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 34 (từ 19/08 - 25/08/2019)

Số: /BC-CATTT *Hà Nội, ngày 26 tháng 08 năm 2019*

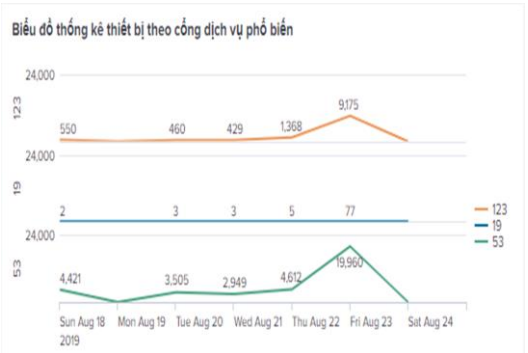
YOUTUBE THÊM TÍNH NĂNG MỚI BÁO CÁO CÁC VIDEO LIÊN QUAN ĐẾN ĐỐI TƯỢNG TRẺ EM

Mới đây, Youtube thông báo sẽ thêm tính năng "báo cáo" vi phạm các video quảng cáo đối tượng trẻ em. Theo một báo cáo mới từ Bloomberg, Youtube đang hoàn thiện các kế hoạch triển khai của mình.

TIN TẶC CỐ GẮNG ĐÁNH CẮP MẬT KHẨU TỪ MẠNG RIÊNG VPN

Hiện nay tin tặc đang tích cực thực hiện nhiều cuộc tấn công nhằm khai thác các máy chủ VPN chưa cập nhật bản vá lỗi mới đây trên 2 dòng sản phẩm nổi tiếng của hãng Fortinet (Fortigate) và Pulse Secure. Mối nguy hại này tồn tại trên 500.000 máy chủ với khoảng 480.000 máy chủ của Fortinet và 50.000 máy chủ của Pulse Secure

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 587 lỗ hổng, trong đó có 49 lỗ hổng mức cao, 170 lỗ hổng mức trung bình, 8 lỗ hổng mức thấp và 360 lỗ hổng chưa đánh giá. Trong đó có ít nhất 64 lỗ hổng cho phép chèn và thực thi mã lệnh.

CÁC CHÍNH CƠ QUAN CHÍNH PHỦ CỦA 23 THÀNH PHỐ THUỘC BANG TEXAS ĐÃ BỊ TIN TẶC TẤN CÔNG

Ngày 20/8/2019, các báo đồng loạt đưa tin về việc nhiều cơ quan chính phủ của 23 thành phố thuộc Bang Texas đã bị tin tặc kiểm soát hệ thống máy tính bằng mã độc mã hóa dữ liệu đòi tiền chuộc (Ransomware). Số tiền kẻ tấn công yêu cầu thanh toán hiện tại đang là 2.5 triệu đô la.

1. Điểm tin đáng chú ý

1.1. Mới đây, Youtube thông báo sẽ thêm tính năng "báo cáo" vi phạm các video quảng cáo đối tượng trẻ em. Theo một báo cáo mới từ Bloomberg, Youtube đang hoàn thiện các kế hoạch triển khai của mình. Động thái này có thể nhằm xoa dịu các cơ quan quản lý tại Ủy ban Thương mại Liên bang, vì các cơ quan này có kế hoạch sẽ tiến hành kiểm tra xem YouTube có vi phạm Đạo luật bảo vệ quyền riêng tư trực tuyến của trẻ em (COPPA) thông qua việc thu thập dữ liệu và không bảo vệ người dùng trẻ trên nền tảng này hay không.

Trước đó, Google (cũng chính là công ty sở hữu nền tảng Youtube), đã ngừng chia sẻ dữ liệu của người dùng trên hệ điều hành Android với các nhà mạng không dây trên toàn cầu vì lo ngại về quyền riêng tư. Theo báo cáo của Reuters, dịch vụ thông tin mạng di động (Mobile Network Insights) do Google ra mắt năm 2017 nhằm giúp các nhà mạng lên kế hoạch hoặc nâng cấp mạng không dây bằng cách hiển thị cho họ cường độ tín hiệu và tốc độ kết nối trong vùng phủ sóng của họ. Tuy nhiên, công ty hiện đã quyết định chấm dứt việc cung cấp dịch vụ miễn phí này, theo báo cáo do lo ngại rằng nó có thể thu hút sự giám sát của người dùng và cơ quan quản lý.

1.2. Ngày 20/8/2019, các báo đồng loạt đưa tin về việc nhiều cơ quan chính phủ của 23 thành phố thuộc Bang Texas đã bị tin tặc kiểm soát hệ thống máy tính bằng mã độc mã hóa dữ liệu đòi tiền chuộc (Ransomware). Số tiền kẻ tấn công yêu cầu thanh toán hiện tại đang là 2.5 triệu đô la.

Các sự cố về ransomware liên tục xảy ra cho thấy các thành phố của Hoa Kỳ cũng chưa được trang bị đầy đủ các biện pháp bảo đảm an toàn thông tin để tự vệ trong môi trường mạng. Một nghiên cứu tháng 5/2019 đã tìm thấy hơn 169 trường hợp nhiễm ransomware lây nhiễm trong các hệ thống của chính quyền tiểu bang và địa phương. Chính quyền địa phương và Viện công nghệ khuyến khích các cơ quan, tổ chức nên có bản sao lưu dữ liệu của các hệ thống quan trọng, đào tạo nhân viên về các vấn đề an toàn thông tin mạng và đảm bảo họ có kế hoạch ứng phó sự cố mạng. Đối với những địa phương không hoàn thành nhiệm vụ cải thiện năng lực của mình, đề nghị các quan chức thành phố xem xét việc thuê ngoài một số hoặc tất cả các bộ phận công nghệ thông tin của họ.

1.3. Hiện nay các tin tặc đang tích cực thực hiện nhiều cuộc tấn công nhằm khai thác các máy chủ VPN chưa cập nhật các bản vá lỗi mới đây của 2 dòng sản phẩm nổi tiếng của hãng Fortinet (Fortigate) và Pulse Secure. Mối nguy hại này dự

kiến tồn tại trên 500.000 máy chủ với khoảng 480.000 máy chủ của Fortinet và 50.000 máy chủ của Pulse Secure.

Chi tiết về lỗ hổng được tiết lộ lần đầu tiên vào tháng 7 bởi Orange Tsai và Meh Chang của nhóm nghiên cứu tại Công ty tư vấn bảo mật DEVCORE, lỗ hổng giúp cho những kẻ tấn công có thể thực thi mã độc từ xa và thay đổi mật khẩu. Tại hội nghị bảo mật Black Hat ở Las Vegas, một số bằng chứng khai thác lỗ hổng này đã được các chuyên gia công khai sau khi trình bày.

Các lỗ hổng bảo là CVE-2018-13379 (lỗ hổng trong FortiOS SSL VPN) và CVE-2019-11510 (lỗ hổng trong Pulse Connect Secure).

Cũng theo Beaumont, CVE-2018-13379 rất dễ khai thác và cho phép kẻ tấn công có được thông tin đăng nhập của quản trị viên ở dạng cleartext. Chuyên gia này cho biết có gần nửa triệu địa chỉ IP được liên kết với các thiết bị Fortinet có thể nhìn thấy trực tuyến.

Hiện tại, theo Bad Packets thống kê có 2.658 điểm cuối Pulse Secure VPN dễ bị khai thác. Các kết quả dò quét cho thấy những điểm cuối dễ bị tấn công thuộc về nhiều tổ chức nhạy cảm bao gồm:

- Quân đội Hoa Kỳ và nhiều cơ quan chính quyền Liên bang, địa phương.

- Các trường Đại học công lập.

- Bệnh viện và nhà cung cấp chăm sóc sức khỏe.

- Các tổ chức tài chính lớn.

- Khoảng 500 công ty khác.

Theo nhà nghiên cứu độc lập Kevin Beaumont cho biết, đã tìm thấy những cuộc tấn công chống lại các máy chủ Fortigate đến từ địa chỉ IP 91.121.209.213 và .52.56.148.178 cũng đang khai thác cùng một lỗ hổng CVE-2018-13379.

Hình 1. Các địa chỉ IP tấn công vào máy chủ VPN của hãng Fortinet

Trong khi đó, Beaumont cho biết, những cuộc tấn công cố gắng khai thác các máy chủ Pulse Secure chưa được vá lỗi đến từ địa chỉ IP 2.137.127.2 và 81.40.150.167 cố gắng khai thác hoặc kiểm tra lỗ hổng CVE-2019-11510.

Source IP	Country	User Agent	Method	URI	POST_Data	Target Port	Tag	FirstSeen	LastSeen	Event Count
81.40.150.167	Spain	-	GET	/dana-na/../dana/html5acc/guacamole/../../../../../../etc/passwd?/dana/html5acc/guacamole/	"-"	443	Pulse Secure PCS Arbitrary File Reading Vulnerability | VPN | CVE-2019-11510	2019-08-23T12:01:40Z	2019-08-23T18:54:08Z	48
2.137.127.2	Spain	-	GET	/dana-na/../dana/html5acc/guacamole/../../../../../../etc/passwd?/dana/html5acc/guacamole/	"-"	443	Pulse Secure PCS Arbitrary File Reading Vulnerability | VPN | CVE-2019-11510	2019-08-22T22:52:35Z	2019-08-22T22:52:35Z	82

Hình 2. Các địa chỉ IP tấn công vào máy chủ Pulse Secure

Những lỗ hổng này rất nghiêm trọng vì chúng ảnh hưởng đến một phần mềm được truy cập Internet và hoạt động như một cổng vào các hệ thống rất quan trọng, nhạy cảm của tổ chức. Những kẻ tấn công sau khi khai thác lỗ hổng sẽ có được hàm băm và trong một số trường hợp có mật khẩu dạng rõ, mã hóa dữ liệu và có thể cho phép mọi người xâm nhập vào các mạng đó.

Khuyến nghị, các cơ quan tổ chức có máy chủ VPN trên 2 nền tảng này cập nhật toàn bộ bản vá mới nhất mà Fortinet và Pulse Secure đã phát hành. Tiến hành rà quét những địa IP và máy chủ đang nằm trong danh sách dễ bị khai thác để có chính sách ngăn chặn sớm nhất.

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

https://ti.khonggianmang.vn/dashboard/news/p/Tin-tac-dang-co-gang-danh-cap-mat-khau-tu-mang-rieng-VPN/

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 587 lỗ hổng, trong đó có 49 lỗ hổng mức cao, 170 lỗ hổng mức trung bình, 8 lỗ hổng mức thấp và 360 lỗ hổng chưa đánh giá. Trong đó có ít nhất 64 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 07 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 79 lỗ hổng trên sản phẩm của Adobe; Nhóm 16 lỗ hổng trên Google Android; Nhóm 31 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-2019-7965 CVE-2019-8003 CVE-2019-8009 ….	Nhóm 79 lỗ hổng trên một số phiên bản của Adobe Acrobat and Reader, Creative Cloud Desktop Application cho phép đối tượng tấn công thực thi mã lệnh tùy ý	Đã có thông tin xác nhận và bản vá
2	Google Android	CVE-2019-2126 CVE-2019-2127 CVE-2019-2128 ...	Nhóm 16 lỗ hổng trên hệ điều hành Android cho phép đối tượng tấn công chèn và thực thi mã lệnh Một số lỗ hổng có điểm CVSS 9.3 Ảnh hưởng tới các phiên bản: Android-7.0, 7.1.1, 7.1.2, 8.0 8.1, 9.	Đã có thông tin xác nhận và bản vá
3	IBM	CVE-2019-4294 CVE-2019-4481 CVE-2019-4483	Nhóm 31 lỗ hổng trên một số sản phẩm của IMB (API Connect, Intelligent Operations Cente DataPower Gateway, Contract Management, Informix Dynamic Server Enterprise Edition…) cho phép đối tượng tấn công thu thập thông tin, khai thác lỗi SQL Injection để tương tác trái phép với cơ sở dữ liệu back-end, lỗi XSS, Path Traversal, tấn công leo thang. Một số lỗ hổng cho phép chèn và thực thi mã lệnh.	Đã có thông tin xác nhận và bản vá
4	Atlassian Jira	CVE-2019-11585 CVE-2019-11588 CVE-2019-11586	Nhóm 10 lỗ hổng trên Jira cho phép đối tượng tấn công khai thác lỗi XSS, CSRF, thu thập thông tin tài khoản người dùng,	Đã có thông tin xác nhận bản vá.

			chuyển hướng người dùng đến trang web độc hại.	
5	Cisco	CVE-2019-1883 CVE-2019-1907 CVE-2019-1900 ...	Nhóm 27 lỗ hổng trên một số sản phẩm của Cisco (NFVIS, Firepower Threat Defense, HyperFlex Software,Integrated Management Controller...) cho phép đối tượng tấn công thu thập thông tin, tấn công nghe lén, chèn và thực thi mã lệnh, tấn công leo thang.	Đã có thông tin xác nhận và bản vá
6	Dlink	CVE-2019-15526 CVE-2019-15527 CVE-2019-15528 ...	Nhóm 05 lỗ hổng trên một số firmware sản phẩm của D-Link DIR-823G cho phép đối tượng tấn công chèn và thực thi mã lệnh để kiểm soát thiết bị.	Đã có thông tin xác nhận và bản vá
7	Lenovo	CVE-2019-6178 CVE-2019-6159 CVE-2019-6177 ...	Nhóm 05 lỗ hổng trên một số sản phẩm, ứng dụng của Lenovo (Lenovo Solution Center, ThinkPad) cho phép đối tượng tấn công thu thập thông tin, khai thác lỗi XSS, tấn công leo thang.	Đã có thông tin xác nhận và bản vá

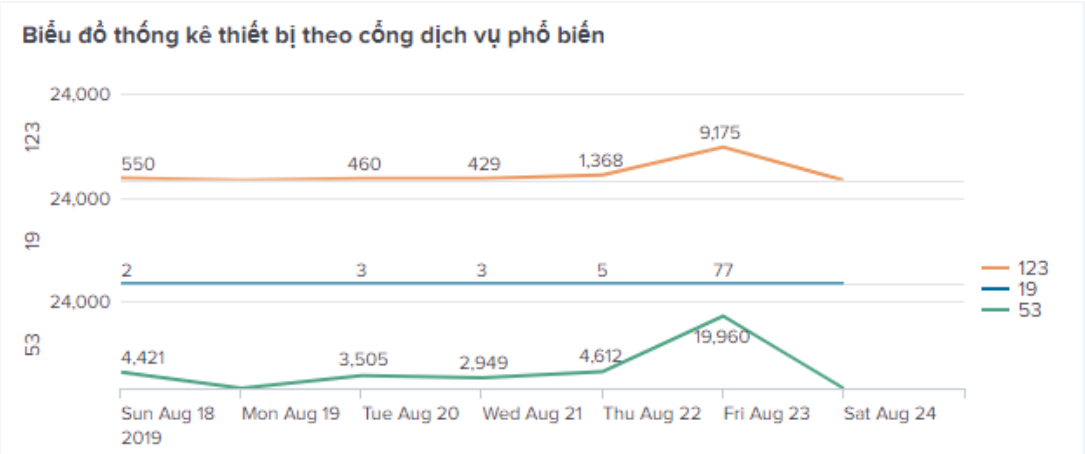
3. Nguy cơ phát tán tấn công từ chối dịch vụ

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

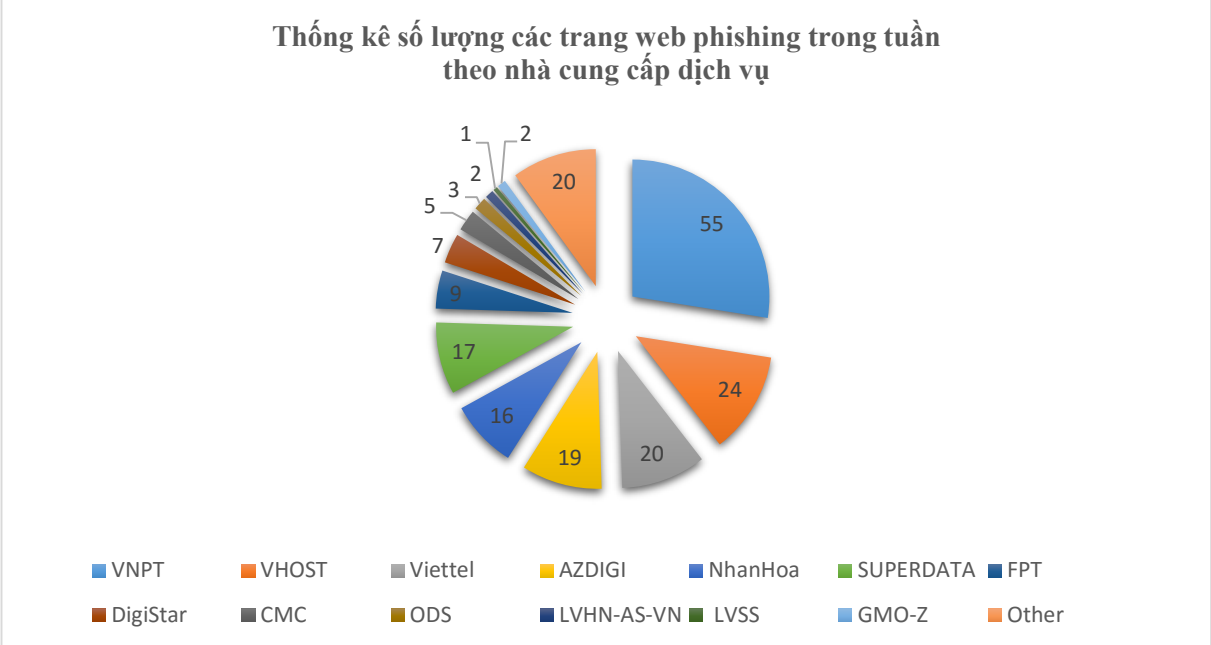
Tại Việt Nam, có rất nhiều máy chủ, thiết bị có thể trở thành nguồn phát tán tấn công DRDoS. Trong tuần có **47,519 (tăng so với tuần trước là 47,494)** thiết bị có khả năng bị huy động và trở thành nguồn tấn công DRDoS. Các thiết bị này đang mở sử dụng các dịch vụ NTP (123), DNS (53), Chargen (19). 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 313 trường hợp tấn công vào trang/cổng thông tin điện tử của Việt Nam: 11 trường hợp tấn công thay đổi giao diện, 200 trường hợp tấn công lừa đảo (Phishing), 106 trường hợp tấn công cài cắm mã độc.

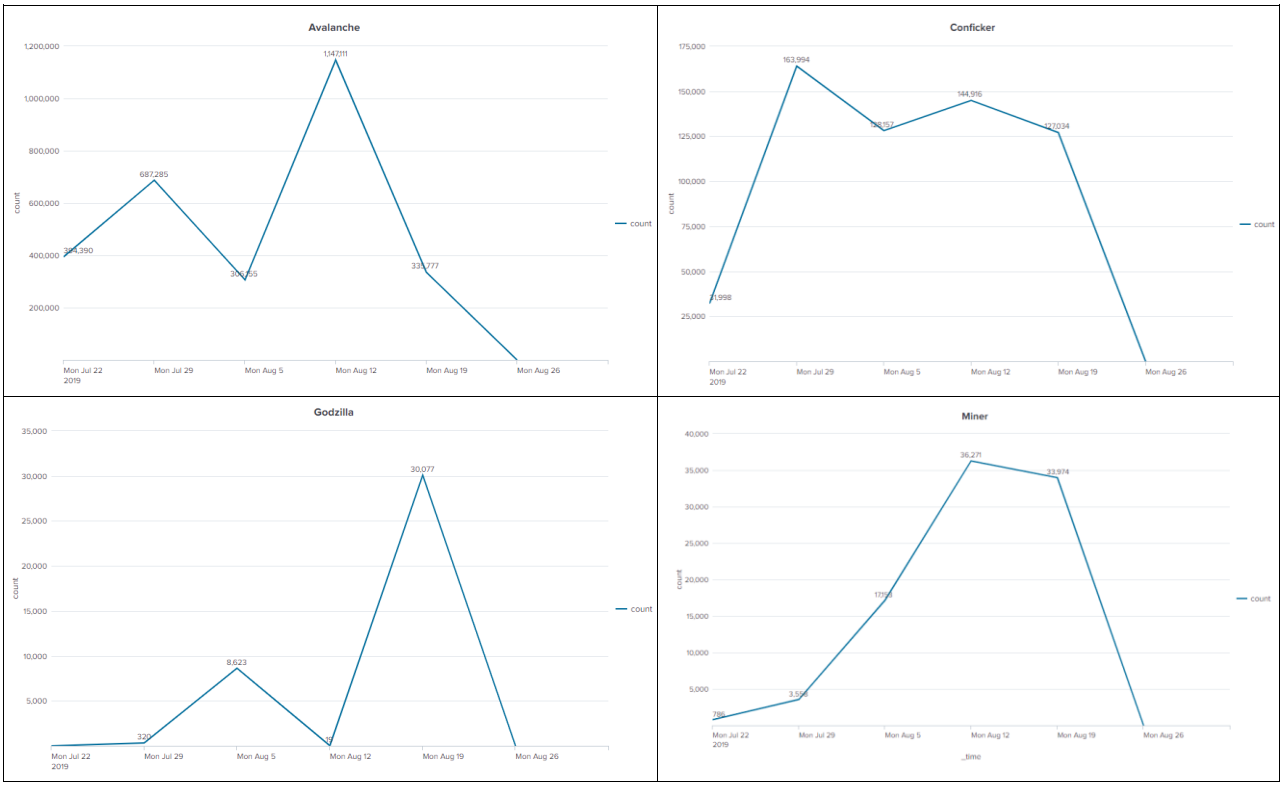


5. Hoạt động của mạng botnet, APT, mã độc tại Việt Nam

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 mạnh so với tuần trước, có 335.777 lượt địa chỉ IP kết nối với máy chủ điều khiển (Tuần 33 là 1.147.111).

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	soplifan.ru
5	xdqzpbcgrvkj.ru
6	xjpakmdcfuqe.com
7	kn0ugjov.ru
8	ixhtiv.info
9	www.cityofangelsmagazine.com
10	somicrososoft.ru
11	morphed.ru
12	urusurofhsorhfuuhl.cc
13	www.corpnox-technologie.fr
14	75ulqnwb.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