BỘ THÔNG TIN VÀ TRUYỀN THÔNG
CỤC AN TOÀN THÔNG TIN
TRUNG TÂM GIÁM SÁT AN TOÀN KHÔNG GIAN MẠNG QUỐC GIA

Báo cáo tóm tắt
Tình hình an toàn thông tin đáng chú ý tuần 35 (từ 26/08 - 01/09/2019)

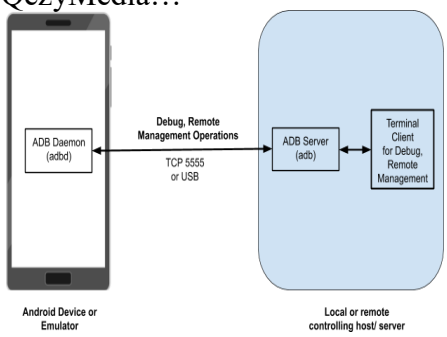
Số: /BC-CATTT *Hà Nội, ngày 03 tháng 09 năm 2019*

ỦY BAN ATTT MẠNG CỦA AUSTRALIA ĐƯỢC TRAO QUYỀN BUỘC CÁC NHÀ MẠNG CHẶN MỘT SỐ NỘI DUNG NHẤT ĐỊNH

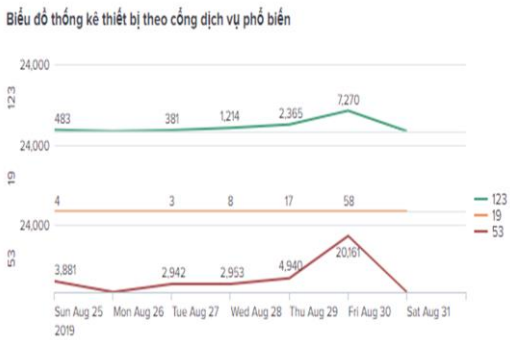
Ngày 25/8/2019, theo Reuters, Ủy ban an toàn thông tin mạng của Australia sẽ được trao quyền buộc các nhà mạng phải chặn một số nội dung nhất định trong tình huống khẩn cấp.

MẠNG BOTNET IOT MỚI NHẮM MỤC TIÊU THIẾT BỊ PHÁT ĐA PHƯƠNG TIỆN CHO TV THÔNG MINH

Hãng WootCloud đã phát hiện ra một botnet IoT mới có tên Ares đang lây nhiễm trên thiết bị Android (hộp set-top) sử dụng cho các TV thông minh phổ biến. Các hãng có sản phẩm đã xác định bị botnet này lây nhiễm, khai thác bao gồm các hộp set-top Android được sản xuất bởi HiSilicon, Cubetek và QezyMedia…



THỐNG KÊ NGUỒN TẤN CÔNG DDOS



ĐIỂM YẾU, LỖ HỔNG AN TOÀN THÔNG TIN

Trong tuần, các tổ chức quốc tế đã công bố và cập nhật ít nhất 461 lỗ hổng, trong đó có 57 lỗ hổng mức cao, 124 lỗ hổng mức trung bình, 5 lỗ hổng mức thấp và 275 lỗ hổng chưa đánh giá. Trong đó có ít nhất 43 lỗ hổng cho phép chèn và thực thi mã

DARK READING ĐÃ CÓ BÀI CHIA SẺ VỀ KHẢ NĂNG SẴN SÀNG ĐỐI MẶT VỚI CÁC NGUY CƠ, RỦI RO TRONG NĂM 2019

Ngày 29/8/2019, DARK reading đã có bài chia sẻ về khả năng sẵn sàng đối mặt với các nguy cơ, rủi ro mất an toàn dữ liệu cá nhân trong năm 2019. Bài viết đã liệt kê hàng loạt vụ lộ lọt, vi phạm dữ liệu đã bị Chính quyền đưa ra án phạt từ đầu năm.

1. Điểm tin đáng chú ý

1.1. Ngày 25/8/2019, theo Reuters, Ủy ban an toàn thông tin mạng của Australia sẽ được trao quyền buộc các nhà mạng phải chặn một số nội dung nhất định trong tình huống khẩn cấp. Thủ tướng Australia Scott Morrison cho biết chính phủ nước này dự định ngăn chặn đối tượng xấu lợi dụng, khai thác các nền tảng kỹ thuật số để đăng nội dung bạo lực. Australia và New Zealand đã gia tăng sự giám sát của các trang web và các công ty truyền thông xã hội sau vụ việc ở thành phố Christchurch vào tháng 3/2019, khi nhiều người bị tấn công bằng súng và bị đối tượng tấn công phát trực tiếp (livestream) trên Facebook. Chính phủ cho biết sẽ thiết lập phương thức để chặn các tên miền lưu trữ tài liệu, thông tin vi phạm.

Australia sẽ xác định từng trường hợp cụ thể những gì cần kiểm duyệt. Trên cơ sở, chính phủ đang làm việc với các tổ chức, doanh nghiệp trong các ngành, lĩnh vực khác nhau về các thỏa thuận để có thể nhanh chóng thực hiện công tác ngăn chặn truy cập. Một Trung tâm điều phối 24/7 (CC Centre) sẽ được thành lập để giám sát trực tuyến thông tin vi phạm. Những công ty công nghệ bao gồm: Facebook, YouTube, Amazon, Microsoft và Twitter, cùng với Telstra, Vodafone, TPG và Optus dự kiến sẽ cung cấp thông tin chi tiết vào cuối tháng tới về cách họ thực hiện yêu cầu của Chính phủ.

1.2. Ngày 29/8/2019, DARK reading đã có bài chia sẻ về khả năng sẵn sàng đối mặt với các nguy cơ, rủi ro mất an toàn dữ liệu cá nhân trong năm 2019. Bài viết đã liệt kê hàng loạt vụ lộ lọt, vi phạm dữ liệu đã bị Chính quyền đưa ra án phạt từ đầu năm như: Cơ quan quản lý quyền riêng tư của Anh đã phạt hãng hàng không Anh British Airways với số tiền 230 triệu USD và 125 triệu USD đối với công ty kinh doanh khách sạn Marriott vì vi phạm các quy định của GDPR (Quy định bảo vệ dữ liệu chung của châu Âu); Tiếp theo là việc Max Schrems (Một Luật sư người Áo ủng hộ quyền riêng tư) đã kiện Facebook về khả năng gây nguy hiểm cho xã hội tương lai với các luồng dữ liệu xuyên biên giới. Và gần đây, FTC (Ủy ban thương mại Hoa Kỳ) công bố phạt công khai mức phạt kỷ lục với số tiền là 5 tỷ USD, liên quan đến bê bối vi phạm dữ liệu của công ty Cambridge Analytica.

Cũng theo bài báo, hơn 500.000 tổ chức đã đăng ký bảo vệ dữ liệu cho nhân viên ở châu Âu theo quy định của GDPR. Tuy nhiên, theo các chuyên gia, để kiểm soát luồng dữ liệu trên hàng ngàn hệ thống dữ liệu, mạng lưới các nhà cung cấp, kiến trúc đám mây v.v… thì các tổ chức dù lớn hay nhỏ phải có sự tham gia của người có trình độ cao, các công nghệ kiểm soát, an toàn dữ liệu và quy trình. Đây thực sự là thách thức lớn, một vấn đề tương đối phức tạp mà gần như các tổ chức, cá nhân chưa thực sự sẵn sàng.

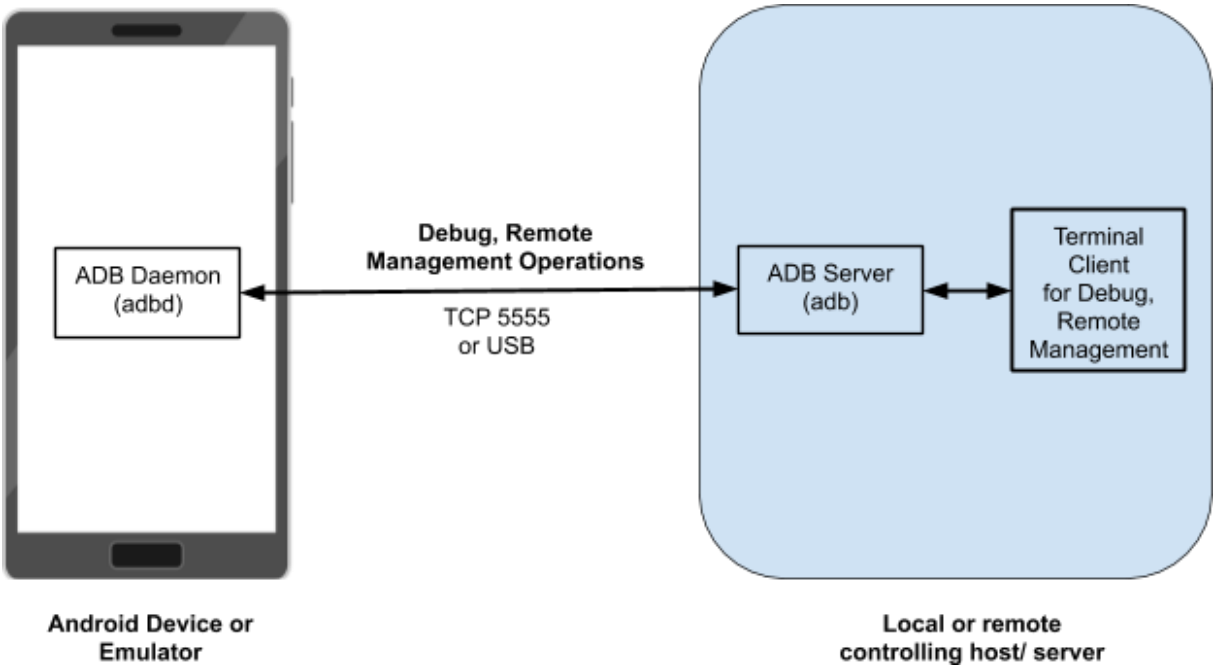
1.3. Hãng WootCloud đã phát hiện ra một mạng botnet IoT mới có tên Ares đang lây nhiễm trên thiết bị Android (hộp set-top) sử dụng cho các dòng TV thông minh phổ biến. Các hãng có sản phẩm đã xác định bị mạng botnet này lây nhiễm, khai thác bao gồm các hộp set-top Android được sản xuất bởi HiSilicon, Cubetek và QezyMedia…

Phương thức tấn công của mạng Botnet mới này không sử dụng lỗ hổng trong hệ điều hành Android, nhưng đang khai thác một dịch vụ cấu hình đã được kích hoạt và không được bảo vệ trên một số cài đặt hộp set-top. Dịch vụ này có tên là Android Debug Bridge (ADB), đây là một tính năng tiêu chuẩn của HĐH Android. Mục đích của nó là cho phép các nhà sản xuất và nhà phát triển ứng dụng truy cập vào HĐH Android thông qua giao diện dòng lệnh. Thiết bị đầu cuối ADB này có thể được truy cập theo ba cách, thông qua kết nối có dây, WiFi hoặc qua mạng hoặc internet (qua cổng 5555 của thiết bị).

Nhà sản xuất thường sử dụng dịch vụ ADB để định cấu hình hoặc chạy thử nghiệm trên các thiết bị dựa trên Android. Trong hầu hết các dây chuyền sản xuất, nhiều công ty đã vô hiệu hóa dịch vụ trước khi vận chuyển thiết bị cho khách hàng.

Tuy nhiên, trong vài năm qua, khi thiết bị Android ngày càng trở nên phổ biến, nhiều nhà cung cấp vô tình không vô hiệu hóa tính năng này, nên thiết bị dễ dàng bị tội phạm mạng tiếp cận để tấn công từ xa.

Các hộp set-top Android là một thiết bị truyền phát đa phương tiện cho TV để chạy phiên bản chuyên biệt của HĐH Android. Chúng được sử dụng ngày càng phổ biến tại các gia đình và các địa điểm công cộng ... Số lượng của các thiết bị này đang tăng theo cấp số nhân.



Hình 1 - Mô hình khai thác thiết bị android của mạng Botnet

Vì tính năng của ADB là mở và không được xác thực nên khi kẻ tấn công phát hiện ra cổng TCP 5555 trên thiết bị, chúng sẽ xác định khả năng kiểm soát, xác thực và ủy quyền của thiết bị. Các chuyên gia thấy rằng dịch vụ ADB trên cổng TCP 5555, không chỉ được sử dụng để gỡ lỗi mà còn cho phép quản lý từ xa.

Khi tính năng quản lý từ xa có thể thực hiện qua giao diện gỡ lỗi, điều đó có nghĩa là việc truy cập thiết bị cho phép thực thi lệnh từ xa, tải lên/tải xuống các ứng dụng tùy chỉnh, truy cập dữ liệu và các ứng dụng khác. WootCloud đã phát hiện ra botnet Ares lây nhiễm và lan truyền bot là thông qua giao diện ADB.

Khi bot Ares được cài đặt trên các thiết bị chạy Android, nó sẽ khởi chạy máy quét để: Lấy dấu vân tay và phát hiện thêm các thiết bị Android thông qua giao diện ADB, Cài đặt payload dành riêng cho các thiết bị bị xâm nhập để kích hoạt thêm bộ tấn công như khai thác tiền điện tử, v.v...

Khuyến nghị biện pháp đối phó như sau:

• Triển khai các giải pháp kiểm soát truy cập qua cổng và dịch vụ của ứng dụng (Chặn cổng TCP 5555).

• Cấu hình các chính sách mạng, phân chia các vùng mạng riêng biệt để hạn chế lưu lượng truy cập mạng đi vào và đi ra của các thiết bị IoT.

• Tắt tính năng ADB trên các thiết bị IOT, đặc biệt là các thiết bị truyền phát đa phương tiện cho TV thông minh.

• Luôn cấu hình mật khẩu cho các phương thức truy cập như Telnet, Web, SNMP, v.v. trên các thiết bị IoT.

Thông tin chi tiết khác có thể tra cứu tại địa chỉ:

https://ti.khonggianmang.vn/dashboard/news/p/Mang-botnet-iot-moi-nham-muc-tieu-lay-nhiem-cac-thiet-bi-thong-minh/

2. Nguy cơ tấn công mạng từ điểm yếu lỗ hổng

Trong tuần, các tổ chức quốc tế đã công bố và cập nhật ít nhất 461 lỗ hổng, trong đó có 57 lỗ hổng mức cao, 124 lỗ hổng mức trung bình, 5 lỗ hổng mức thấp và 275 lỗ hổng chưa đánh giá. Trong đó có ít nhất 43 lỗ hổng cho phép chèn và thực thi mã lệnh.

Hệ thống kỹ thuật của Cục ATTT chủ động rà quét trên không gian mạng Việt Nam, đánh giá, thống kê cho thấy có 06 lỗ hổng/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 88 lỗ hổng trên sản phẩm của Microsoft; Nhóm 136 lỗ hổng trên nhiều plugin của Wordpress; Nhóm 79 lỗ hổng trên Adobe Acrobat and Reader, Nhóm 16 lỗ hổng trên Android, Nhóm 31 lỗ hổng trên sản phẩm của IBM, v.v…Thông tin chi tiết về 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-2019-7968 CVE-2019-7969 CVE-2019-7970 ….	Nhóm 34 lỗ hổng phiên bản sản phẩm của Adobe Photoshop CC cho phép đối tượng tấn công thực thi mã lệnh tùy ý Tuần 34 đã cảnh báo 79 lỗ hổng trong sản phẩm Adobe Acrobat.	Đã có thông tin xác nhận và bản vá
2	DLink	CVE-2019-15526 CVE-2019-15527 CVE-2019-15528 ...	Nhóm 08 lỗ hổng trên một số sản phẩm của DLink (Router Wifi DIR-823G, DIR-825AC G1) cho phép đối tượng tấn công chèn và thực thi mã lệnh qua nhiều tham số khác nhau, thực hiện, thu thập và chuyển dữ liệu giữa các vùng mạng cô lập khác nhau.	Một số lỗ hổng đã có thông tin xác nhận và bản vá
3	Linux Kernel	CVE-2019-15504 CVE-2019-15505 CVE-2019-15666 ...	Nhóm 05 lỗ hổng nghiêm trọng trong nhân Linux cho phép đối tượng tấn công giả mạo luồng dữ liệu USB, khai thác lỗi Out of Bounds để đọc dữ liệu trên hệ thống, tấn công từ chối dịch vụ Lỗ hổng có điểm CVSS 9.8	Đã có thông tin xác nhận và bản vá
	Xymon	CVE-2019-13451 CVE-2019-13452	Nhóm 08 lỗ hổng trên hệ điều hành Xymon cho phép khai	

		CVE-2019-13455 ...	thác lỗi tràn bộ đệm để chèn và thực thi mã lệnh. Lỗ hổng có điểm CVSS 7.5	
4	Atlassian	CVE-2019-11589 CVE-2019-8445 CVE-2019-14999 ...	Nhóm 12 lỗ hổng trên một số sản phẩn của Atlassian (Jira,Atlassian Universal Plugin Manager) cho phép đối tượng tấn công khai thác lỗi XSS, CSRF, thu thập thông tin tài khoản người dùng, chuyển hướng người dùng đến trang web độc hại. Một số lỗ hổng đã được cảnh báo trong tuần 34	Đã có thông tin xác nhận bản vá.
5	Ricoh	CVE-2019-14305 CVE-2019-14307 CVE-2019-14308 ...	Nhóm 04 lỗ hổng trên nhiều dòng máy in của Ricoh cho phép đối tượng tấn công khai thác lỗi tràn bộ đệm để chèn và thực thi mã lệnh, từ đó có thể thu thập được nhiều thông tin quan trọng trên các máy in này.	Đã có thông tin xác nhận và bản vá
6	Wordpress	CVE-2015-9372 CVE-2019-15774 CVE-2019-15836 ...	Nhóm 75 lỗ hổng trên nhiều thành phần plugin của Wordpress (Membership Add-on for iThemes Exchange, nd-booking, wp-ultimate-recipe, ...) cho phép đối tượng tấn công khai thác lõi XSS, CSRF, SQL Injection, sửa đổi thông số cài đặt,	Một số lỗ hổng đã có thông tin xác nhận và bản vá

3. Nguy cơ phát tán tấn công từ chối dịch vụ

Tấn công từ chối dịch vụ là hình thức tấn công đã có từ lâu, và hiện tại vẫn được đối tượng tấn công ưa thích sử dụng để thực hiện các ý đồ xấu. Tấn công từ

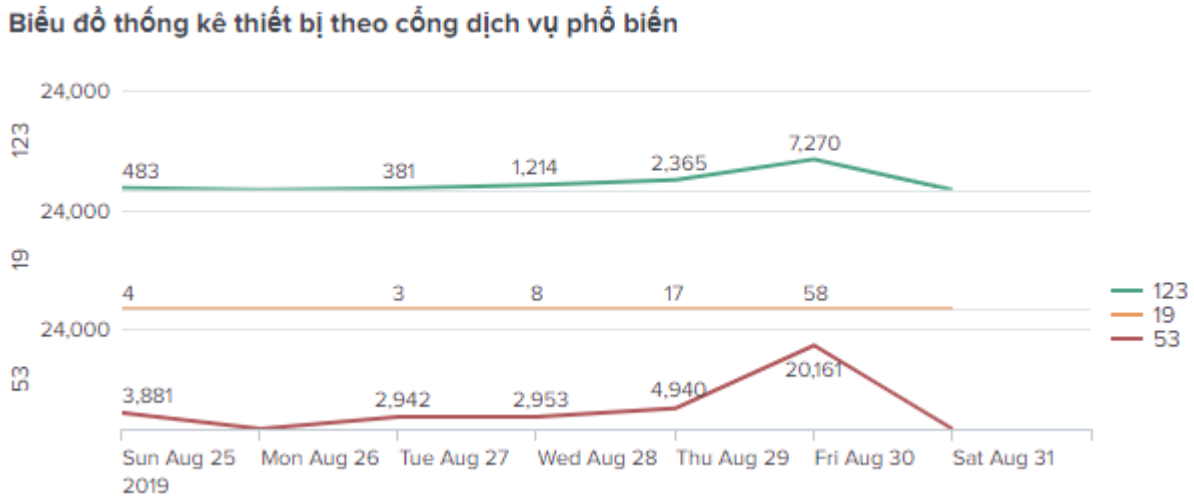
chối dịch vụ về cơ bản không nguy hiểm nhưng lại gây ảnh hưởng đến hoạt động của hệ thống, gây thiệt hại về kinh tế cho tổ chức bị tấn công.

Tấn công từ chối dịch vụ có thể được thực hiện với nhiều kỹ thuật khác nhau, nhưng trong những năm gần đây phần lớn tin tặc huy động các thiết bị đang mở cổng dịch vụ sử dụng giao thức UDP để thực hiện tấn công. Các thiết bị này có thể bị huy động dễ dàng để thực hiện tấn công DRDoS (tấn công từ chối dịch vụ phản xạ phân tán/Distributed Reflective Denial-of-Service) mà hiệu quả tấn công lại rất cao. Rất nhiều giao thức tầng ứng dụng đều có điểm yếu/lỗ hổng cho phép thực hiện tấn công này.

Giao thức	**Số lần khuếch đại băng thông**
DNS	28 lần 54
NTP	556.9
SNMPv2	6.3
NetBIOS	3.8
SSDP	30.8
CharGEN	358.8
QOTD	140.3
BitTorrent	3.8
Kad	16.3
Quake Network Protocol	63.9
Steam Protocol	5.5
Multicast DNS (mDNS)	2 đến 10
RIPv1	131.24
Portmap (RPCbind)	7 đến = 28
LDAP	46 đến 55
CLDAP	56 đến 70
TFTP	60
Memcached	10,000 đến 51,000

Tại Việt Nam, có rất nhiều máy chủ, thiết bị có thể trở thành nguồn phát tán tấn công DRDoS. Trong tuần có **46,680 (giảm so với tuần trước là 47, 519)** thiết bị

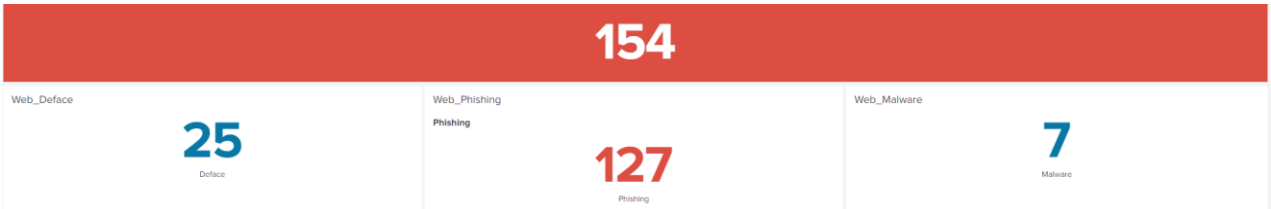
có khả năng bị huy động và trở thành nguồn tấn công DRDoS. Các thiết bị này đang mở sử dụng các dịch vụ NTP (123), DNS (53), Chargen (19). Dưới đây là biểu đồ thống kê thiết bị theo cổng dịch vụ phổ biến trong tuần

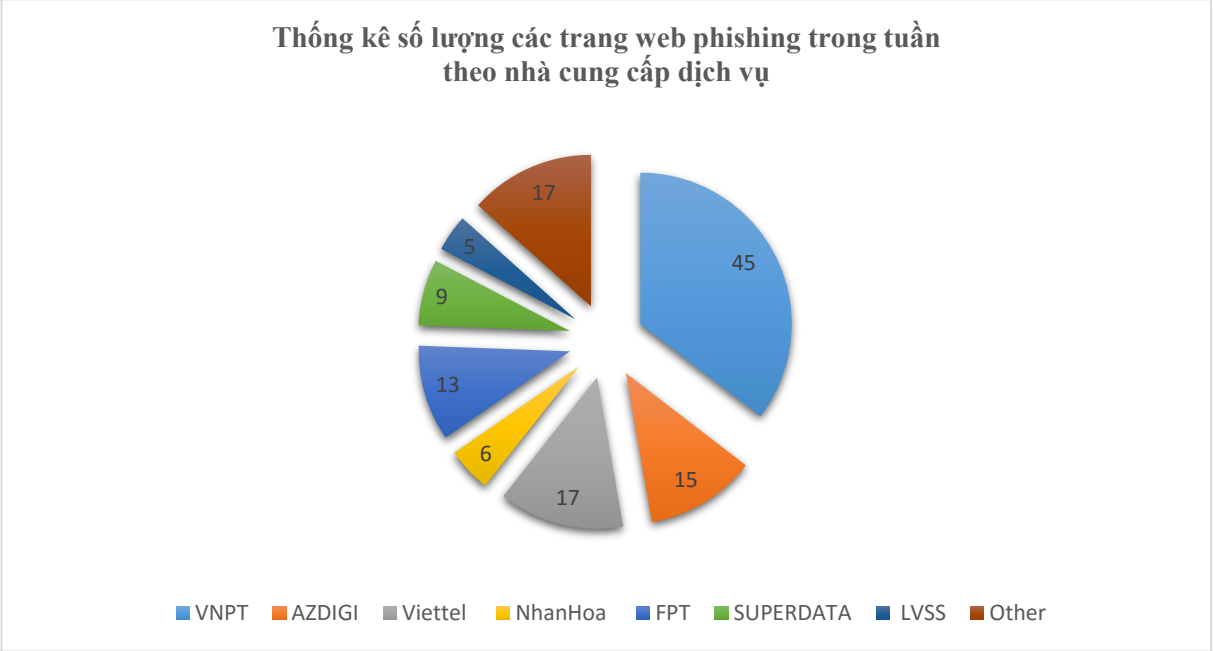


4. Tấn công vào Cổng TTĐT/ứng dụng web của Việt Nam

Website/Cổng thông tin điện tử là kênh cung cấp thông tin hiệu quả tuy nhiên hầu hết không được quan tâm đến việc bảo đảm an toàn cho website, rất nhiều trang tồn tại điểm yếu, lỗ hổng bảo mật, đối tượng tấn công có thể khai thác để thực hiện: tấn công thay đổi giao diện, tấn công lừa đảo thu thập thông tin tài khoản, thông tin cá nhân, tấn công cài cắm và phát tán mã độc.

Trong tuần, có 154 trường hợp tấn công vào trang/cổng thông tin điện tử của Việt Nam: 25 trường hợp tấn công thay đổi giao diện, 127 trường hợp tấn công lừa đảo (Phishing), 07 trường hợp tấn công cài cắm mã độc.

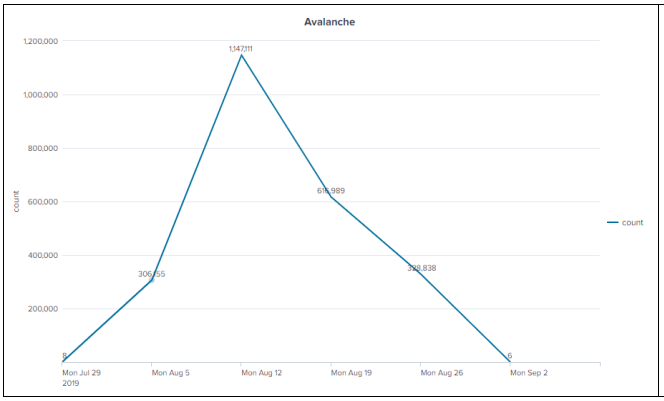


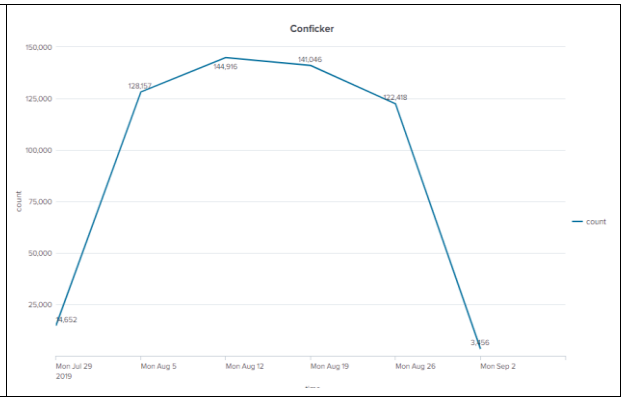


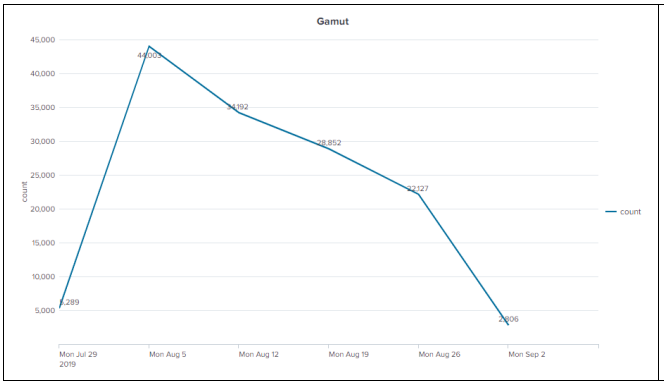
5. Hoạt động của mạng botnet, APT, mã độc tại Việt Nam

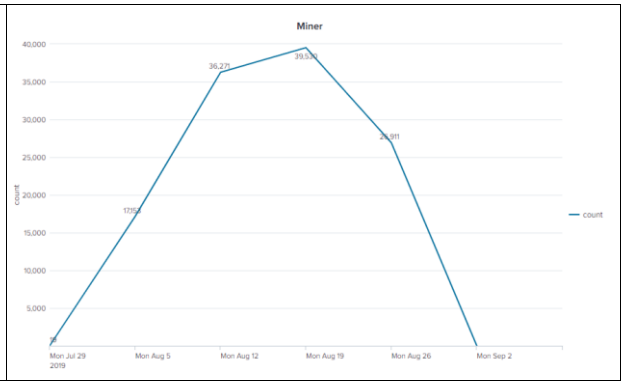
5.1. Các mạng botnet phổ biến

Tại Việt Nam có nhiều mạng botnet lớn trên thế giới đang hoạt động, trong đó nổi bật là Avalanche, Conficker, Gamut, IoTbotnet/Mirai, PonyLoader, Sality, Wanacry … Các mạng này được hình thành từ những máy tính, điện thoại thông minh, thiết bị mạng … bị lây nhiễm mã độc. Mỗi mạng botnet đều có đặc điểm, mục tiêu khác nhau, tuy nhiên đều có đặc điểm là khi đã bị lây nhiễm mã độc và tham gia vào các mạng botnet này thì sẽ bị đối tượng tấn công kiểm soát từ xa và lợi dụng để: phát tán thư rác/mã độc mới, thu thập thông tin, dữ liệu trên máy tính người dùng, tấn công từ chối dịch vụ … và góp phần làm tăng tỉ lệ lây nhiễm mã độc ở Việt Nam. Dưới đây là biểu đồ hoạt động của một số mạng mạng botnet lớn trong tuần:









Trong tuần mạng botnet **Avalanche** (chuyên đánh cắp thông tin người dùng) hoạt động nhiều nhất và giảm so với tuần trước, có 328.838 lượt địa chỉ IP kết nối với máy chủ điều khiển (Tuần 34 là 335.777).

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	y3w75xctac.ru
5	xjpakmdcfuqe.com
6	soplifan.ru
7	v99ay4wuo.ru
8	p84epcnjzy.ru
9	xdqzpbcgrvkj.ru
10	ixhtiv.info
11	www.cityofangelsmagazine.com
12	kukutrustnet777.info
13	mel.cloudcontentsmak.com
14	disorderstatus.ru

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 ATTT khuyến nghị:

- Theo dõi và cập nhật bản vá cho các lỗ hổng, đặc biệt là lỗ hổng nêu tại *mục 2* báo cáo này.

- Đối với nguy cơ bị lợi dụng để thực hiện tấn công từ chối dịch vụ nêu tại *mục 3*: Kiểm tra các dịch vụ sử dụng giao thức UDP, hạn chế tối đa việc mở các cổng dịch vụ sử dụng giao thức UDP. Trong trường hợp sử dụng phải thường xuyên theo dõi và cập nhật bản vá lỗ hổng bảo mật cho dịch vụ, đồng thời cấu hình cứng hóa dịch vụ, hạn chế tối đa truy cập đến và đi liên quan đến địa chỉ/dải địa chỉ ko cần thiết.

- 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 4*, các cơ quan tổ chức cần phải thường xuyên kiểm tra, rà soát máy chủ web để kịp thời phát hiện và cập nhật.

- 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 ATTT đã chia sẻ, đặc biệt là các tên miền đã nêu trong *mục 5.2* báo cáo này.

- Chủ động kiểm tra, rà soát, bóc gỡ mã độc ra khỏi hệ thống mạng. Cục ATTT 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 ATTT theo thông tin bên dưới để phối hợp thực hiện.

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./.

CỤC AN TOÀN THÔNG TIN