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 33 (từ 13/08 - 19/08/2019)

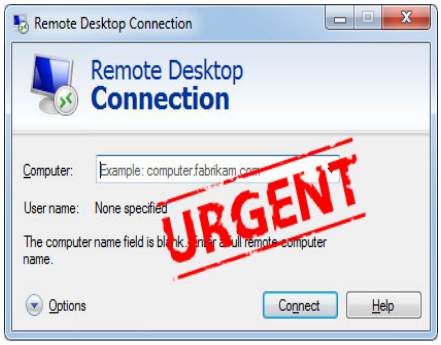
Số: /BC-CATTT *Hà Nội, ngày 20 tháng 08 năm 2019*

CÔNG TY HONDA BỊ LỘ LỌT CƠ SỞ DỮ LIỆU CHỨA THÔNG TIN CÁC NHÂN

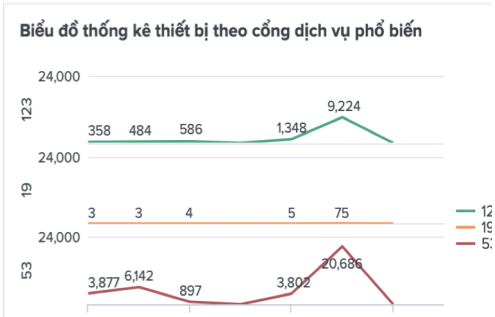
Gần đây, một cơ sở dữ liệu bị lộ, lọt trên mạng có chứa thông tin của khoảng 300.000 cá nhân, bao gồm tên, địa chỉ thư điện tử, thông tin đăng nhập của họ trên máy tính, thông tin mạng của nhà cung cấp bảo mật điểm cuối của máy tính. Cơ sở dữ liệu chứa thông tin tin bị lộ, lọt này được cho là xuất phát từ các máy tính sử dụng trong nội bộ hãng Honda.

LỖ HỔNG NGHIÊM TRỌNG MỚI TRONG DỊCH VỤ REMOTE DESTOP

Ngày 13/8 Microsoft (MRSC- Trung tâm phản ứng bảo mật của Microsoft) đã cảnh báo và khuyến nghị người dùng vá lỗ hổng nghiêm trọng trong dịch vụ Remote Desktop có khả năng bị mã độc khai thác và lây lan tự động thông qua..



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 447 lỗ hổng, trong đó có 16 lỗ hổng mức cao, 80 lỗ hổng mức trung bình, 13 lỗ hổng mức thấp và 338 lỗ hổng chưa đánh giá. Trong đó có ít nhất 48 lỗ hổng cho phép chèn và thực thi mã

CƠ QUAN KHÔNG GIAN MẠNG CỦA TRUNG QUỐC TĂNG CƯỜNG RÀ QUÉT VÀ XỬ LÝ TRÊN KHÔNG GIAN MẠNG

Theo thời báo Hoàn cầu, Cơ quan giám sát không gian mạng của Trung Quốc (The Cyberspace Administration of China - CAC) đã xử lý gần 3.000 trang web trong Quý II/2019 do cung cấp dịch vụ tin tức bất hợp pháp hoặc phát tán thông tin vi phạm pháp luật.

1. Điểm tin đáng chú ý

1.1. Gần đây, một cơ sở dữ liệu bị lộ, lọt trên mạng có chứa thông tin của khoảng 300.000 cá nhân, bao gồm tên, địa chỉ thư điện tử, thông tin đăng nhập của họ trên máy tính, thông tin mạng của nhà cung cấp bảo mật điểm cuối của máy tính. Cơ sở dữ liệu chứa thông tin tin bị lộ, lọt này được cho là xuất phát từ các máy tính sử dụng trong nội bộ hãng Honda (một trong những nhà sản xuất động cơ lớn nhất thế giới của Nhật Bản).

Theo một chuyên gia nghiên cứu an toàn thông tin, cơ sở dữ liệu này còn chứa thông tin hệ thống như tên máy chủ, địa chỉ MAC, địa chỉ IP nội bộ, phiên bản hệ điều hành, trạng thái bản vá và thông tin của phần mềm bảo mật điểm cuối. Chuyên gia này còn cho biết cơ sở dữ liệu bị lộ, lọt còn chứa dữ liệu trên các máy tính được sử dụng bởi CFO, CSO, CEO. Những thông tin này có thể hỗ trợ cho đối tượng tấn công thực hiện tấn công, kiểm soát mạng lưới hệ thống của Honda một cách dễ dàng hơn. Honda cho biết đã tiến hành kiểm tra, rà soát nhật ký truy cập hệ thống và không nhận thấy có dấu hiệu nào của việc dữ liệu bị tải xuống bởi bên thứ ba. Tuy nhiên, Honda sẽ có những hành động phù hợp theo luật pháp, quy định có liên quan và tiếp tục thực hiện giải pháp bảo đảm an toàn thông tin chủ động để ngăn chặn các cuộc tấn công có thể xảy ra trong tương lai.

1.2. Theo thời báo Hoàn cầu, Cơ quan giám sát không gian mạng của Trung Quốc (The Cyberspace Administration of China - CAC) đã xử lý gần 3.000 trang web trong Quý II/2019 do cung cấp dịch vụ tin tức bất hợp pháp hoặc phát tán thông tin vi phạm pháp luật. CAC cũng đã cảnh báo tới chủ quản của 636 trang web và yêu cầu 56 trang web ngừng cập nhật thông tin. Hơn 200.000 tài khoản bất hợp pháp, một số trong đó có hành vi gian lận tài chính, cũng bị yêu cầu đóng tài khoản.

CAC vẫn đang tiếp tục tăng cường thực thi pháp luật để đảm bảo an toàn mạng và tiếp tục xử lý mạnh các hành vi vi phạm trên không gian mạng. Cơ quan này đã yêu cầu 26 nền tảng âm thanh trực tuyến, bao gồm ứng dụng hẹn hò Soul, đóng cửa hoặc khắc phục các dịch vụ của họ do truyền bá nội dung vi phạm. Một số trang web văn học trực tuyến, bao gồm Thành phố Văn học Tấn Giang, một trang web có ảnh hưởng ở Trung Quốc, đã được lệnh ngừng cập nhật và xóa nội dung vào tháng 7/2019.

1.3. Ngày 13/8 Microsoft (MRSC- Trung tâm phản ứng bảo mật của Microsoft) đã cảnh báo và khuyến nghị người dùng vá lỗ hổng nghiêm trọng trong dịch vụ Remote Desktop có khả năng bị mã độc khai thác và lây lan tự động thông qua.. Theo thống kê sơ bộ của Cục An toàn thông tin, hiện có hơn 22.000 máy tính ở Việt Nam đang mở cổng RDP - Remote Desktop Protocol (TCP 3389) trên Internet,

nếu các máy tính này chưa cập nhật bản vá thì sẽ trở thành mục tiêu khai thác đầu tiên và lây nhiễm sang các máy khác trong cùng vùng mạng.

Thông tin chi tiết về có trong văn bản cảnh báo số 751/CATTT-NCSC ngày 14/8/2019, đã được Cục ATTT gửi đến các đơn vị trong mạng lưới. Quý đơn vị có thể tra cứu lại tại địa chỉ:

https://ti.khonggianmang.vn/dashboard/news/p/canh-bao-rdp/

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 447 lỗ hổng, trong đó có 16 lỗ hổng mức cao, 80 lỗ hổng mức trung bình, 13 lỗ hổng mức thấp và 338 lỗ hổng chưa đánh giá. Trong đó có ít nhất 48 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 09 lỗ hổng trên các hệ điều hành, ứng dụng thực thi HTTP/2, Lỗ hổng trên thiết bị hỗ trợ kết nối Bluetooth, 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	Microsoft	CVE-2019-1151 CVE-2019-1144 CVE-2019-1181 ….	Nhóm 88 lỗ hổng trên sản phẩm, ứng dụng của Microsoft (Remote Desktop Service, Office, Windows 10, Azure Active Directory, Defender, DHCP Client, Microsoft Edge) cho phép đối tượng tấn công thu thập thông tin, chèn và thực thi mã lệnh, tấn công leo thang, Một số lỗ hổng nghiêm trọng (CVE-2019-1181, CVE-2019-1182) đã được Cục ATTT cảnh báo trong văn bản cảnh báo số	Đã có thông tin xác nhận và bản vá

			751/CATTT-NCSC	
2	Atlassian	CVE-2019-11581 CVE-2019-15053 CVE-2018-20826 CVE-2019-8448	Nhóm 05 lỗ hổng trong một số sản phẩm của Atlassian (Jira, Confluence Server, Jira Server and Data Center, …) cho phép đối tượng tấn công thiết lập Reporter, khai thác lỗi XSS, chèn và thực thi mã lệnh. Lỗ hổng CVE-2019-11581 đã được Cục ATTTT cảnh báo trực tiếp đến tổ chức đang public máy chủ Jira trên Internet trong văn bản số 705/CATTT-NCSC	Đã có thông tin xác nhận và bản vá
3	Wordpress	CVE-2019-14948 CVE-2017-18515 CVE-2016-10889	Nhóm 136 lỗ hổng trong nhiều plugin (newstatpress, wp-statistics, events-manager, FV Flowplayer Video Player, nextgen-gallery, 10Web Photo Gallery, subscriber, wp-google-map-plugin,...) của Wordpress cho phép đối tượng tấn công thự chiện khai thác lỗi SQL Injection,	Đã có thông tin xác nhận và bản vá
4	Huawei	CVE-2019-5223 CVE-2019-5299 CVE-2019-5280	Nhóm 03 lỗ hổng trên một số sản phẩm của Huawei (PCManager, Huawei CloudLink Phone, Huawei mobile phones Hima) cho phép đối tượng tấn công chèn và thực thi mã lệnh, tấn công nghe lén	Đã có thông tin xác nhận và bản vá
5	Adobe	CVE-2019-8062 CVE-2019-7870 CVE-2019-8063	Nhóm 09 lỗ hổng trên một số sản phẩm của Adobe (Adobe Experience Manager, Adobe Premiere Pro CC, Adobe	Đã có thông tin xác nhận bản vá.

			Prelude CC, Creative Cloud Desktop Application) cho phép đối tượng tấn công thu thập thông tin, chèn và thực thi mã lệnh, tấn công leo thang	
6	Bluetooth	CVE-2019-9506	Lỗ hổng trong tất cả thiết bị hỗ trợ kết nối Bluetooth BR/EDR trong quá trình thiết lập khóa mật mã cho phép đối tượng tấn công lấy dò đoán khóa mã hóa để giải mã dữ liệu trao đổi từ đó có thể thu thập thông tin và tấn công leo thang.	Đã có thông tin xác nhận và bản vá
7	HTTP/2	CVE-2019-9512 CVE-2019-9513 CVE-2019-9511 ...	Nhóm 09 Lỗ hổng trong việc thực thi HTTP/2 cho phép thực hiện nhiều hình thức tấn công từ chối dịch vụ. Lỗ hổng này có thể được khai thác trên diện rộng để thực hiện tấn công từ chối dịch vụ quy mô lớn Ảnh hưởng tới nhiều ứng dụng, máy chủ tham khảo chi tiết tại: https://vuls.cert.org/confluence/pages/viewpage.action?pageId=56393752	

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

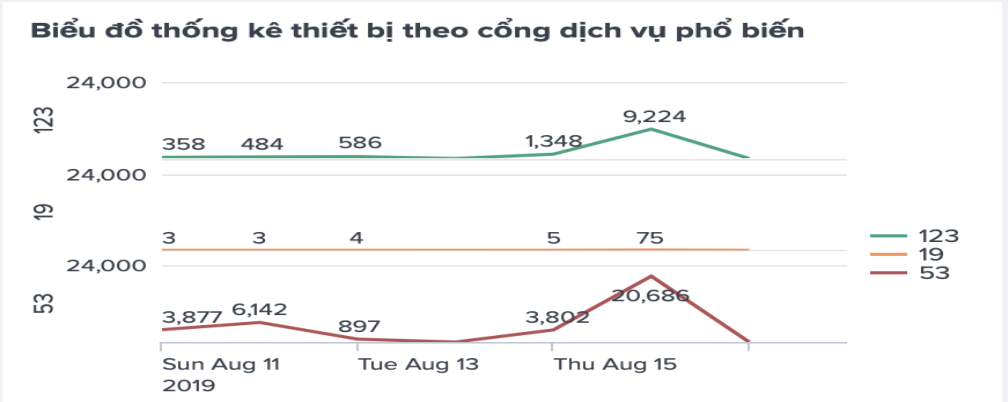
Tấn công từ chối dịch vụ là hình thức tấn công đã có từ lâu, và hiện tại vẫn được đối tượng tấn công ưa thích sử dụng để thực hiện các ý đồ xấu. Tấn công từ chối dịch vụ về cơ bản không nguy hiểm nhưng lại gây ảnh hưởng đến hoạt động của hệ thống, gây thiệt hại về kinh tế cho tổ chức bị tấn công.

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

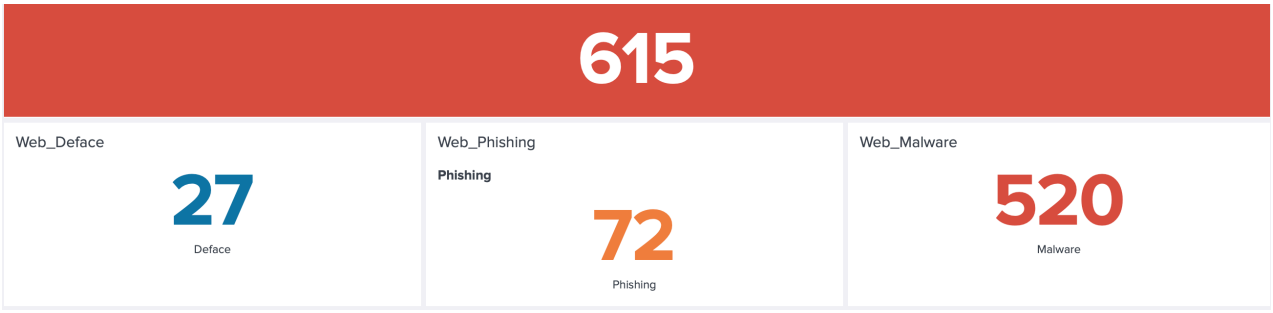
Tại Việt Nam, có rất nhiều máy chủ, thiết bị có thể trở thành nguồn phát tán tấn công DRDoS. Trong tuần có **47,494 (giảm so với tuần trước là 52,518)** thiết bị có khả năng bị huy động và trở thành nguồn tấn công DRDoS. Các thiết bị này đang mở sử dụng các dịch vụ NTP (123), DNS (53), Chargen (19). Dưới đây là biểu đồ thống kê thiết bị theo cổng dịch vụ phổ biến trong tuần

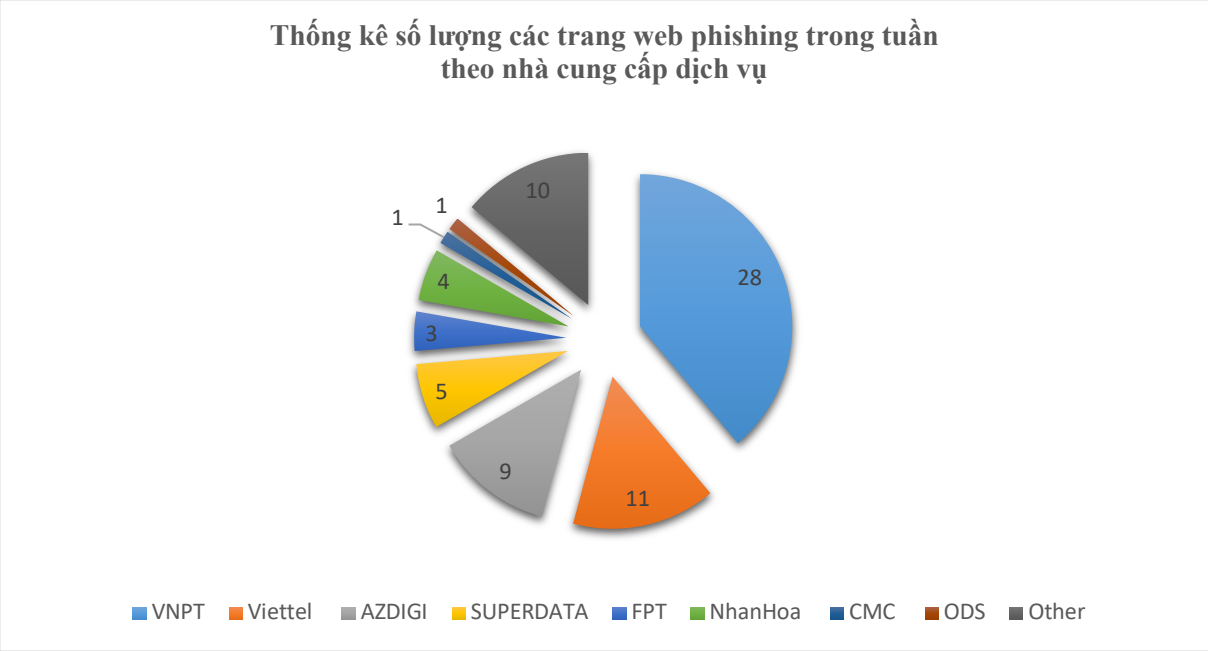


4. Tấn công vào Cổng TTĐT/ứng dụng web của Việt Nam

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 615 trường hợp tấn công vào trang/cổng thông tin điện tử của Việt Nam: 27 trường hợp tấn công thay đổi giao diện, 72 trường hợp tấn công lừa đảo (Phishing), 520 trường hợp tấn công cài cắm mã độc.

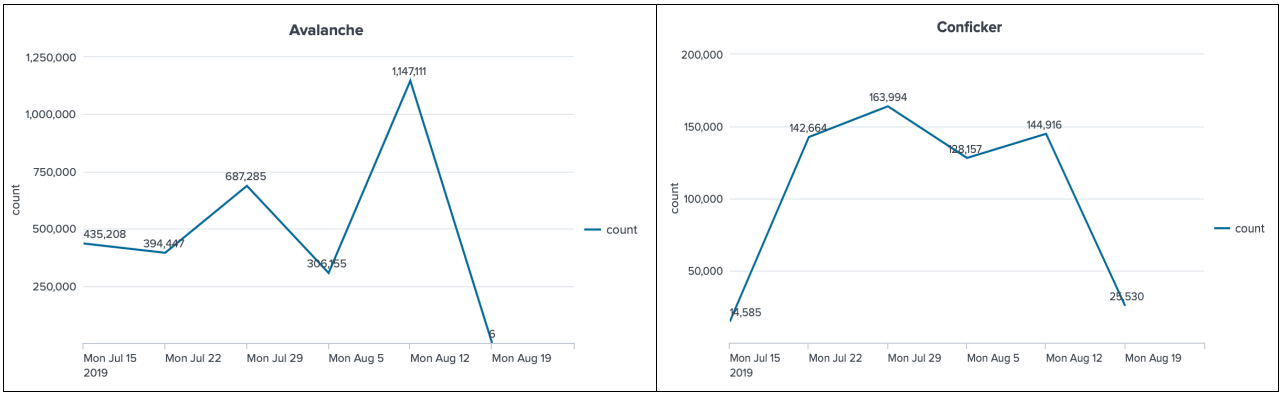


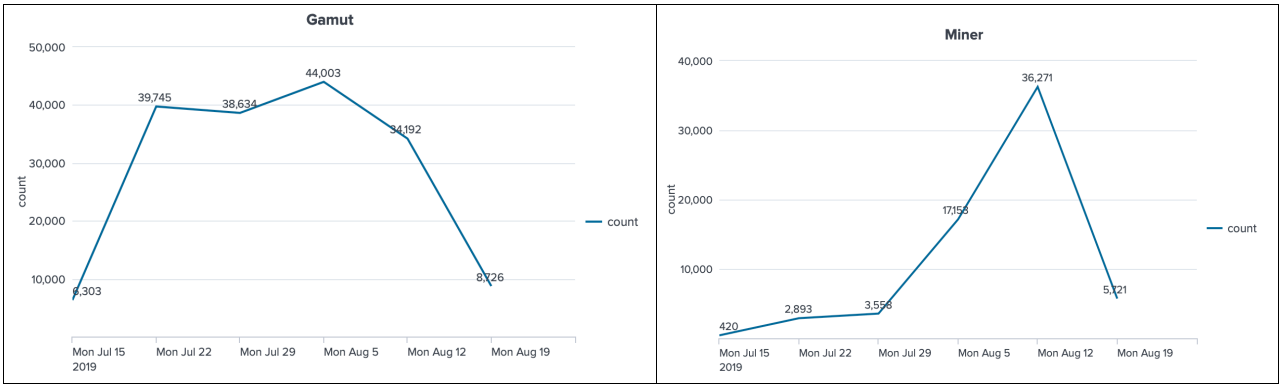


5. Hoạt động của mạng botnet, APT, mã độc tại Việt Nam

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 mạnh nhất và tăng mạnh so với tuần trước, có 1.147.111 lượt địa chỉ IP kết nối với máy chủ điều khiển (Tuần 32 là 306.155).

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	kn0ugjov.ru
5	soplifan.ru
6	xjpakmdcfuqe.com
7	xdqzpbcgrvkj.ru
8	75ulqnwb.ru
9	www.cityofangelsmagazine.com
10	somicrososoft.ru
11	morphed.ru
12	ixhtiv.info
13	cp.4nbizac8.ru
14	www.corpnox-technologie.fr

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