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 27 (từ 01/07 - 07/07/2019)

Số: /BC-CATTT *Hà Nội, ngày 09 tháng 07 năm 2019*

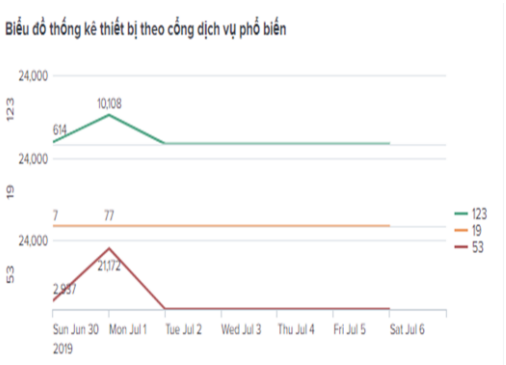
VIỆN TIÊU CHUẨN VÀ CÔNG NGHỆ QUỐC GIA HOA KỲ XUẤT BẢN BÀI BÁO LIÊN QUAN ĐẾN CÁC THIẾT BỊ IOT

Cuối tháng 6/2019, Viện Tiêu chuẩn và Công nghệ quốc gia Hoa Kỳ (NIST) đã xuất bản một tài liệu nhằm giúp các cơ quan liên bang và các tổ chức khác hiểu rõ hơn về quản lý rủi ro an toàn thông tin mạng và quyền riêng tư liên quan đến thiết bị

RANSOMWARE SODIN KHAI THÁC LỖ HỔNG WINDOWS VÀ KIẾN TRÚC BỘ XỬ LÝ

Ransomware Sodin (hay còn được gọi là Sodinokibi và Revil) được biết đến nửa đầu năm 2019, nó phát tán thông qua lỗ hổng Oracle Weblogic và tấn công nhằm vào nhà cung cấp MSP.

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 429 lỗ hổng, trong đó có 42 lỗ hổng mức cao, 116 lỗ hổng mức trung bình, 11 lỗ hổng mức thấp và 260 lỗ hổng chưa đánh giá; 03 lỗ hổng đã có mã khai thác.

VI PHẠM THÔNG TIN CÁ NHÂN

Một nghiên cứu mới đây về nguy cơ bị tấn công lừa đảo (phishing) của những người làm việc trong các ngành nghề khác nhau cho thấy những người làm trong ngành xây dựng có khả năng trở thành mục tiêu của tấn công phishing là cao nhất.

1. Điểm tin đáng chú ý

1.1. Cuối tháng 6/2019, Viện Tiêu chuẩn và Công nghệ quốc gia Hoa Kỳ (NIST) đã xuất bản một tài liệu nhằm giúp các cơ quan liên bang và các tổ chức khác hiểu rõ hơn về quản lý rủi ro an toàn thông tin mạng và quyền riêng tư liên quan đến các thiết bị IoT. Theo NIST, tài liệu này là ấn phẩm nền tảng cho một loạt các ấn phẩm tiếp theo cung cấp các nội dung cụ thể hơn trong việc quản lý bảo mật IoT. Tài liệu này xác định các vấn đề cần quan tâm đối với bảo đảm an toàn thông tin cho thiết bị IoT, thách thức và cách kiểm soát có liên quan cần điều chỉnh cho các thiết bị này.

NIST đưa ra một số cảnh báo như việc một số trường hợp nhà sản xuất IoT có thể ngừng phát hành bản vá hoặc không phát hành bản vá cho các thiết bị trong một khoảng thời gian dài. Điều đó có thể khiến các cơ quan, tổ chức gặp nhiều rủi ro do không thể loại bỏ các lỗ hổng đã được công bố. Ngoài ra, truy cập từ xa thường gây ra nhiều rủi ro bảo mật cho thiết bị IoT khi so sánh với các thiết bị CNTT khác. Các giao diện kết nối của IoT thường cho phép truy cập từ xa vào các hệ thống vật lý mà trước đây chỉ có thể được truy cập cục bộ. Điều này khiến các hệ thống vật lý có thể truy cập thông qua các thiết bị IoT có nguy cơ bị tấn công cao hơn nhiều. Các phương thức xác thực mạnh, chẳng hạn như xác thực đa yếu tố, cũng ít được triển khai đối với các thiết bị IoT.

Tham khảo thêm thông tin tài liệu của NIST tại:

https://nvlpubs.nist.gov/nistpubs/ir/2019/NIST.IR.8228.pdf

1.2. Một nghiên cứu mới đây về nguy cơ bị tấn công lừa đảo (phishing) của những người làm việc trong các ngành nghề khác nhau cho thấy những người làm trong ngành xây dựng có khả năng trở thành mục tiêu của tấn công phishing là cao nhất. Báo cáo về tấn công lừa đảo (phishing) trong các ngành công nghiệp năm 2019 của KnowBe4 đã nghiên cứu 19 ngành công nghiệp, các doanh nghiệp trong nghiên cứu được chia thành 3 loại: Loại nhỏ (dưới 250 nhân viên), loại trung bình (250-999) và loại lớn (1000 nhân viên trở lên).

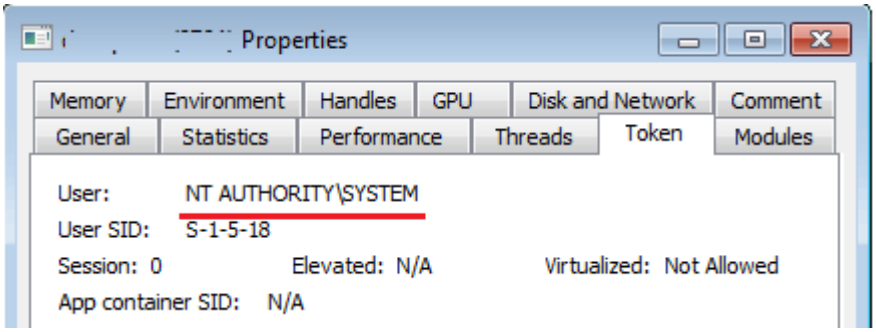
Kết quả cho thấy, đối với các tập đoàn, doanh nghiệp lớn thì ngành công nghiệp khách sạn chiếm vị trí đầu tiên. Đối với các doanh nghiệp vừa và nhỏ thì những người làm trong ngành xây dựng đứng đầu danh sách các cuộc tấn công. Bán lẻ/bán buôn và bảo hiểm lần lượt đứng thứ 2 và 3 trong danh sách các cuộc tấn công vào doanh nghiệp vừa và nhỏ.

Các chuyên gia cho rằng, để giảm thiểu nguy cơ của việc tấn công lừa đảo (phishing) cho những người làm việc trong các ngành nghề phi công nghệ thông tin

(non IT) thì việc đào tạo, tuyên truyền nâng cao nhận thức là quan trọng nhất, cần được ưu tiên triển khai trước các biện pháp kỹ thuật.

1.3. Ransomware Sodin (hay còn được gọi là Sodinokibi và Revil) được biết đến nửa đầu năm 2019, nó phát tán thông qua lỗ hổng Oracle Weblogic và tấn công nhằm vào nhà cung cấp MSP. Cùng với đó, tháng 8 năm ngoái Ransomware Sodin đã khai thác lỗ hổng CVE-2018-8453 (lỗ hổng trong win32k.sys) để nâng cao đặc quyền trong Windows và sử dụng chức năng xử lý để vượt qua các giải pháp bảo mật.

Trong khoảng từ tháng 4 đến tháng 6, theo Kaspersky, Sodin đã tấn công vào nhiều quốc gia trên thế giới trong đó có cả Việt Nam. Quốc gia bị tấn công nhiều nhất gồm Đài Loan, Hồng Kông, Hàn Quốc



Hình 1. Thông tin Trojan Sodin sau khi thực thi có được đặc quyền cao trong Windows

Trojan Sodin được lưu trữ ở dạng mã hóa trong đó phần thân là một khối lệnh cấu hình lưu cài đặt và dữ liệu cần thiết để Trojan hoạt động.

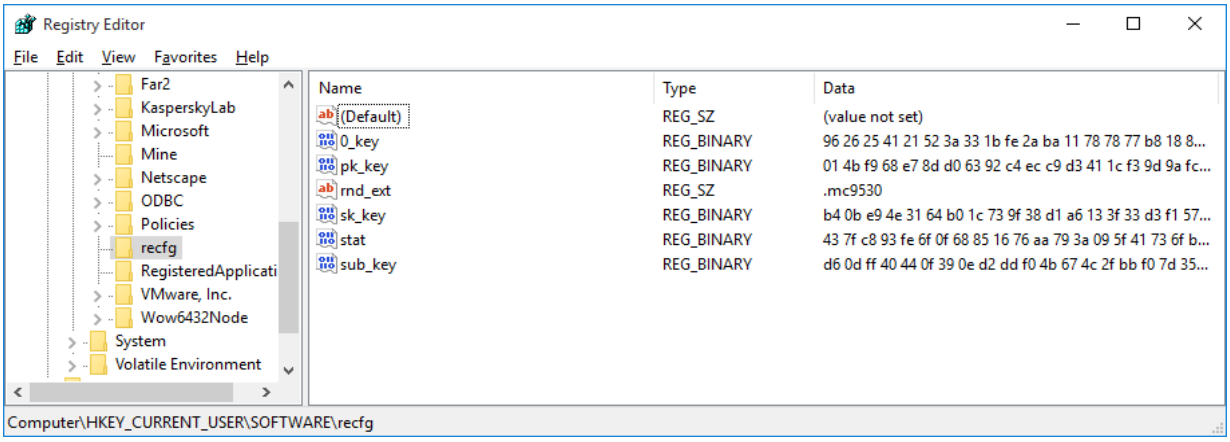
Hình 2. Khối lệnh cấu hình Trojan được giải mã

Bảng hiển thị các thành phần trong khối lệnh cấu hình Trojan Sodin

Field	**Purpose**
Pk	Khóa công khai

Pid	Id
Sub	Id chiến dịch
Dbg	Gỡ lỗi
Fast	Chế độ mã hóa nhanh (tối đa 0x100000 byte)
Lau	Xóa một số tệp nhất định và ghi đè nội dung của chúng bằng các byte ngẫu nhiên
Wfld	Tên của các thư mục trong đó Trojan xóa các tệp
Wht	Tên của thư mục và tệp và danh sách các phần mở rộng không được mã hóa
Prc	Tên của các quá trình được chấm dứt
Dmn	Địa chỉ máy chủ để gửi số liệu thống kê
Net	Gửi số liệu thống kê mạng bị nhiễm
Nbody	Tiền chuộc
Nname	Tên tập tin
Exp	Sử dụng khai thác để leo thang đặc quyền
Img	Văn bản cho hình nền máy tính

Sodin sử dụng lược đồ lai để mã hóa lại các tệp. Nội dung tệp được mã hóa bằng thuật toán đối xứng Salsa20 và thuật toán ECIES để tạo các khóa trong hệ thống Windows.



Hình 3. Dữ liệu và các khóa được tạo bởi Trojan Sodin

Khi lây nhiễm vào máy, mã độc sẽ gửi thông tin máy bị nhiễm về máy chủ điều khiển, dữ liệu truyền đi sẽ được mã hóa bằng thuật toán ECIES sử dụng mã hóa công khai.

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 429 lỗ hổng, trong đó có 42 lỗ hổng mức cao, 116 lỗ hổng mức trung bình, 11 lỗ hổng mức thấp và 260 lỗ hổng chưa đánh giá; 03 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 18 lỗ hổng trong một số sản phẩm của Cisco; Nhóm 26 lỗ hổng trên sản phẩm, phần mềm IBM; Nhóm 13 lỗ hổng trên Wordpress 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-2019-1922 CVE-2019-1932 CVE-2019-1889 CVE-2019-1933 ….	Nhóm 18 lỗ hổng trên một số sản phẩm của Cisco (Phần mềm điện thoại IP SIP, AsyncOS) cho phép kẻ tấn công thực hiện tấn công từ chối dịch vụ, chèn và thực thi mã lệnh, tấn công leo thang để chiếm quyền kiểm soát thiết bị.	Đã có thông tin xác nhận và bản vá
2	IBM	CVE-2019-4057 CVE-2019-4154 CVE-2019-4322 CVE-2019-4369 …..	Nhóm 26 lỗ hổng dựa trên một số sản phẩm của IBM (DB2, Security Guardium, WebSphere Application Server) cho phép kẻ tấn công xác thực cục bộ thực thi mã tùy ý trên hệ thống, gây tràn bộ đệm. Truy cập tài khoản DB2 thực mã tùy ý và lấy thông tin nhạy cảm.	Đã có thông tin xác nhận và bản vá

3	Wordpress	CVE-2019-5971 CVE-2019-5962 CVE-2019-12826 ….	Nhóm 13 lỗ hổng trên máy chủ sử dụng Wordpress cho phép kẻ tấn công khia thác lỗi CSRF, XSS để lấy thông tin xác thực và chiếm quyền quản trị viên, thay đổi cài đặt ứng dụng.	Đã có thông tin xác nhận và bản vá
4	Jetbrains	CVE-2019-12842 CVE-2019-12845 CVE-2019-12846 …..	Nhóm 21 lỗ hổng trên sản phẩm của Jetbrains (JetBrains Hub, IntelliJ IDEA, Ktor) cho phép người dùng tạo kết nối không được mã hóa làm lộ thông tin đăng nhập, một số lỗ hổng cho phép thực hiện tấn công từ xa thực thi mã khi cấu hình đang chạy.	Đã có thông tin xác nhận và bản vá
5	D-Link	CVE-2019-13373 CVE-2019-13374 CVE-2019-13375 …..	Nhóm 19 lỗ hổng trên một số sản phẩm của D-Link (Central WiFi Manager CWM, D-Link DCS-1100, DCS-1130) cho phép đối tượng khai thác lỗi SQL Injection qua nhiều tham số khác nhau, thực thi các đoạn mã PHP độc hại, khai thác lỗi tràn bộ đệm để cài cắm mã độc vào thiết bị.	Đã có thông tin xác nhận và bản vá

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

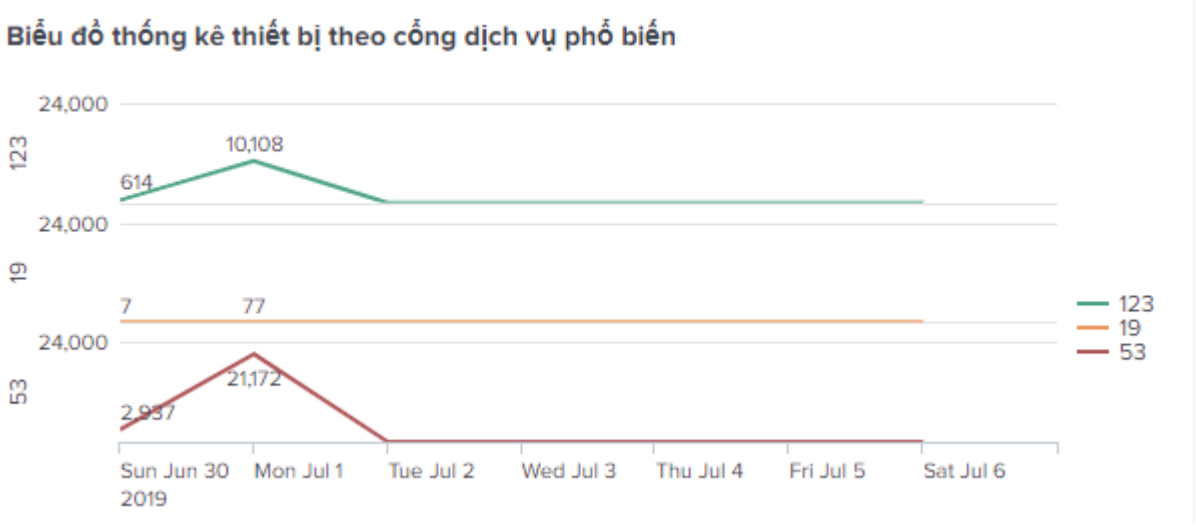
Tấn công từ chối dịch vụ là hình thức tấn công đã có từ lâu, và hiện tại vẫn được đối tượng tấn công ưa thích sử dụng để thực hiện các ý đồ xấu. Tấn công từ chối dịch vụ về cơ bản không nguy hiểm nhưng lại gây ảnh hưởng đến hoạt động của hệ thống, gây thiệt hại về kinh tế cho tổ chức bị tấn công.

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

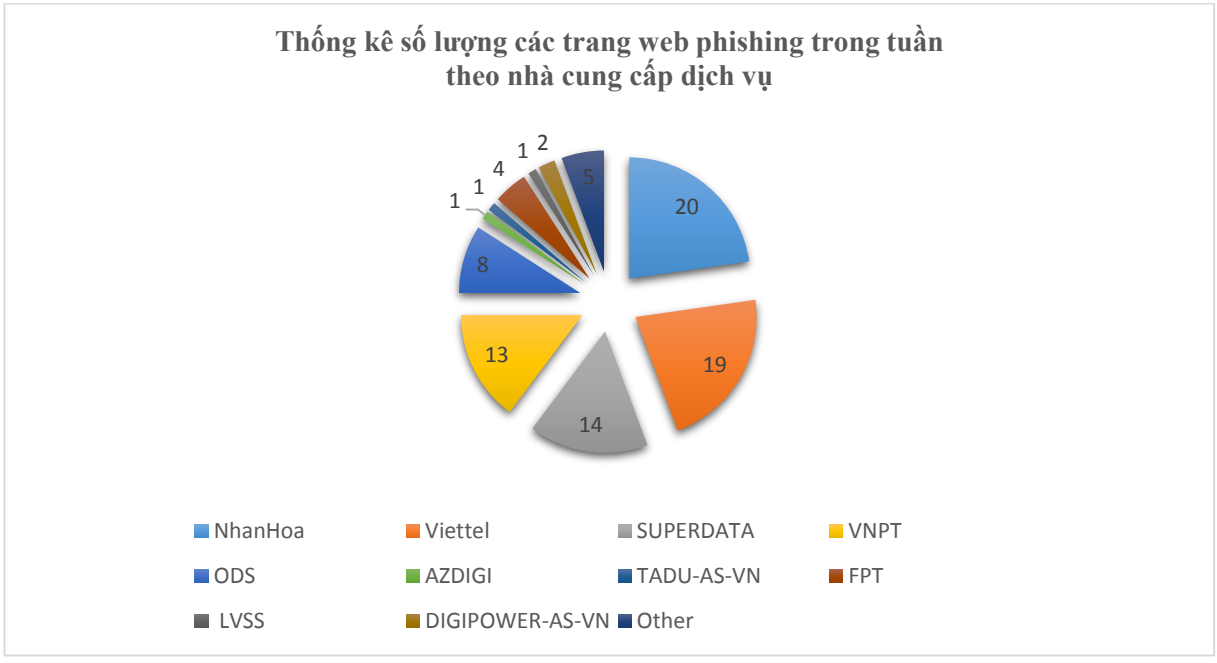
Tại Việt Nam, có rất nhiều máy chủ, thiết bị có thể trở thành nguồn phát tán tấn công DRDoS. Trong tuần có **34,915** (giảm ~ 10.000 so với tuần 26**)** thiết bị có khả năng bị huy động và trở thành nguồn tấn công DRDoS. Các thiết bị này đang mở sử dụng các dịch vụ NTP (123), DNS (53), Chargen (19). 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.

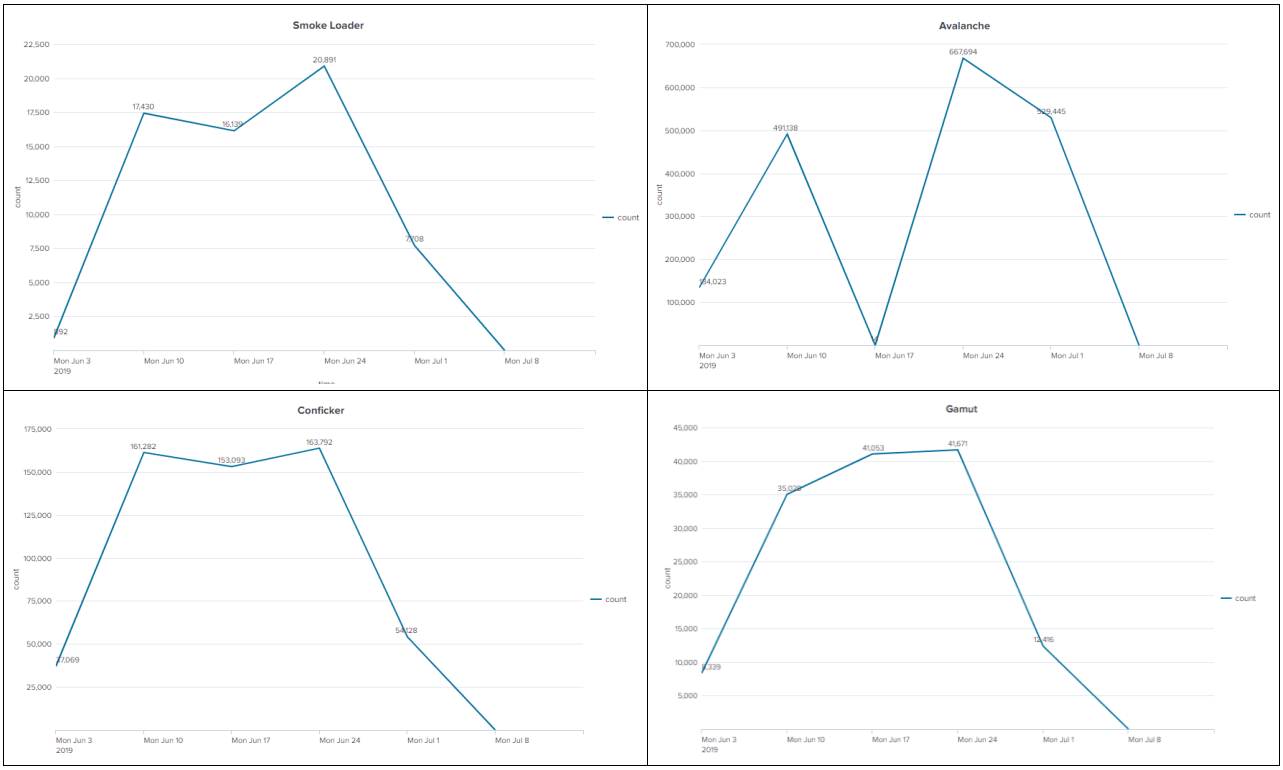
Trong tuần, có 178 trường hợp tấn công vào trang/cổng thông tin điện tử của Việt Nam: 05 trường hợp tấn công thay đổi giao diện, 88 trường hợp tấn công lừa đảo (Phishing), 85 trường hợp tấn công cài cắm mã độc.



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, có 529.445 lượt địa chỉ IP kết nối đến các máy chủ điều khiển của mạng botnet này.

5.2. Danh sách IP/tên miền độc hại có nhiều kết nối từ Việt Nam

TT	Tên miền/IP
1	differentia.ru
2	disorderstatus.ru
3	atomictrivia.ru

4	soplifan.ru
5	somicrososoft.ru
6	www.cityofangelsmagazine.com
7	kodklq.info
8	morphed.ru
9	bharatisangli.in
10	a.deltaheavy.ru
11	www.corpnox-technologie.fr
12	caarmelcollege.org
13	hzmksreiuojy.in

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