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 26 (từ 24/6 - 30/6/2019)

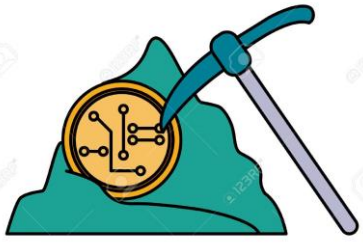
Số: /BC-CATTT *Hà Nội, ngày 02 tháng 7 năm 2019*

HÀN QUỐC SỬA ĐỔI LUẬT THU THẬP DỮ LIỆU TRẺ EM

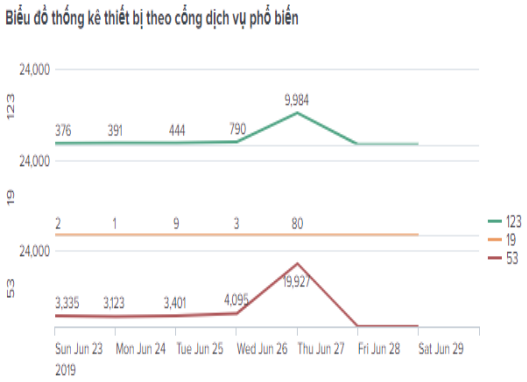
Hàn Quốc sửa đổi luật liên quan tới việc thu thập dữ liệu trẻ em, theo đó cơ quan chức năng yêu cầu các doanh nghiệp phải có được sự đồng ý rõ ràng từ cha mẹ hoặc người giám hộ hợp pháp của trẻ em dưới 14 tuổi khi tiến hành thu thập dữ liệu của nhóm đối tượng này.

PHÁT HIỆN CHIẾN DỊCH TẤN CÔNG KHAI THÁC TIỀN ĐIỆN TỬ

Hãng Trend Micro đã phát hiện một chiến dịch tấn công sử dụng phần mềm độc hại khai thác tiền điện tử mới xuất hiện thông qua cổng dịch vụ của phần mềm ADB (Android Debug Bridge), mã độc này có thể lây lan qua giao thức SSH.



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 302 lỗ hổng, trong đó có 15 lỗ hổng mức cao, 84 lỗ hổng mức trung bình, 18 lỗ hổng mức thấp và 141 lỗ hổng chưa đánh giá; 01 lỗ hổng đã có mã khai thác

VI PHẠM THÔNG TIN CÁ NHÂN

Liên minh tín dụng Desjardins lộ lọt thông tin của khoảng 2.9 triệu khách hàng. Desjardins là liên minh tín dụng lớn nhất Canada và lớn thứ năm trên thế giới. Có trụ sở tại tỉnh Quebec Desjardins đang quản lý số tài sản trị giá 304 tỷ CAD (230 tỷ USD)

1. Điểm tin đáng chú ý

1.1. Hàn Quốc sửa đổi luật liên quan tới việc thu thập dữ liệu trẻ em, theo đó cơ quan chức năng yêu cầu các doanh nghiệp phải có được sự đồng ý rõ ràng từ cha mẹ hoặc người giám hộ hợp pháp của trẻ em dưới 14 tuổi khi tiến hành thu thập dữ liệu của nhóm đối tượng này. Theo Ủy ban Truyền thông Hàn Quốc (KCC) luật sửa đổi sẽ có hiệu lực vào năm 2020.

Trước đây tại Hàn Quốc cũng đã có quy định trẻ em dưới 14 tuổi phải có sự đồng ý của cha mẹ hoặc người giám hộ hợp pháp trước khi chuyển dữ liệu cá nhân cho doanh nghiệp nhưng không giải thích rõ ràng cách thức thực hiện, gây khó khăn cho việc thực thi. Luật mới yêu cầu doanh nghiệp khi thu thập dữ liệu cá nhân của trẻ em thì phải có sự đồng ý của cha mẹ/người giám hộ thông qua văn bản hoặc xác thực qua điện thoại thông minh.

Các doanh nghiệp không nhận được sự đồng ý của cha mẹ/người giám hộ trước khi thu thập dữ liệu từ trẻ em sẽ chịu mức phạt lên tới 3% doanh thu, kèm theo các hình phạt hành chính khác. KCC cho biết luật mới sẽ tạo môi trường cho trẻ em có thể sử dụng các dịch vụ truyền thông trực tuyến mà vẫn bảo đảm quyền riêng tư và dữ liệu.

1.2. Liên minh tín dụng Desjardins bị lộ lọt thông tin của khoảng 2.9 triệu khách hàng. Desjardins là liên minh tín dụng lớn nhất Canada và lớn thứ năm trên thế giới, có trụ sở tại tỉnh Quebec. Desjardins đang quản lý số tài sản trị giá 304 tỷ CAD (230 tỷ USD). Vụ việc liên quan tới việc một nhân viên của Desjardins đã đánh cắp lượng dữ liệu này và tiết lộ ra bên ngoài mà không được phép.

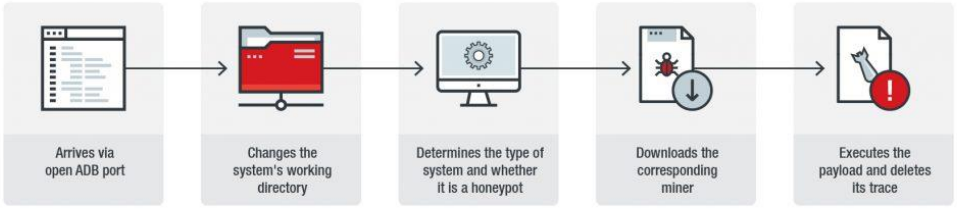
Nhân viên này đã cung cấp ra bên ngoài thông tin cá nhân của gần 2.7 triệu người dùng bao gồm họ tên đầy đủ, ngày sinh, địa chỉ, số điện thoại, địa chỉ email, số bảo hiểm xã hội và chi tiết về thói quen sự dụng ngân hàng và các sản phẩm của Desjardins. Bên cạnh đó, thông tin của gần 173.000 khách hàng doanh nghiệp cũng đã bị lộ lọt. Trong trường hợp khách hàng doanh nghiệp, dữ liệu bị lộ lọt bao gồm tên doanh nghiệp, địa chỉ doanh nghiệp, số điện thoại doanh nghiệp, tên chủ sở hữu và tên người dùng trên tài khoản "AccèsD Affaires". Theo thông tin ban đầu, thì không có mật khẩu ngân hàng điện tử, câu hỏi bảo mật, mã PIN tài khoản và số thẻ tín dụng và thẻ ghi nợ bị tiết lộ.

Ngay sau khi phát hiện ra vụ việc, Desjardins đã thông báo cho Văn phòng Ủy viên quyền riêng tư Canada, Ủy ban truy cập thông tin ở Quebec (d'accès à l'information du Québec) và Cơ quan quản lý thị trường (Autorité des marchés) về vụ việc; sa thải nhân viên cố ý gây ra vụ việc; thực hiện các biện pháp giám sát và

bảo đảm an toàn bổ sung để bảo vệ thông tin cá nhân và thông tin tài chính của khách hàng.

1.3. Hãng Trend Micro đã phát hiện một chiến dịch tấn công sử dụng phần mềm độc hại khai thác tiền điện tử mới xuất hiện thông qua cổng dịch vụ của phần mềm ADB (Android Debug Bridge), mã độc này có thể lây lan qua giao thức SSH. Chiến dịch này lợi dụng các máy chủ bị nhiễm sang bất kỳ cổng ADB mở không có xác thực theo mặc định. Mã độc được thiết kế cho phép lây lan vào hệ thống có kết nối SSH với máy chủ đã bị lây nhiễm.

Việc sử dụng ADB làm cho các thiết bị trên nền tảng Android dễ bị lây nhiễm mã độc. Hãng đã phát hiện hoạt động từ phần mềm độc hại này ở 21 quốc gia khác nhau và được phát hiện nhiều nhất ở Hàn Quốc.



Hình 1. Cách thức tấn công của mã độc.

Để tối ưu hóa hoạt động khai thác, mã độc này còn bật tính năng HugePages (cho phép tăng bộ nhớ của thiết bị) được tích hợp trong nhân Linux 2.6.

Mã độc này cũng cố gắng sửa đổi file "*/etc/hosts"*, bằng cách thêm bản ghi "0.0.0.0 miningv2.duckdns.org" để vô hiệu hóa địa chỉ này (địa chỉ này cũng có thể đang được một nhóm tấn công khác sử dụng để khai thác tiền điện tử). Đồng thời nó cũng hủy tiến trình của nhóm tấn công khác bằng lệnh "pkill -9 r32".

Cuối cùng, nó sử dụng một kỹ thuật ẩn danh bằng cách xóa các tệp đã tải xuống. Sau khi lây lan sang các thiết bị khác được kết nối với hệ thống, nó sẽ xóa toàn bộ dấu vết trên máy chủ.

Điểm đặc biệt của chiến dịch tấn công này là cơ chế lây lan qua SSH. Bất kỳ thiết bị nào đã từng kết nối qua SSH với máy bị lây nhiễm đều có khả năng đã xác thực, nên mã độc có thể lợi dụng để lây nhiễm vào thiết bị trong lần kết nối tiếp theo. Cổng dịch vụ ADB là một tính năng hữu ích cho quản trị viên và nhà phát triển, nhưng một khi cổng ADB được kích hoạt có thể khiến thiết bị và những thiết bị được kết nối với nó bị đe dọa. Cục An toàn thông tin khuyến nghị người dùng có thể thực hiện một số biện pháp để hạn chế này: Kiểm tra và thay đổi cài đặt mặc định; cập nhập các bản vá mới; tải và cài đặt ứng dụng từ nguồn đáng tin cậy.

Tham khảo thông tin kỹ thuật chi tiết tại:

https://ti.khonggianmang.vn/dashboard/news/p/ma-doc-lay-lan-android-ssh/

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 302 lỗ hổng, trong đó có 15 lỗ hổng mức cao, 84 lỗ hổng mức trung bình, 18 lỗ hổng mức thấp và 141 lỗ hổng chưa đánh giá; 01 lỗ hổng đã có mã khai thác.

Hệ thống kỹ thuật của Cục ATTT 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: Nhóm 04 lỗ hổng trong một số sản phẩm của Cisco; Nhóm 37 lỗ hổng trên phần mềm IBM; Nhóm 07 lỗ hổng trên LiveZilla 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	Cisco	CVE-2019-1619 CVE-2019-1620 CVE-2019-1621 CVE-2019-1622 …	Nhóm 04 lỗ hổng dựa trên một số sản phẩm của Cisco (Trung tâm dữ liệu Cisco DCNM) cho phép kẻ tấn công truy cập từ xa, chiếm quyền điều khiển, thực thi mã độc, tấn công cục bộ, xác thực các lệnh tùy ý.	Đã có thông tin xác nhận và bản vá
2	IBM	CVE-2018-1858 CVE-2018-2011 CVE-2018-2013 CVE-2019-4382 …	Nhóm 37 lỗ hổng dựa trên một số sản phẩm của IBM (API Connect, PureApplication, Security Access Manager) cho phép kẻ tấn công giả mạo yêu cầu thực hiện các hành động độc hại, thực hiện các câu lệnh SQL để xóa và sửa đổi thông tin trong cơ sở dữ liệu, thực hiện giải mã thông tin có độ nhạy cảm cao.	Đã có thông tin xác nhận và bản vá
3	LiveZilla	CVE-2019-12961 CVE-2019-12961 CVE-2019-12939 CVE-2019-12964 …	Nhóm 07 lỗ hổng trên máy chủ LiveZilla các phiên bản trước 8.0.1.1 dễ bị tấn công DoS, lỗ hổng trong SQL Injection và dễ bị XSS trong mobile.	Đã có thông tin xác nhận và bản vá

4	Google	CVE-2017-5028 CVE-2018-16064 CVE-2018-16069 CVE-2018-17460 …	Nhóm 73 lỗ hổng trên sản phẩm của Google (Chrome) cho phép kẻ tấn công từ xa rò rỉ dữ liệu thông qua trang HTML.	Đã có thông tin xác nhận và bản vá
5	Mcafee	CVE-2019-3632 CVE-2019-3628 CVE-2019-3629 CVE-2019-3629 …	Nhóm 05 lỗ hổng trên một số sản phẩm của Mcafee (Security Manager (EMS)) cho phép người dùng xác thực quyền nâng cao, truy cập vào một thành phần hệ thống lỗi, thực thi mã tùy ý.	Đã có thông tin xác nhận và bản vá

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

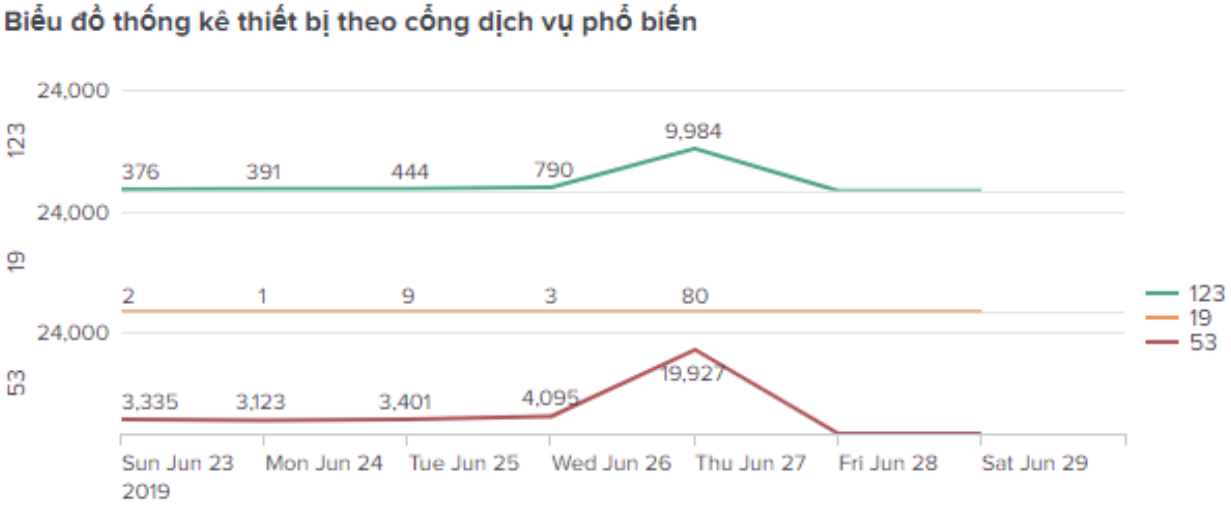
Tấn công từ chối dịch vụ là hình thức tấn công đã có từ lâu, và hiện tại vẫn được đối tượng tấn công ưa thích sử dụng để thực hiện các ý đồ xấu. Tấn công từ chối dịch vụ về cơ bản không nguy hiểm nhưng lại gây ảnh hưởng đến hoạt động của hệ thống, gây thiệt hại về kinh tế cho tổ chức bị tấn công.

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

Giao thức	Số lần khuếch đại băng thông
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 **45.961** 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.

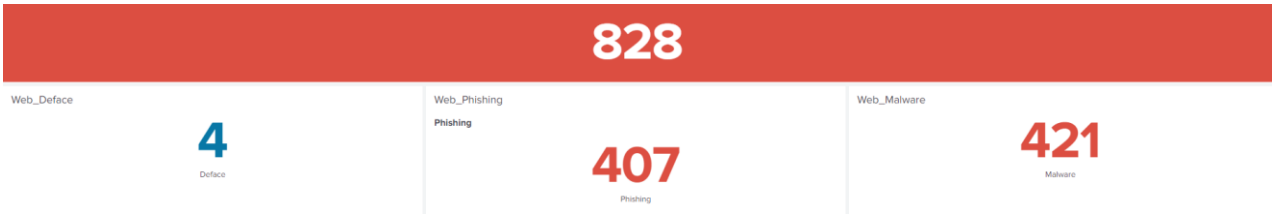


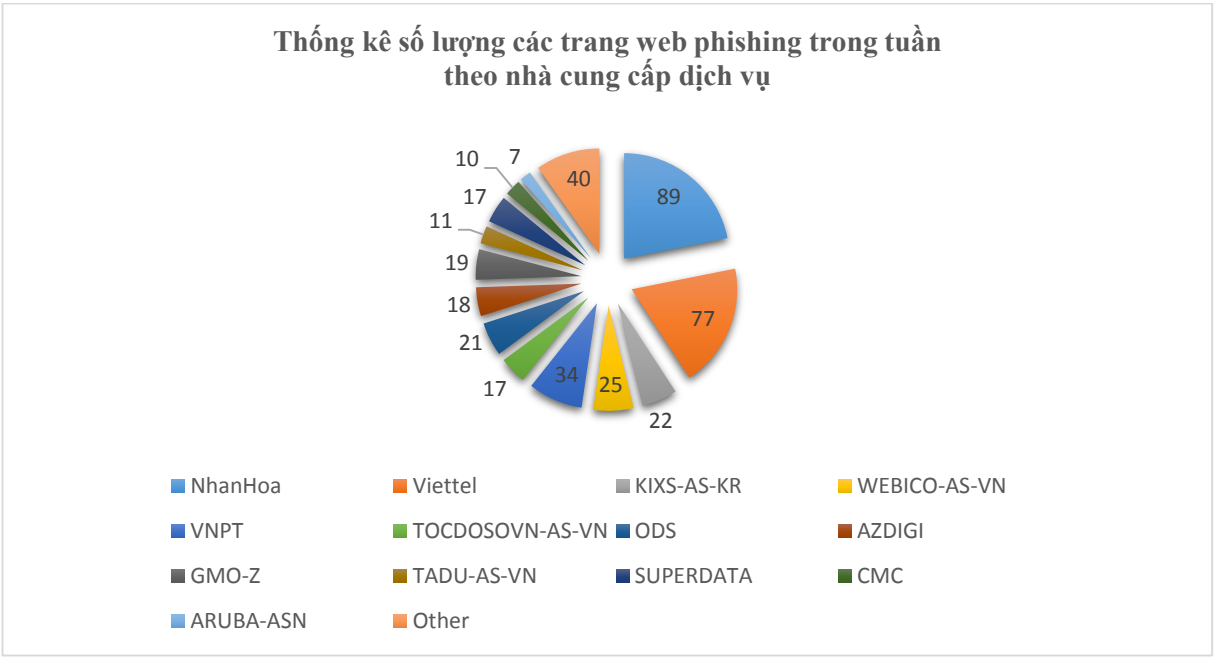
4. Tấn công vào Cổng TTĐT/ứng dụng web của Việt Nam

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 828 trường hợp tấn công vào trang/cổng thông tin điện tử của Việt Nam: 04 trường hợp tấn công thay đổi giao diện, 407 trường hợp tấn công lừa đảo (Phishing), 421 trường hợp tấn công cài cắm mã độc.

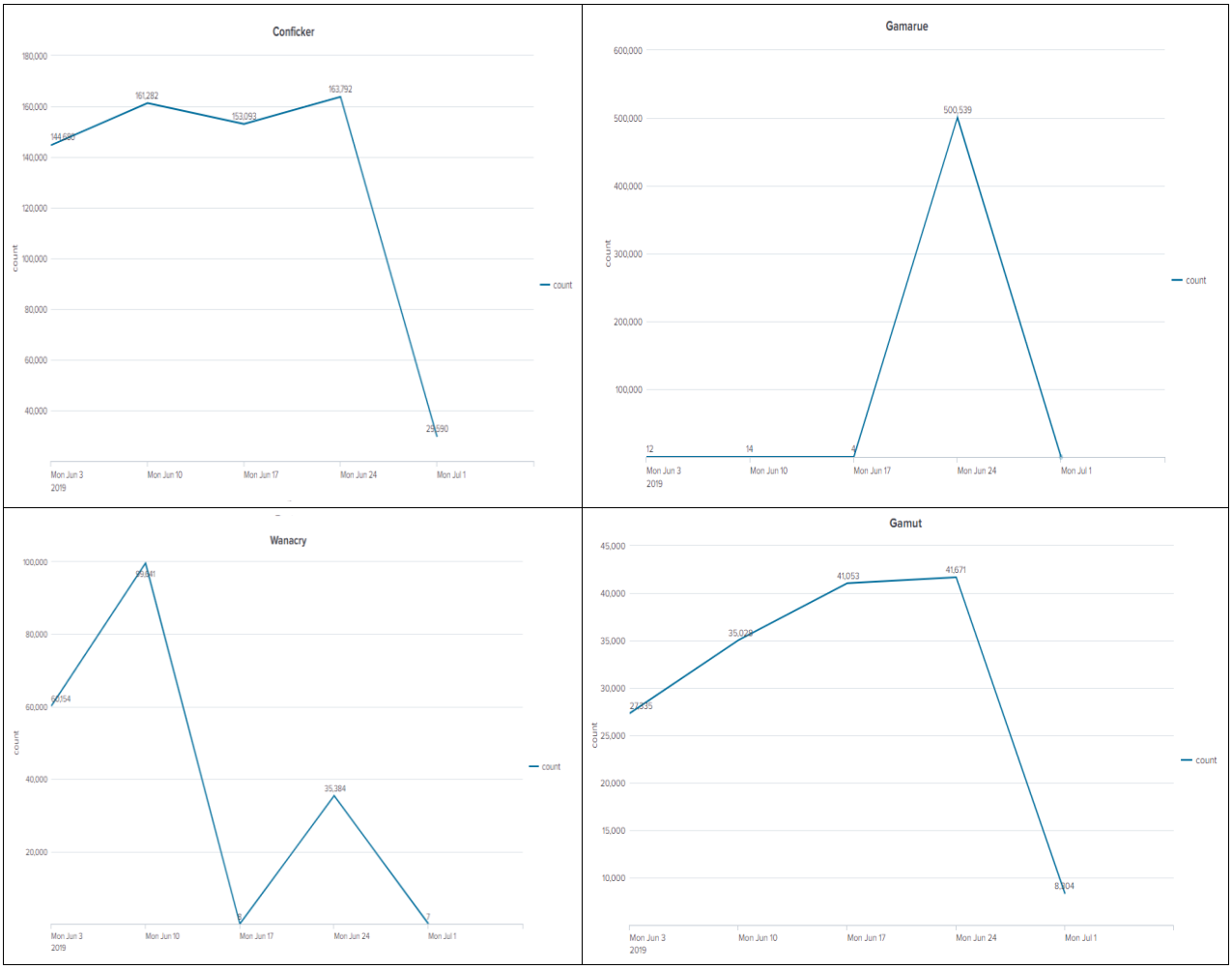




5. Hoạt động của mạng botnet, APT, mã độc tại Việt Nam

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 **Gamarue** (chuyên đánh cắp thông tin người dùng) hoạt động mạnh nhất, có 500.539 lượt địa chỉ IP kết nối với máy chủ điều khiển.

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	www.iuqerfsodp9ifjaposdfjhgosurijfaewrwergwea.com
5	soplifan.ru
6	4m9k7jh1.ru
7	xjpakmdcfuqe.com
8	somicrososoft.ru
9	www.cityofangelsmagazine.com
10	kodklq.info
11	ivz7x63ymy.ru
12	morphed.ru
13	kukutrustnet777.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 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