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: **41**/BC-CATTT

Hà Nội, ngày 11 tháng 9 năm 2018

TÓM TẮT
Tình hình an toàn thông tin đáng chú ý trong tuần 36/2018
(từ ngày 03/9/2018 đến ngày 09/9/2018)

BẢNG TỔNG HỢP

1. Trong 2 năm trở lại đây, cách tiếp cận của chính quyền Đức với an toàn thông tin đã thay đổi. Trong quá khứ, nước Đức chú trọng vào việc phòng thủ, bảo vệ hệ thống mạng trước các cuộc tấn công. Mới đây, Đức đã thành lập một cơ quan mới chuyên trách trong vấn đề đầu tư nghiên cứu các công cụ tấn công và phòng thủ mạng, với mục tiêu "phòng thủ không gian mạng một cách chủ động".

2. Ngày 07/9/2018, British Airways đã cho đăng tin xin lỗi khách hàng sau khi có thông tin nhiều khách hàng của hãng bị ảnh hưởng trong một cuộc tấn công mạng.

3. Ngày 09/9/2018 nhóm chuyên gia của Palo Alto tiếp tục công bố biến thể mới của 02 mạng botnet lớn (IoT Mirai và Gafgyt). Đây là những mạng botnet thực hiện nhiều cuộc tấn công từ chối dịch vụ lớn từ 2016 đến nay.

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. Trong 2 năm trở lại đây, cách tiếp cận của chính quyền Đức với an toàn thông tin đã thay đổi. Trong quá khứ, nước Đức chú trọng vào việc phòng thủ, bảo vệ hệ thống mạng trước các cuộc tấn công. Mới đây, Đức đã thành lập một cơ quan mới chuyên trách trong vấn đề đầu tư nghiên cứu các công cụ tấn công và phòng thủ mạng, với mục tiêu "phòng thủ không gian mạng một cách chủ động".

Sử dụng các công cụ tấn công mạng phụ thuộc vào khả năng xác định và lợi dụng các lỗ hổng bảo mật trong phần cứng, phần mềm và các dịch vụ trực tuyến. Việc này cần phải thu thập và khai thác các lỗ hổng tiềm ẩn và nguy hiểm hay các lỗi zero day. Các lỗ hổng bảo mật "có giá trị" thường gây tác động đến những hệ điều hành hay phần mềm được sử dụng rộng rãi (như Windows, Android, iOS), những phần mềm phục vụ cho các hoạt động quân sự, tình báo và cả các lỗ hổng liên quan đến các hệ thống điều khiển công nghiệp hay phần cứng, phần mềm chuyên biệt.

Các lỗ hổng chính phủ Đức muốn tìm kiếm, thu thập cho hoạt động phòng thủ chủ động có thể cũng sẽ bị các tổ chức đối lập, các đối tượng tấn công mạng và các tổ chức khác lợi dụng.

Thông thường các công ty tư nhân, chủ quản cơ sở hạ tầng quan trọng và xã hội nói chung sẽ quan tâm đến việc chính phủ của mình đang nghiên cứu và sử dụng những lỗ hổng bảo mật trên những sản phẩm phổ biến như thế nào. Việc một lỗ hổng bảo mật do chính phủ tìm ra bị rò rỉ ra ngoài cũng sẽ gây ảnh hưởng tới công tác bảo vệ cơ sở hạ tầng, hệ thống thông tin quan trọng và các thông tin cá nhân của người dân. Nhà cung cấp phần cứng, phần mềm và dịch vụ trực tuyến cũng mong muốn xác định và xử lý các lỗ hổng trên sản phẩm của mình để đảm bảo an toàn cho dịch vụ và ngăn chặn tổn hại về tài chính và danh tiếng. Khối tư nhân và người dân mong muốn sử dụng các thiết bị và dịch vụ an toàn để tránh trở thành nạn nhân của việc nghe lén và các đối tượng tấn công mạng, hay đơn giản vì họ muốn được giao tiếp một cách tự do và an toàn. Nhìn chung, hệ sinh thái internet sẽ có lợi hơn từ việc vá các lỗ hổng bảo mật hơn là sử dụng chúng.

1.2. Ngày 07/9/2018, British Airways đã cho đăng tin xin lỗi khách hàng sau khi có thông tin nhiều khách hàng của hãng bị ảnh hưởng trong một cuộc tấn công mạng. Thông tin thẻ tín dụng của một số lượng lớn khách hàng bị đánh cắp trong vòng 2 tuần bởi một cuộc tấn công nghiêm trọng vào trang mạng và ứng dụng của hãng hàng không British Airways. Theo Giám đốc Điều hành Alex Cruz của British Airways, hãng hàng không này đã ngay lập tức thông báo với những khách hàng bị ảnh hưởng sau khi hậu quả của vụ tấn công được làm rõ.

Khoảng 380,000 thanh toán qua thẻ đã bị xâm nhập, trong đó đối tượng tấn công đã thu thập được tên, địa chỉ, địa chỉ thư điện tử, số thẻ tín dụng, thời gian hết hạn và mã xác minh thẻ - những thông tin đủ để thực hiện các giao dịch.

Hãng bảo mật Avast cho rằng, dựa trên các thông tin được cung cấp, đối tượng tấn công đã tấn công vào cổng giao tiếp giữa hãng hàng không và hệ thống xử lý thanh toán bởi vì không có thông tin nào về các chuyến bay bị đánh

cắp. Cơ quan chức năng của Anh cho biết, đã nhận được thông báo của British Airways và đang tiến hành xem xét. Theo như luật bảo vệ thông tin cá nhân GDPR mới, các công ty phải thông báo cho chính quyền về các cuộc tấn công mạng trong vòng 72 giờ đồng hồ.

1.3. Thời gian gần đây nhiều biến thể mã độc mới của các mạng botnet đã được phát hiện và công bố. Trong đó ngày 09/9/2018 nhóm chuyên gia của Palo Alto tiếp tục công bố biến thể mới của 02 mạng botnet lớn (IoT Mirai và Gafgyt). Đây là những mạng botnet thực hiện nhiều cuộc tấn công từ chối dịch vụ lớn từ 2016 đến nay. Trong đó:

- Biến thể của Mirai có khả năng khai thác 16 điểm yếu lỗ hổng, khác với những biến thể mã độc trước đây chỉ có khả năng khai thác 01 lỗ hổng đơn lẻ. Trong số đó nhiều lỗ hổng nằm trong thiết bị Home router, thiết bị camera vốn dĩ đã không có bản vá kịp thời khi có lỗ hổng được phát hiện. Đáng chú ý có cả lỗ hổng CVE-2017-5638 của Apache Strut, đây là lỗ hổng cho phép chèn và thực thi mã lệnh được phát hiện và công bố từ ngày tháng 10 năm 2017. Và lỗ hổng này đã có bản vá.

- Biến thể của Gafgyp tấn công vào lỗ hổng CVE-2018-9866 mới được công bố vào tháng 7 năm 2018, lỗ hổng trên cho phép chèn và thực thi mã lệnh trên SonicWall Global Management System GMS. Lỗ hổng này đã có bản vá.

Việc phát triển các mạng botnet khai thác lỗ hổng của Apache Struts và Sonic wall (những lỗ hổng đã có bản vá) cho thấy việc vá các lỗ hổng bảo mật trên các thiết bị, ứng dụng của các tổ chức ở nhiều quốc gia trên thế giới trong đó có Việt Nam chưa thực sự được quan tâm. Đây cũng chính là một trong những nguyên nhân, nguồn gốc của các cuộc tấn công mạng và đến khi xảy ra thì việc giải quyết hậu quả khó hơn gấp nhiều lần so với việc vá lỗ hổng bảo mật.

Dưới đây là một số thông tin kỹ thuật cơ bản các tổ chức có thể tham khảo để có những hành động kịp thời trong việc bảo đảm an toàn thông tin cho hệ thống thông tin của mình.

Địa chỉ IP/tên miền mã độc sử dụng: l.ocalhost.host; 185.10.68.213; 185.10.68.127

Danh sách lỗ hổng biến thể mã độc Mirai khai thác:

Mã/Tên lỗ hổng	**Thiết bị ảnh hưởng**	**Ghi chú**
CVE-2017-5638,	Apache Struts 2 2.3.x, 2.5.x	Mã khai thác ngày 07/3/2017

Linksys RCE	Thiết bị E-Series của Linksys	Không có mã CVE, Mã khai thác 16/2/2014
Vacron NVR RCE	Thiết bị Vacron NVR	Không có mã CVE Mã khai thác từ 08/10/2017
D-Link command.php RCE	Một số thiết bị Dlink	Không có mã CVE Mã khai thác từ ngày 2013-08-12
CCTV/DVR RCE	Thiết bị CCTV của nhiều hãng khác nhau	Không có mã CVE Mã khai thác từ ngày 2016-03-23
EnGenius RCE	EnGenius EnShare IoT Gigabit Cloud Service 1.4.11	Không có mã CVE Mã khai thác từ ngày 2017-06-04
AVTECH Unauthenticated Command Injection	Thiết bị AVTECH IP Camera/NVR/DVR	Không có mã CVE Mã khai thác từ ngày 2016-10-11
CVE-2017-6884	Router Zyxel	Mã khai thác từ ngày 2017-04-02
NetGain ‘ping’ Command Injection	Ứng dụng NetGain Enterprise Manager 7.2.562	Không có mã CVE Mã khai thác từ ngày 2017-02-23
NUUO OS Command Injection	NUUO NVRmini 2 3.0.8	Không có mã CVE Mã khai thác từ ngày 2016-08-06
Netgear setup.cgi unauthenticated RCE	Router DGN1000 Netgear	Không có mã CVE Mã khai thác từ ngày 2017-10-25
CVE-2015-2051	Thiết bị D-Link	Mã khai thác từ ngày 2015-06-01
D-Link OS Command Injection	Thiết bị D-Link DSL-2750B	Không có mã CVE Mã khai thác từ ngày 2018-05-25
JAWS Webserver authenticated shell command execution	MVPower DVRs và các thiết có sử dụng JAWS.	Không có mã CVE Mã khai thác từ ngày 2017-02-27

CVE-2018-10561, CVE-2018-10562	Router Dasan GPON	Mã khai thác từ ngày 2018-05-03

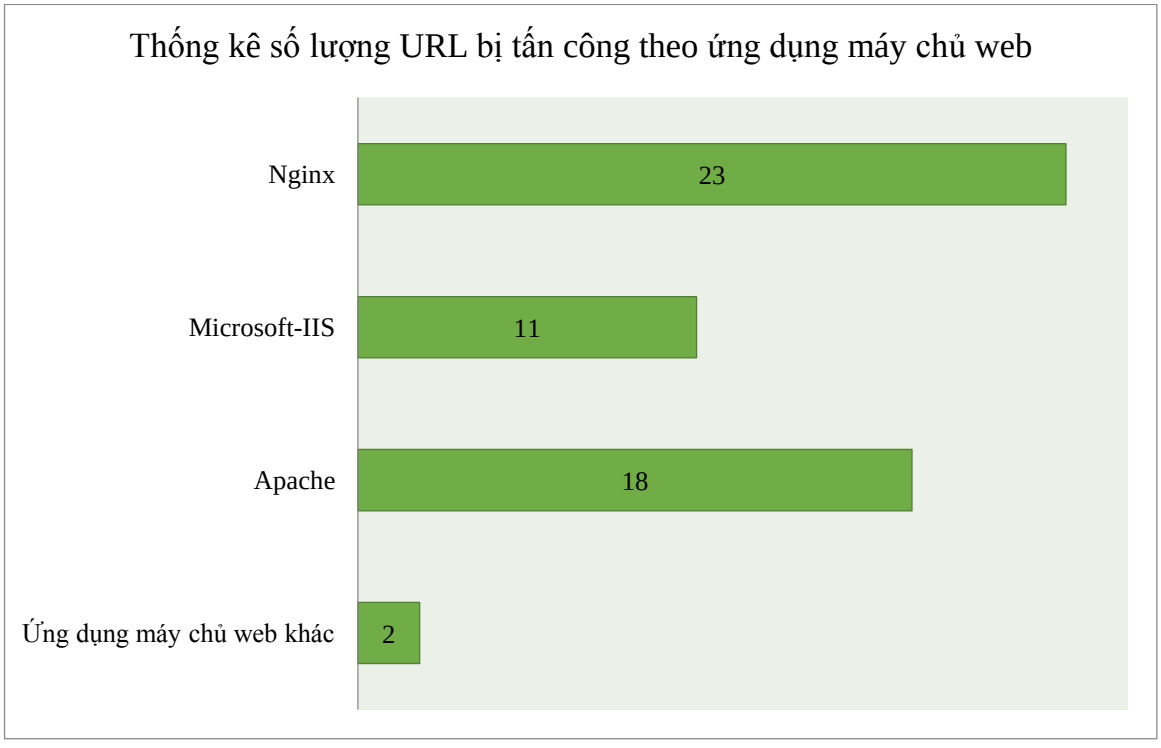
Tham khảo thêm mã hash (SHA256) của mẫu mã độc tại đường dẫn:

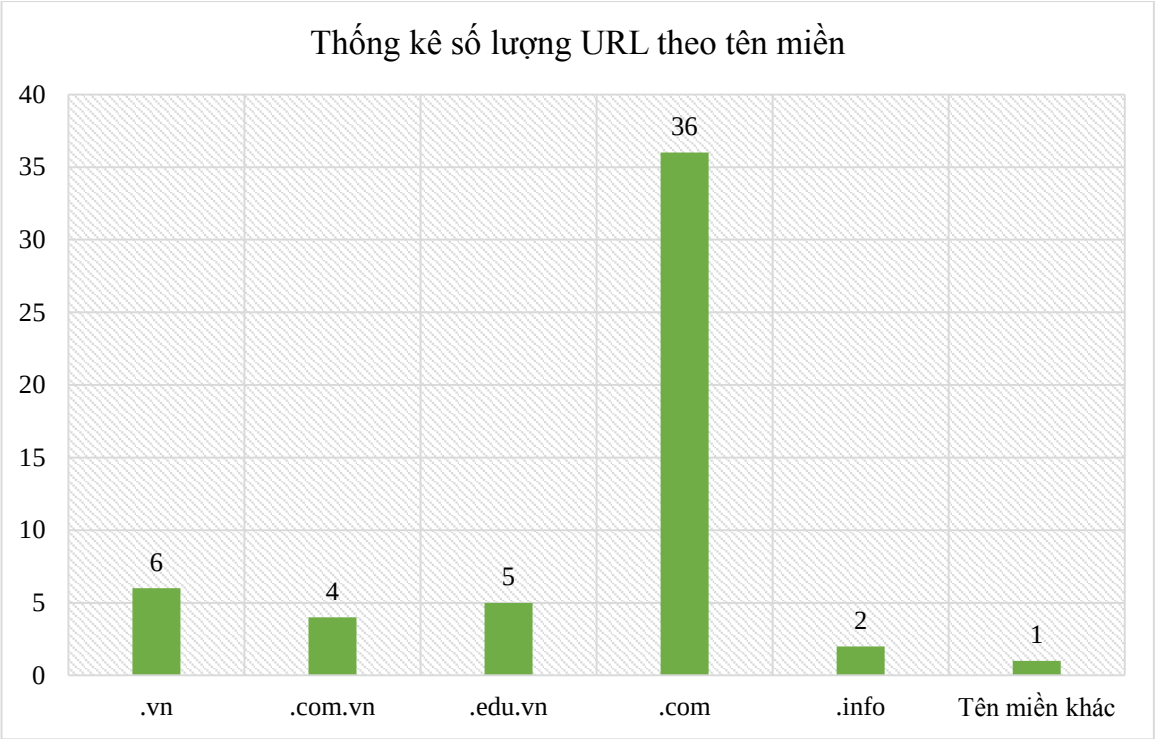
https://ti.khonggianmang.vn/dashboard/news/p/tin-tac-phat-trien-bien-the-ma-doc-moi-mirai-gafgypt

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…).

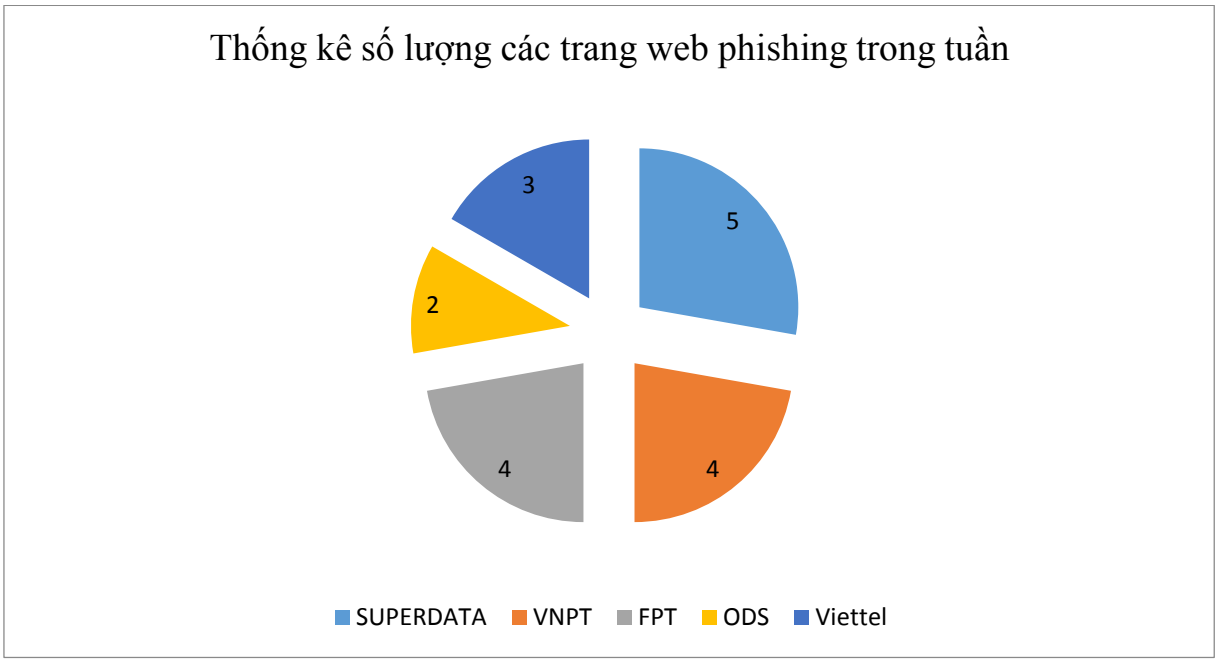
Trong tuần, Cục ATTT ghi nhận có ít nhất **54** đường dẫn (URL) trên các trang web tại Việt Nam bị tấn công, lợi dụng để thực hiện các hành vi gây mất an toàn thông tin. Trong đó, thống kê, phân loại các đường dẫn này theo loại ứng dụng máy chủ web (IIS, Apache …) và nhà cung cấp cụ thể như sau:



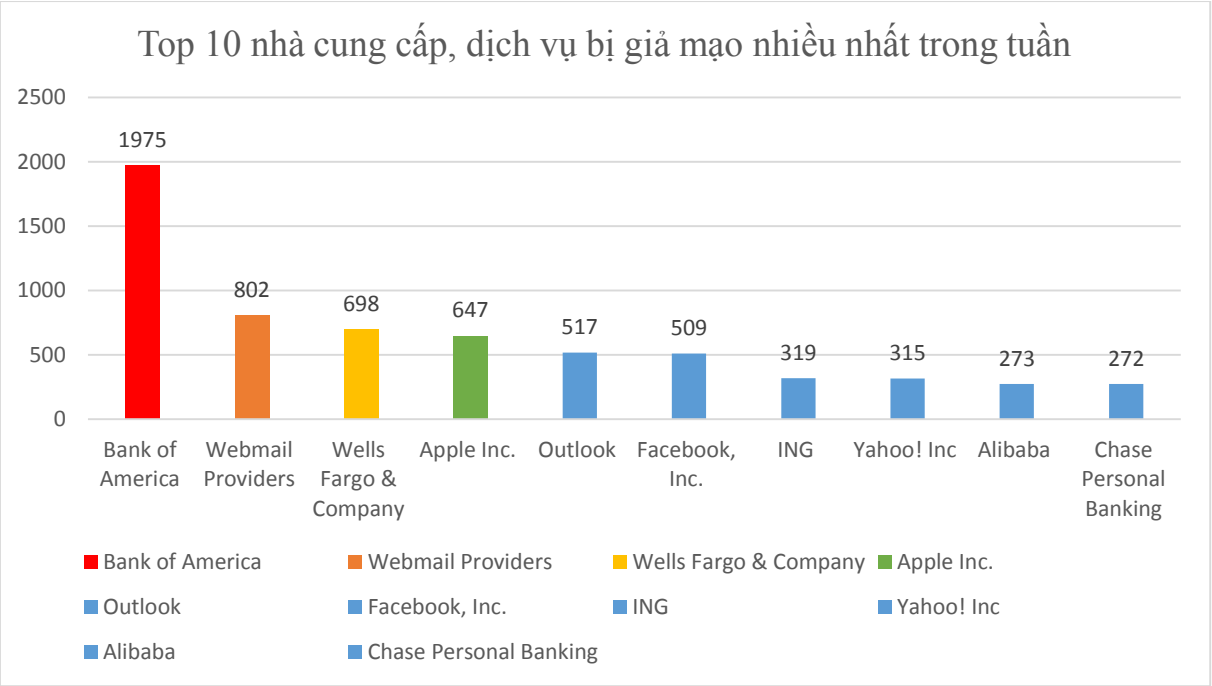


3. Tình hình tấn công lừa đảo (Phishing) trong tuần

3.1. Qua thu thập, theo dõi, trích xuất từ hệ thống kỹ thuật, Cục ATTT còn ghi nhận có ít nhất **20** 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 279 lỗ hổng, trong đó có ít nhất 15 lỗ hổng RCE (cho phép chèn và thực thi mã lệnh) và 6 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 **09** 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 7 lỗ hổng trên các sản phẩm của IBM; Nhóm 5 lỗ hổng trên hệ điều hành Android và sản phẩm gVisor của Google..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	Asus	CVE-2018-0647	Lỗ hổng trên thiết bị WL-330NUL của Asus cho phép đối tượng thực hiện tấn công CSRF.	Chưa có thông tin xác nhận

2	D-link	CVE-2018-16408	Lỗ hổng trên thiết bị DIR-846 với firmware phiên bản 100.26 của D-link cho phép đối tượng tấn công chèn và thực thi mã lệnh.	Đã có xác nhận và bản vá
3	Fortinet	CVE-2018-1353 CVE-2018-9194 CVE-2018-9192	Nhóm 3 lỗ trên trên các sản phẩm phần mềm của Fortinet (FortiOS, FortiManager) cho phép đối tượng thực hiện đánh cắp thông tin nhạy cảm, tấn công nghe lén.	Đã có thông tin xác nhận và bản vá
4	Google	CVE-2018-0664 CVE-2018-0650 CVE-2018-11262 CVE-2018-11263 CVE-2018-16359	Nhóm 5 lỗ hổng trên hệ điều hành Android và sản phẩm gVisor của Google cho phép đối tượng thực hiện tấn công truy cập và thay đổi thông tin hệ thống.	Đã có thông tin xác nhận và bản vá
5	Huawei	CVE-2018-7937 CVE-2018-7936 CVE-2018-7990 CVE-2018-7938	Nhóm 4 lỗ hổng trên các thiết bị của Huawei (HiRouter-CD20-10, Mate 10 Pro, P10) cho phép đối tượng thực hiện khống chế thiết bị qua ứng dụng độc hại, vô hiệu hóa tính năng FRP, đánh cắp thông tin.	Đã có thông tin xác nhận và bản vá
6	IBM	CVE-2018-1789 CVE-2018-1115 CVE-2018-1114 CVE-2018-1757 CVE-2018-1756 …	Nhóm 7 lỗ hổng trên các sản phẩm của IBM (API Connect, Campaign, Security Identity Governace and Intelligent, Websphere Application Server) cho phép đối tượng thực hiện tấn công SQL Injection, HTML Injection, chèn và thực thi JavaScript, đánh cắp thông tin	Đã có thông tin xác nhận và bản vá
7	Team Viewer	CVE-2018-16550	Lỗ hổng trên Team Viewer các phiên bản từ 10.x đến	Chưa có thông tin

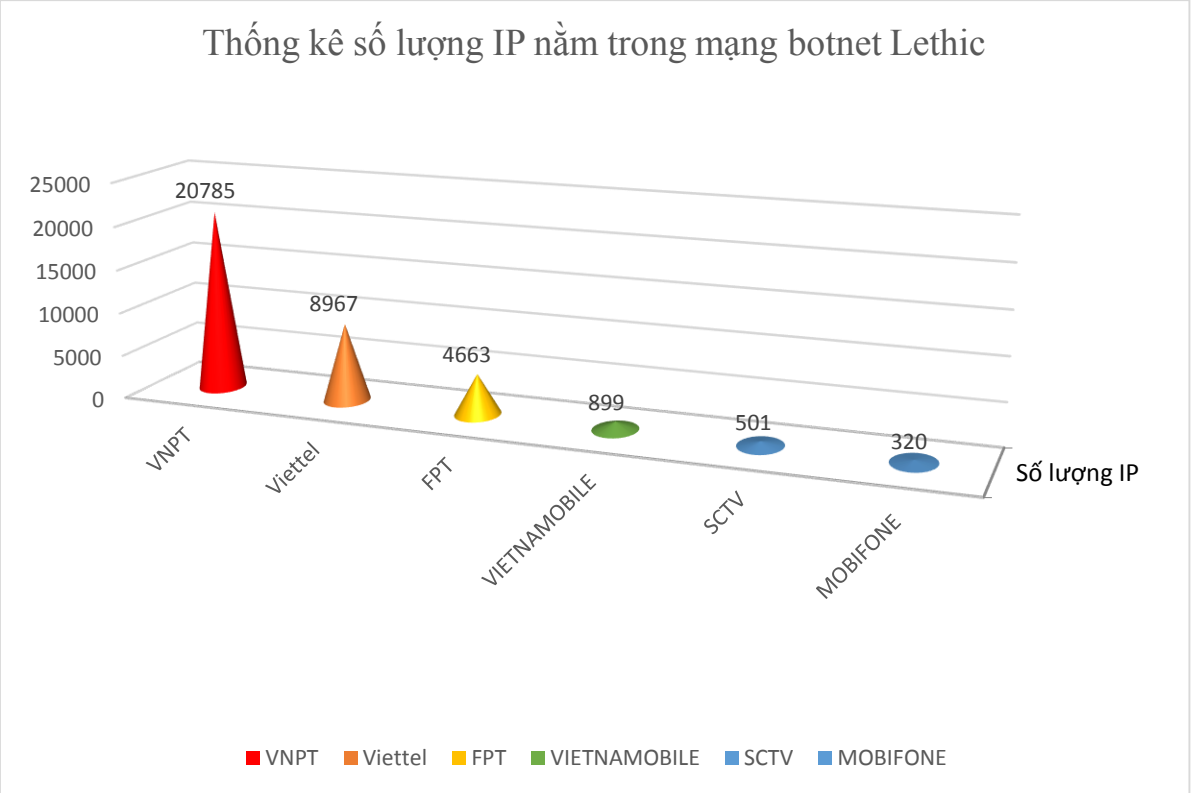
			13.x cho phép đối tượng bỏ qua các bước trong quá trình xác thực để thu được mã PIN mặc định gồm 4 ký tự.	xác nhận và bản vá
8	Wordpress	CVE-2018-16285	Lỗ hổng trên tiện ích UserPro của nền tảng Wordpess cho phép đối tượng thực hiện tấn công XSS.	Chưa có thông tin xác nhận và bản vá

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	disorderstatus.ru
2	differentia.ru
3	atomictrivia.ru
4	wxrk0otbm.ru
5	kukutrustnet777.info
6	i7gd9ultgx.ru
7	104.244.14.252
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	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