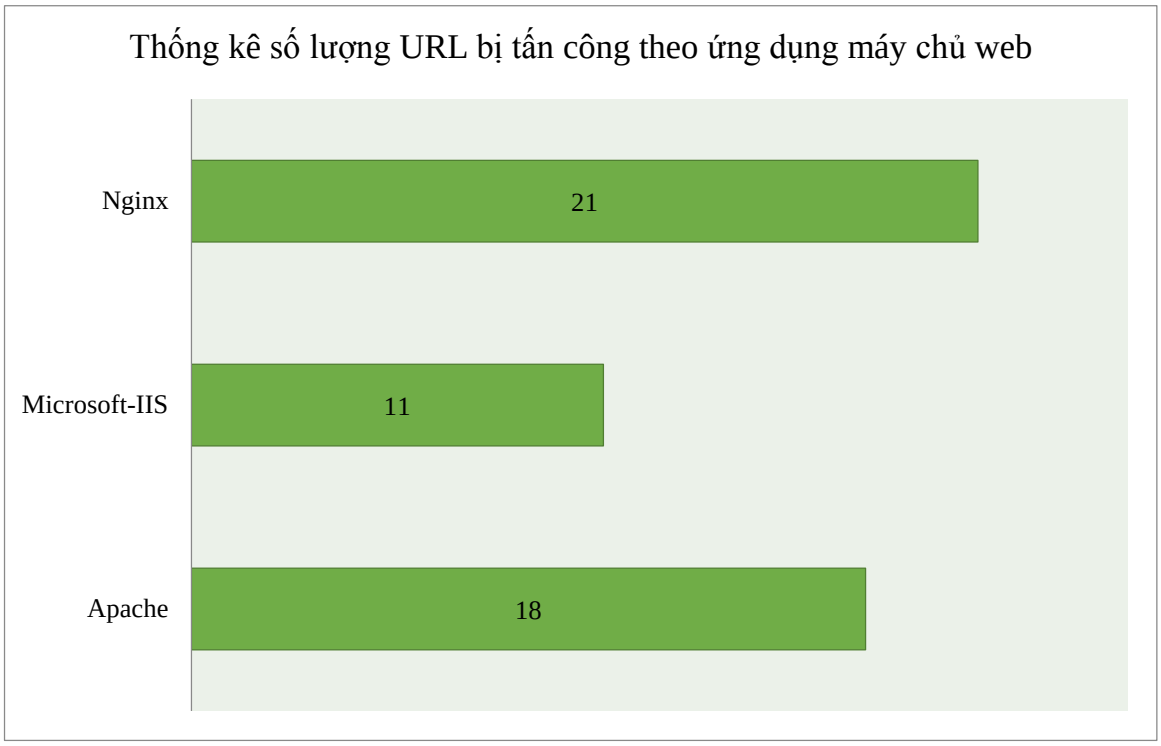
hxxps://github.com/pan-unit42/iocs/blob/master/fake_Flash_updates/2018-09-fake-Flash-updates-APPENDIX-B.txt

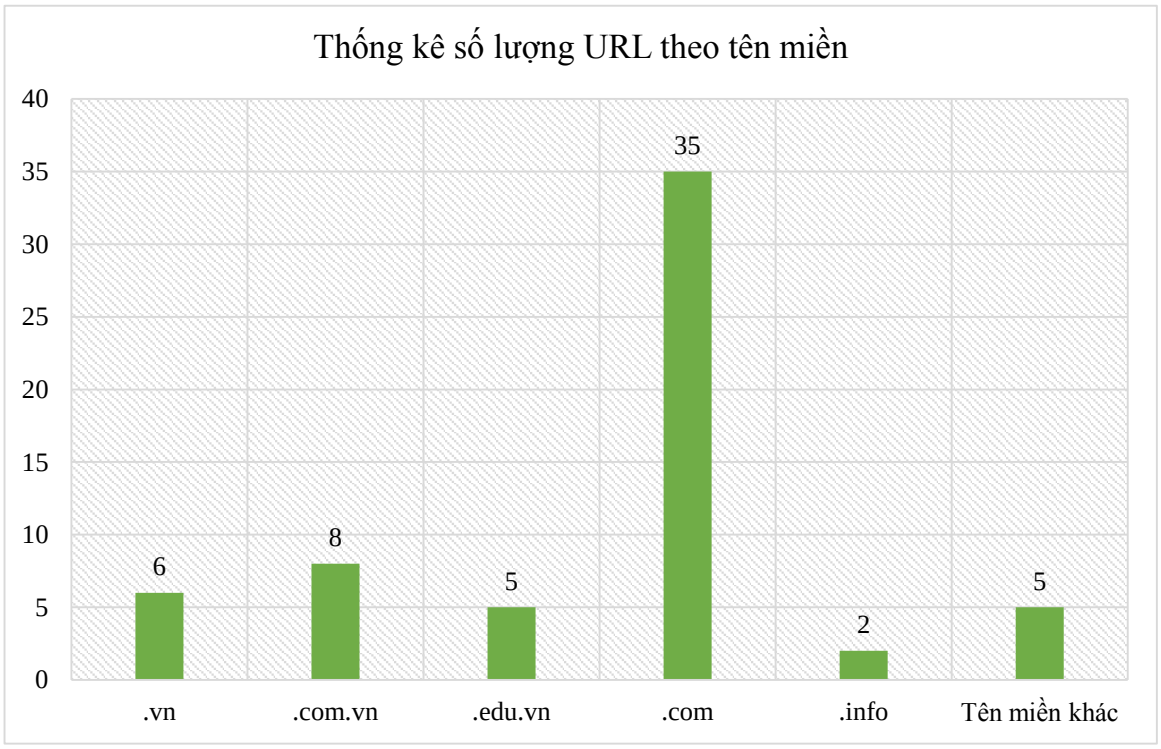
**2. Tình hình tấn công gây nguy hại trên các trang web tại Việt Nam**

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

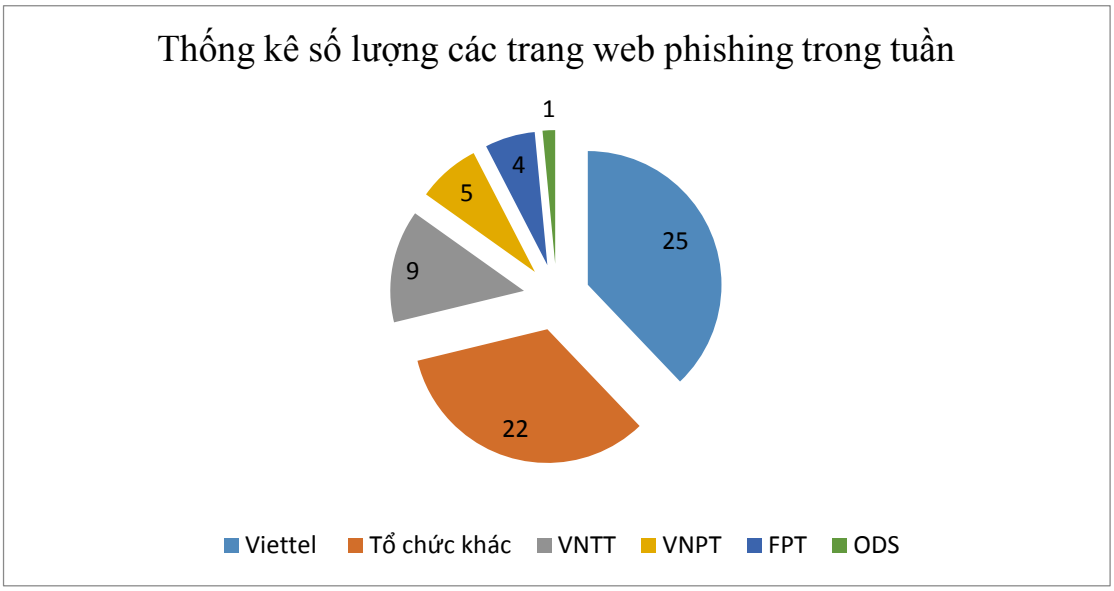
an toàn thông tin. Trong đó, thống kê, phân loại các đường dẫn này theo loại ứng dụng máy chủ web ( IIS, Apache …) và nhà cung cấp cụ thể như sau:



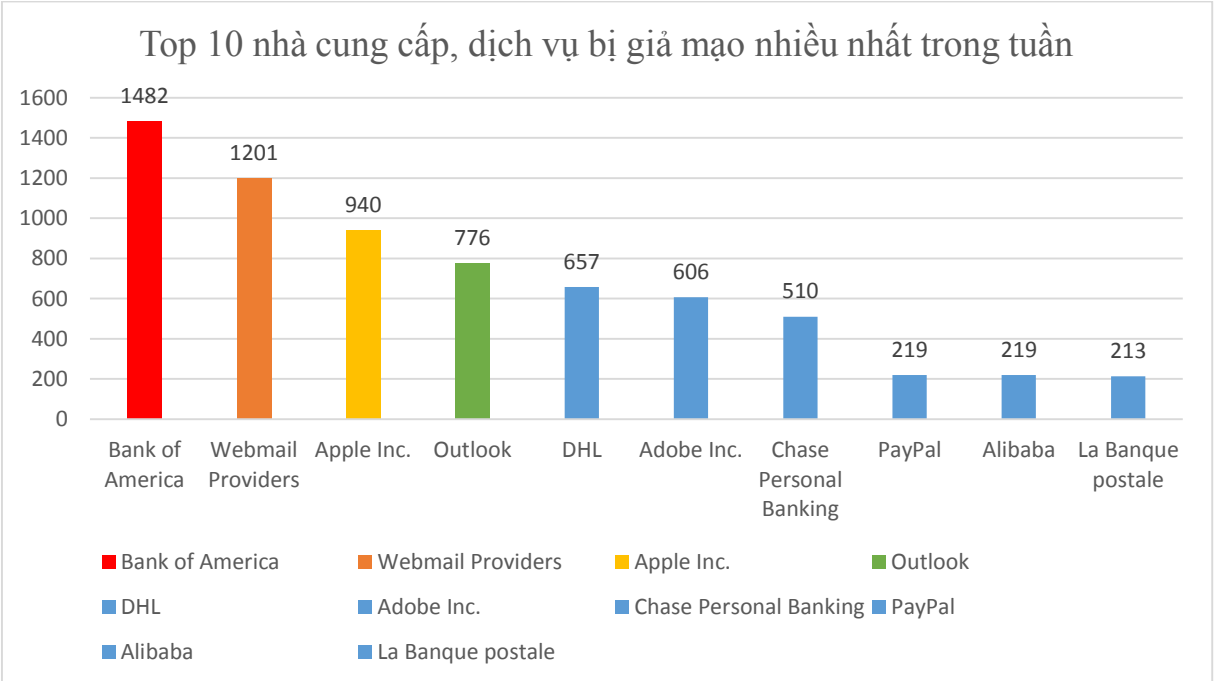



### 3. Tình hình tấn công lừa đảo (Phishing) trong tuần

3.1. Qua thu thập, theo dõi, trích xuất từ hệ thống kỹ thuật, Cục ATTT còn ghi nhận có ít nhất **66** 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 và cập nhật ít nhất 441 lỗ hổng, trong đó có ít nhất 97 lỗ hổng RCE (cho phép chèn và thực thi mã lệnh) và 17 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 **08** 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 86 lỗ hổng trong phần mềm trong một số phiên bản Adobe Acrobat & Reader; Nhóm 49 lỗ hổng trên một nhiều sản phẩm của Microsoft..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 | Adobe | CVE-2018-12860<br>CVE-2018-12836<br>CVE-2018-12835<br>... | Nhóm 86 lỗ hổng trong một số phiên bản của phần mềm Adobe Acrobat & Reader cho phép đối tượng tấn công thực hiện nhiều hình thức tấn công khác nhau, trong đó có 46 lỗ hổng cho phép chèn và thực thi mã lệnh. | Đã có thông tin xác nhận và bản vá |
| 2 | Auto-maskin | CVE-2018-5399<br>CVE-2018-5402<br>CVE-2018-5400<br>… | Nhóm 04 lỗ hổng trên các sản phẩm của Auto-maskin (bảng điều khiển từ xa sử dụng để giám sát và điều khiển từ xa - dùng trong nhiều hệ thống điều khiển công nghiệp) cho phép đối tượng tấn công có thể lấy được tài khoản Root (do đã thiết lập thông tin tài khoản sẵn trong file cấu hình); cho phép thay đổi cấu hình của thiết bị và cài cắm tập tin độc hại lên hệ thống. | Chưa có thông tin xác nhận và bản vá |

| | | | | |
|---|---|---|---|---|
| 3 | D-link | CVE-2018-17443<br>CVE-2018-17441<br>CVE-2018-17442<br>….. | Nhóm 06 lỗ hổng trên thiết bị phát wifi của D-link cho phép đối tượng tấn công thực hiện một số hình thức tấn công gồm: tấn công XSS, thực thi mã lệnh, thu thập thông tin xác thực do lưu trữ mật khẩu ở dạng rõ. | Đã có mã khai thác<br>Chưa có thông tin xác nhận và bản vá |
| 4 | Foxit | CVE-2018-3992<br>CVE-2018-3945<br>CVE-2018-3997<br>… | Nhóm 14 lỗ hổng trên một số sản phẩm, phần mềm của Foxit (PDF Reader, PhantomPDF) cho phép đối tượng tấn công chèn và thực thi mã lệnh. Đối tượng tấn công có thể khai thác lỗ hổng thông qua tập tin đính kèm hoặc plugin của trình duyệt. | Đã có thông tin xác nhận và bản vá |
| 5 | Intel | CVE-2018-12153<br>CVE-2018-12152<br>CVE-2018-12172<br>… | Nhóm 08 lỗ hổng trên một số sản phẩm Intel (gồm Intel Graphics Drivers, Intel NUC FW, Intel NVMe, Intel QuickAssist Technology for Linux, Intel Rapid Web Server 3, Intel Server Board) cho phép đối tượng tấn công thực hiện một hoặc kết hợp các hình thức tấn công: chèn và thực thi mã lệnh, tấn công leo thang và thu thập thông tin nhạy cảm. | Đã có thông tin xác nhận và bản vá |
| 6 | Joomla | CVE-2018-17857<br>CVE-2018-17859<br>CVE-2018-17856<br>… | Nhóm 05 lỗ hổng trên phần mềm mã nguồn mở Joomla cho phép đối tượng tấn công thực hiện tấn công CSRF, nâng quyền truy cập, thực thi mã lệnh. | Chưa có tin xác nhận và bản vá |
| 7 | Juniper | CVE-2018-0063<br>CVE-2018-0060<br>CVE-2018-0057<br>…. | Nhóm 21 lỗ hổng trên một số sản phẩm, thiết bị của Juniper (Juniper Device Manager, Juniper NFX | Đã có thông tin xác nhận và bản vá |

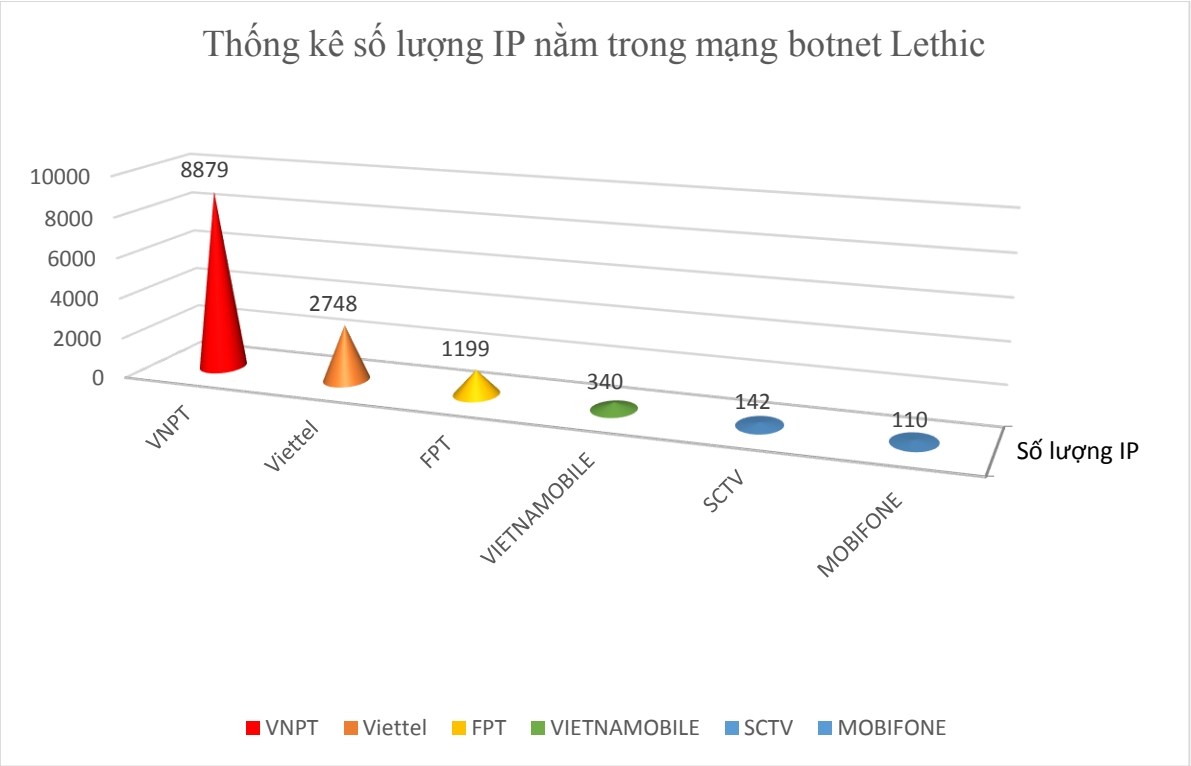
| | | | | |
|---|---|---|---|---|
| | | | Series, QFX5000 Series & EX4600 switch, ScreenOS, Juniper Networks Junos OS) cho phép đối tượng tấn công thực hiện một số hình thức tấn công khác nhau: tấn công XSS, tấn công từ chối dịch vụ, thực thi mã lệnh từ xa, thu thập thông tin trong hệ thống mạng thông qua thiết bị bao gồm cả những thông tin xác thực. | |
| 8 | Microsoft | CVE-2018-8500<br>CVE-2018-8530<br>CVE-2018-8503<br>... | Nhóm 49 lỗ hổng trên nhiều sản phẩm của Microsoft (ChakraCore, Microsoft Edge, Microsoft Exchange Outlook Web Access, Internet Explorer, Windows Media Player, SharePoint Server, Microsoft SQL Server Management Studio ... ) cho phép đối tượng tấn công thực hiện chèn và thực thi mã lệnh, thu thập thông tin và tấn công leo thang để kiểm soát hệ thống | 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 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 | disorderstatus.ru |
| 2 | differentia.ru |
| 3 | atomictrivia.ru |
| 4 | 83nmzuij.ru |
| 5 | koaoglxp.ru |
| 6 | kvamuvsju.ru |
| 7 | kukutrustnet777.info |
| 8 | ofytcx99yi.ru |
| 9 | 104.244.14.252 |
| 10 | kukutrustnet888.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;
- 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.

(email)

**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