ỦY BAN NHÂN DÂN THÀNH PHỐ HÀ NỘI **SỞ THÔNG TIN VÀ TRUYỀN THÔNG**	**CỘNG HÒA XÃ HỘI CHỦ NGHĨA VIỆT NAM** **Độc lập - Tự do - Hạnh phúc**
Số: 2409/STTTT - CNTT V/v rà soát, thực hiện các cảnh báo về an toàn thông tin của Cục An toàn thông tin - Bộ TTTT tháng 8/2019.	*Hà Nội, ngày 11 tháng 9 năm 2019*

Kính gửi:
- Các Sở, ban, ngành;
- UBND các quận, huyện, thị xã.

Theo các báo cáo số: 37/BC-CATTT ngày 05/8/2019; số 38/BC-CATTT ngày 13/8/2019; số 40/BC-CATTT ngày 26/8/2019 của Cục An toàn thông tin, Bộ Thông tin và Truyền thông, tình hình an toàn thông tin tháng 7/2019 có những diễn biến phức tạp. Trong đó, các nguy cơ mất ATTT chủ yếu tập trung vào khai thác điểm yếu, lỗ hổng bảo mật của các thiết bị, hệ thống, cổng thông tin, dịch vụ, ứng dụng công nghệ thông tin nhằm mục đích kiểm soát, làm tổn hại đến dữ liệu máy tính.

Nhằm đảm bảo an toàn thông tin và phòng tránh nguy cơ mất an toàn thông tin có thể xảy ra, Sở Thông tin và Truyền thông đề nghị các Sở, ban, ngành và UBND các quận, huyện, thị xã (gọi tắt là các đơn vị) tổ chức rà soát, thực hiện các khuyến nghị của Cục An toàn thông tin tại các Báo cáo nêu trên đối với các hệ thống mạng công nghệ thông tin tại đơn vị mình *(Bản chụp các báo cáo của Cục An toàn thông tin kèm theo)*.

Trong quá trình tổ chức thực hiện nếu có khó khăn vướng mắc đề nghị các đơn vị liên hệ với Đội ứng cứu sự cố an toàn thông tin mạng của Sở Thông tin và Truyền thông Hà Nội theo số điện thoại **024.3512.1616**./.

Nơi nhận:
- Như trên;
- Đ/c Giám đốc Sở (để b/c);
- Phó Giám đốc Sở: Đặng Vũ Tuấn, Nguyễn Xuân Quang;
- Cục An toàn thông tin - Bộ TT&TT;
- Trung tâm Dữ liệu nhà nước (để t/h);
- Lưu: VT, CNTT.

KT.GIÁM ĐỐC
PHÓ GIÁM ĐỐC

SỞ THÔNG TIN VÀ TRUYỀN THÔNG

Đặng Vũ Tuấn

BỘ THÔNG TIN VÀ TRUYỀN THÔNG
TRUNG TÂM ỨNG CỨU KHẨN CẤP AN TOÀN THÔNG TIN
TRUNG TÂM ỨNG CỨU KHẨN CẤP AN TOÀN KHÔNG GIAN MẠNG QUỐC GIA

Báo cáo tóm tắt
Tình hình an toàn thông tin đáng chú ý tuần 31 (từ 29/07 - 04/08/2019)

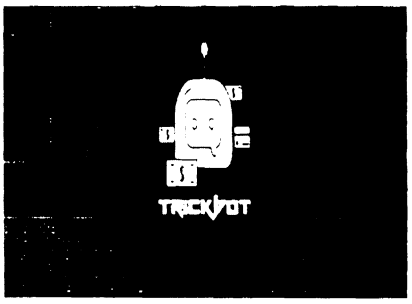
Số: /BC-CATTT *Hà Nội, ngày 05 tháng 08 năm 2019*

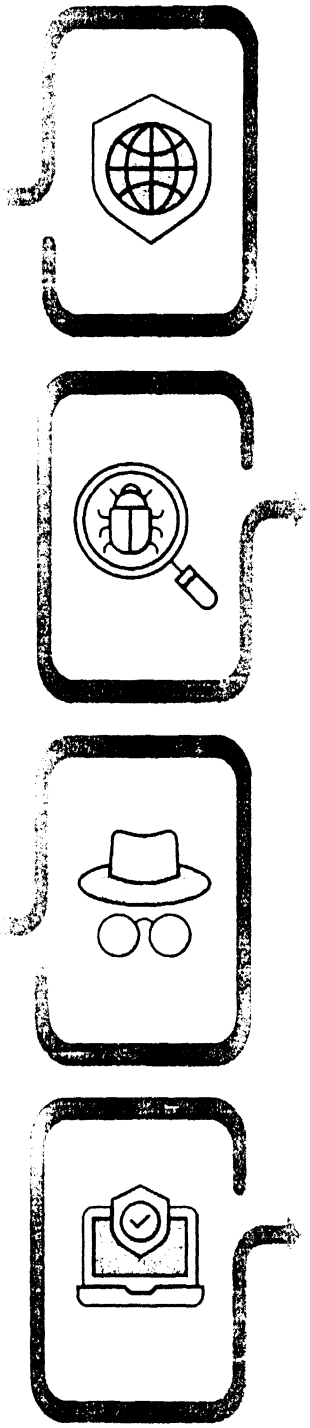
KHUNG ĐÀO TẠO CHO NHÂN VIÊN BẢO VỆ DỮ LIỆU

Ủy ban bảo vệ dữ liệu cá nhân (PDPC) của Singapore giới thiệu khung đào tạo cho Nhân viên bảo vệ dữ liệu (DPO - data protection officers). Khung đào tạo này được xây dựng nhằm mục đích chuẩn hóa việc đào tạo bảo vệ dữ liệu cho các DPO làm việc tại những cơ quan, tổ chức ở Singapore, để họ đạt được các tiêu chuẩn mong muốn.

BIẾN THỂ TRICKBOT MỚI NHẮM VÀO WINDOWS DEFENDER CỦA MICROSOF

Một biến thể mới của mã độc TrickBot tiếp tục được đối tượng tấn công mạng phát triển với tính năng ngăn chặn việc phát hiện và loại bỏ nó. Trong phiên bản mới, TrickBot đã đặt mục tiêu vào Windows Defender - phần mềm chống mã độc được cài đặt trên máy Windows.





THỐNG KÊ NGUỒN TẤN CÔNG DDOS

Bé đã [illegible]

ĐIỂM YẾU, LỖ HỔNG AN TOÀN THÔNG TIN

Trong tuần, các tổ chức quốc tế đã công bố và cập nhật ít nhất 618 lỗ hổng, trong đó có 35 lỗ hổng mức cao, 120 lỗ hổng mức trung bình, 45 lỗ hổng mức thấp và 418 lỗ hổng chưa đánh giá. Trong đó có ít nhất 57 lỗ hổng cho phép chèn và thực thi mã lệnh.

CHÍNH PHỦ KAZAKHSTAN ÁP DỤNG CHÍNH SÁCH KIỂM SOÁT LƯU LƯỢNG TRUY CẬP HTTPS

Tháng 7/2019, Chính phủ Kazakhstan đã bắt đầu áp dụng chính sách kiểm soát tất cả lưu lượng truy cập HTTPS bên trong biên giới lãnh thổ của mình. Các nhà cung cấp dịch vụ Internet (ISP) tại Kazakhstan được Chính phủ hướng dẫn để yêu cầu khách hàng của họ cài đặt chứng chỉ do chính phủ cấp cho tất cả các thiết

1. Điểm tin đáng chú ý

1.1. Ủy ban bảo vệ dữ liệu cá nhân (PDPC) của Singapore giới thiệu khung đào tạo cho Nhân viên bảo vệ dữ liệu (DPO - data protection officers). Khung đào tạo này được xây dựng nhằm mục đích chuẩn hóa việc đào tạo bảo vệ dữ liệu cho các DPO làm việc tại những cơ quan, tổ chức ở Singapore, để họ đạt được các tiêu chuẩn mong muốn. Theo luật bảo vệ dữ liệu cá nhân (PDPA) mọi cơ quan, tổ chức được yêu cầu phải chỉ định ít nhất một DPO giám sát và bảo vệ dữ liệu trong cơ quan, tổ chức của mình. Một khảo sát của PDPC cho thấy 39% các tổ chức lo ngại về việc liệu DPO của họ có được trang bị các kỹ năng và kiến thức cần thiết để giảm rủi ro vi phạm dữ liệu và tăng khả năng phục hồi.

Bộ trưởng Bộ Thông tin và Truyền thông Singapore, Iswaran đã công bố khung đào tạo này tại Hội thảo Bảo vệ dữ liệu cá nhân. Ông Iswaran cho biết khung đào tạo liệt kê rõ ràng bộ kỹ năng mà DPO nên có. Các doanh nghiệp cũng có thể tham khảo khung này để hỗ trợ trong việc đưa ra quyết định tuyển dụng, lập kế hoạch đào tạo cho các DPO và các nhóm bảo vệ dữ liệu. Ông Iswaran nhấn mạnh rằng các doanh nghiệp nên coi việc bảo vệ dữ liệu là một yêu cầu bắt buộc quan trọng chứ không phải là một phí tổn không cần thiết. Theo ông nếu quản lý tốt dữ liệu thì đây là một nguồn cạnh tranh trong kinh doanh và là phương tiện để tạo ra những cơ hội mới cho doanh nghiệp.

1.2. Tháng 7/2019, Chính phủ Kazakhstan đã bắt đầu áp dụng chính sách kiểm soát tất cả lưu lượng truy cập HTTPS bên trong biên giới lãnh thổ của mình. Các nhà cung cấp dịch vụ Internet (ISP) tại Kazakhstan được Chính phủ hướng dẫn để yêu cầu khách hàng của họ cài đặt chứng chỉ do chính phủ cấp cho tất cả các thiết bị và mọi trình duyệt. Chính phủ Kazakhstan có kế hoạch kiểm soát lưu lượng truy cập HTTPS vào năm 2016 nhưng đã phải xem xét lùi thời hạn thực hiện do các ý kiến phản đối của một số tổ chức, bao gồm: các ISP, ngân hàng và chính phủ nước ngoài.

Chứng chỉ gốc được đề cập đến trong chính sách kiểm soát nói trên được gọi là "chứng chỉ tin cậy" hoặc "chứng chỉ bảo mật quốc gia", nếu được cài đặt, nó sẽ cho phép các ISP giám sát các kết nối HTTPS và TLS được mã hóa của người dùng, giúp cơ quan chức năng theo dõi và kiểm duyệt nội dung. Chính phủ Kazakhstan cho biết biện pháp này là nhằm tăng cường bảo vệ công dân, cơ quan chính phủ và doanh nghiệp trước các cuộc tấn công mạng, đặc biệt là tấn công lừa đảo.

1.3. Một biến thể mới của mã độc TrickBot tiếp tục được đối tượng tấn công mạng phát triển với tính năng ngăn chặn việc phát hiện và loại bỏ nó. Trong phiên bản mới, TrickBot đã đặt mục tiêu vào Windows Defender - phần mềm chống mã độc được cài đặt trên máy Windows.

TrickBot là một mã độc dạng Trojan được thiết kế với mục tiêu đánh cắp thông tin ngân hàng trực tuyến, ví tiền điện tử, thông tin trình duyệt và nhiều thông tin khác được lưu trên máy tính và trình duyệt của người dùng.

Khi TrickBot được thực thi, nó khởi động Loader trên hệ thống bằng cách vô hiệu hoá các dịch vụ và tiến trình của Windows liên quan tới phần mềm bảo mật để chiếm đặc quyền trong hệ thống. Sau đó, Loader này tải thành phần độc hại chính bằng cách chèn DLL độc hại và tải xuống các mô-đun khác nhằm đánh cắp thông tin từ máy tính, tầng truyền thông/giao tiếp của các dịch vụ trên hệ thống và thực hiện nhiều hoạt động độc hại khác.

Trước khi xuất hiện biến thể mới này, TrickBot đã nhắm mục tiêu vào Windows Defender bằng cách được thực hiện các bước sau:

- Vô hiệu hoá và sau đó xoá dịch vụ WinDefend.

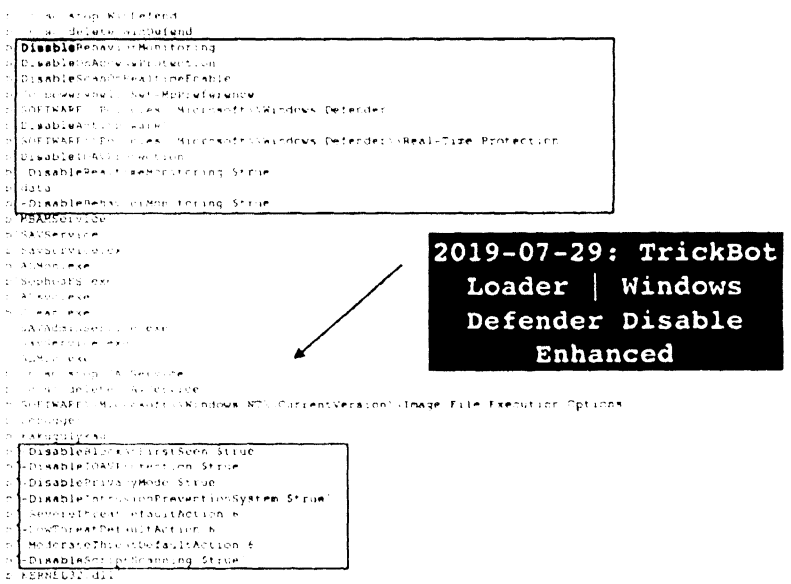
- Dừng tiến trình MsMpEng.exe, MSASCuiL.exe và MSASCui.exe

- Thêm chính sách DisableAntiSpyware vào Windows Policy và thiết lập thành True để tắt Windows Defender và các phần mềm antivirus khác.

- Vô hiệu hóa thông báo bảo mật Windows Security.

- Vô hiệu hoá tính năng bảo vệ thời gian thực của Windows Defender

Với biến thể mới TrickBot đã thêm 12 phương thức bổ sung nhằm mục tiêu và vô hiệu hoá Windows Defender và Microsoft Defender APT trong Windows. Các phương thức này sử dụng cài đặt Registry hoặc lệnh Set-MpPreference PowerShell để đặt tuỳ chọn Windows Defender.



Hình 1. TrickBot nhắm mục tiêu Windows Defnder nâng cao

Khi TrickBot phát hiện một số chương trình bảo mật được cài đặt, nó sẽ cấu hình trình gỡ lỗi cho tiến trình đó bằng cách sử dụng khoá registry File Execution Options và giúp trình gỡ lỗi chạy trước khi chương trình được thực thi, trình gỡ lỗi tồn tại thì chương trình bảo mật đó sẽ không được thực hiện.

Việc mã độc vượt qua phần mềm bảo mật (anti-virus) cài đặt trên máy tính để đánh cắp thông tin dữ liệu cũng như thực hiện hành động độc hại trên hệ thống không còn mới là mới, do vậy người dùng cũng như quản trị viên hệ thống không nên quá tin tưởng và chủ quan khi đã cài đặt giải pháp phòng chống mã độc trên máy tính, cũng như cần phải tự trang bị kiến thức và kỹ năng để hạn chế tối đa các nguy cơ bị lây nhiễm mã độc khi tham gia môi trường Internet.

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 618 lỗ hổng, trong đó có 35 lỗ hổng mức cao, 120 lỗ hổng mức trung bình, 45 lỗ hổng mức thấp và 418 lỗ hổng chưa đánh giá. Trong đó có ít nhất 57 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 249 lỗ hổng trên phần mềm Cpanel; Nhóm 06 lỗ hổng trên EspoCRM; Nhóm 08 lỗ hổng trên sản phẩm của D-Link, 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	Cpanel	CVE-2019-14408 CVE-2018-20863 CVE-2018-20869	Nhóm 249 lỗ hổng trên cpanel - ứng dụng phổ biến sử dụng để quản lý web, cho phép đối tượng tấn công khai thác lỗi SQL Injection, XSS, chèn và thực thi mã lệnh qua nhiều thành phần khác nhau, tấn công leo thang.	Đã có thông tin xác nhận và ban vá

2	EspoCRM	CVE-2019-14329 CVE-2019-14330 CVE-2019-14349 ...	Nhóm 06 lỗ hổng trên phần mềm EspoCRM - phần mềm quản lý khách hàng cho phép đối tượng tấn công khai thác lỗi XSS qua nhiều thành phần khác nhau, thực hiện tấn công vét cạn để đánh cắp thông tin tài khoản.	Một số lỗ hổng đã có cách khắc phục.
3	Jenkins	CVE-2019-10356 CVE-2019-10362 CVE-2019-10344 ...	Nhóm 14 lỗ hổng trên một số plugin của Jenkins (phần mềm nguồn mở cho phép xây dựng và triển khai tự động ứng dụng, dùng nhiều trong phát triển phầm mềm) cho phép đối tượng tấn công khai thác lỗi XSS, thu thập thông tin xác thực do lưu trữ không mã hóa, truy cập trái phép vào dữ liệu trên hệ thống, một số lỗ hổng cho phép chèn và thực thi mã lệnh.	Đã có thông tin xác nhận và bản vá
4	D-Link	CVE-2019-14334 CVE-2019-14336 CVE-2019-14333 ...	Nhóm 08 lỗ hổng trên một số sản phẩm của D-Link cho phép đối tượng tấn công thực hiện khai thác lỗi XSS, thu thập thông tin xác thực, lấy thông tin cấu hình của thiết bị, một số lỗ hổng cho phép chèn và thực thi lệnh nguy hiểm	Đã có thông tin xác nhận và bản vá
5	Elastic	CVE-2019-7615 CVE-2019-7614 CVE-2019-7616	Nhóm 03 lỗ hổng trên sản phẩm của Elastic gồm Elasticsearch, Kibana và APM agent cho phép đối tượng tấn công thực hiện tấn công nghe lén, khai thác lỗi SSRF, truy cập dữ liệu nhạy cảm của người dùng khác trên cùng hệ thống.	Chưa có thông tin xác nhận bản vá.

6	IBM	CVE-2019-4062 CVE-2019-4275 CVE-2019-4285 ...	Nhóm 07 lỗ hổng trên một số sản phẩm, ứng dụng của IBM (i2 Intelligent Analyis Platform, Jazz for Service Management, Spectrum Protect for Enterprise Resource Planning, BM WebSphere Application Server) cho phép đối tượng tấn công thu thập thông tin, tấn công từ chối dịch vụ, lấy thông tin mật khẩu ở dạng rõ.	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.

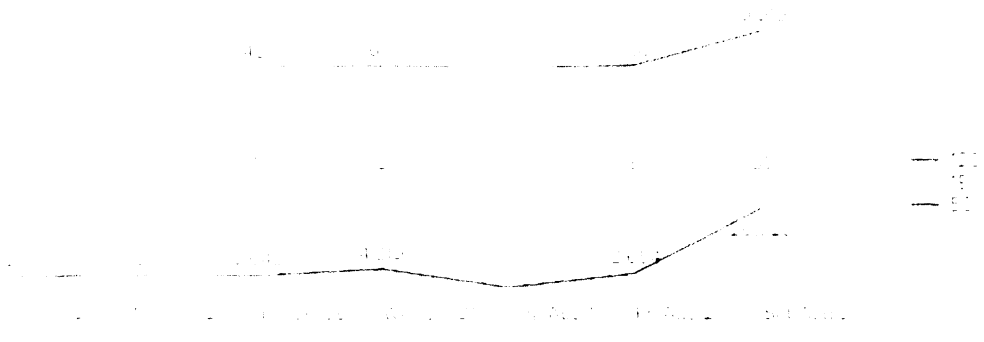
Tấn công từ chối dịch vụ có thể được thực hiện với nhiều kỹ thuật khác nhau, nhưng trong những năm gần đây phần lớn tin tặc huy động các thiết bị đang mở cổng dịch vụ sử dụng giao thức UDP để thực hiện tấn công. Các thiết bị này có thể bị huy động dễ dàng để thực hiện tấn công DRDoS (tấn công từ chối 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

Giao thức	Số lần khuếch đại băng thông
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 **50,428 (giảm so với tuần trước là 50,756)** 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.

Biểu đồ thống kê thiết bị theo cổng dịch vụ phổ biến



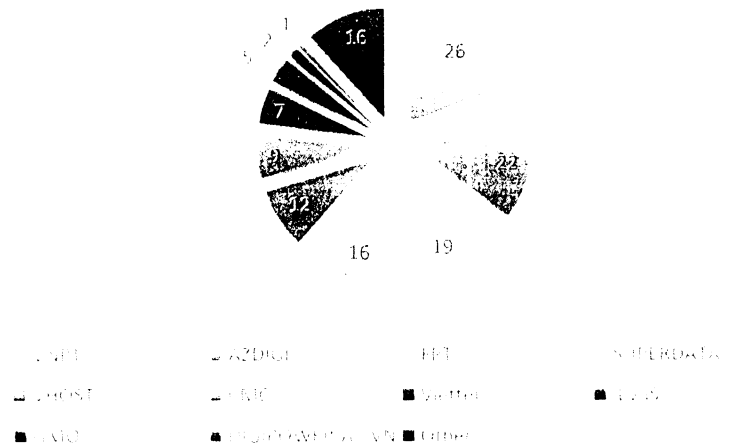
4. Tấn công vào Cổng TTĐT/ứng dụng web của Việt Nam

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 422 trường hợp tấn công vào trang/cổng thông tin điện tử của Việt Nam: 05 trường hợp tấn công thay đổi giao diện, 135 trường hợp tấn công lừa đảo (Phishing), 282 trường hợp tấn công cài cắm mã độc.

Thống kê số lượng các trang web phishing trong tuần theo nhà cung cấp dịch vụ



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 có tăng so với tuần trước, có 687.285 lượt địa chỉ IP kết nối với máy chủ điều khiển (Tuần 30 là 394.447).

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	www.iuqerfsodp9ifjaposdfjhgosurijfaewrwergwea.com
6	25hj1urb.ru
7	somicrososoft.ru
8	xjpakmdefuqe.com
9	uaqbzunani.info
10	www.cityofangelsmagazine.com
11	morphed.ru
12	qsqjeuno53.ru
13	www.corpnox-technologie.fr
14	cp.qc0zt6eo.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

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)

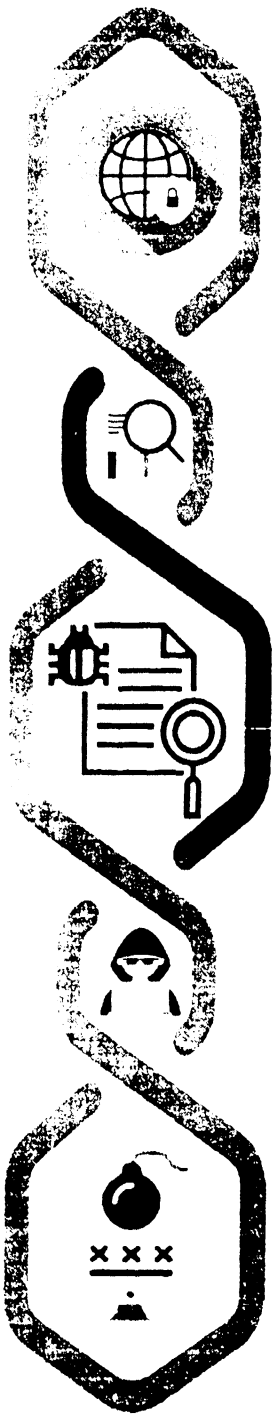
Số: /BC-CATTT *Hà Nội, ngày 26 tháng 08 năm 2019*

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

Bảo đảm thông tin thời gian thực

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

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 bao 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 ban 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 ban 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 bao 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 qua 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.

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, chuyển hướng người dùng đến trang web độc hại.	Đã có thông tin xác nhận bản vá.
5	Cisco	CVE-2019-1883	Nhóm 27 lỗ hổng trên một số	Đã có

		CVE-2019-1907 CVE-2019-1900 ...	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.	thông tin xác nhận và ban 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 ban 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 ban 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.

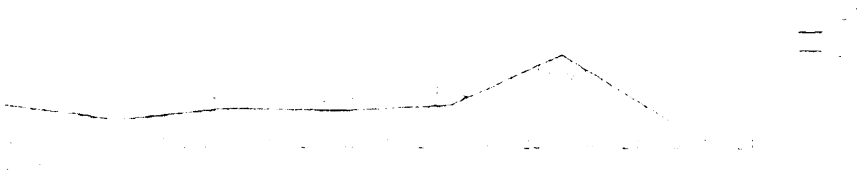
Tấn công từ chối dịch vụ có thể được thực hiện với nhiều kỹ thuật khác nhau, nhưng trong những năm gần đây phần lớn tin tặc huy động các thiết bị đang mở cổng dịch vụ sử dụng giao thức UDP để thực hiện tấn công. Các thiết bị này có thể bị huy động dễ dàng để thực hiện tấn công DRDoS (tấn công từ chối 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

Giao thức	Số lần khuếch đại băng thông
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

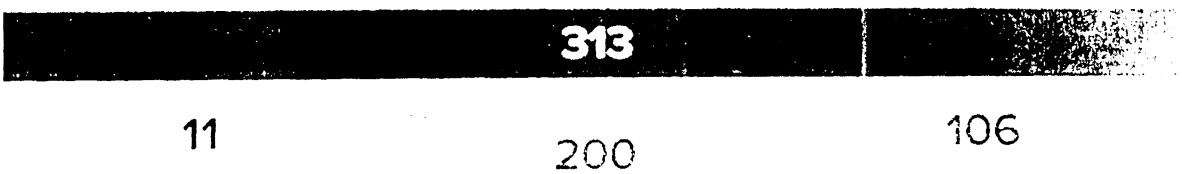
Biểu đồ thống kê thiết bị theo công dịch vụ phổ biến



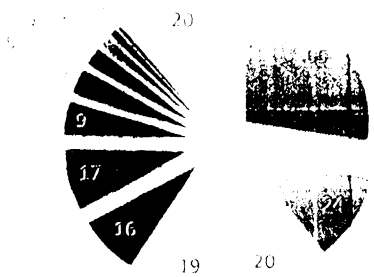
4. Tấn công vào Cổng TTĐT/ứng dụng web của Việt Nam

Website/Cổng thông tin điện tử là kênh cung cấp thông tin hiệu qua 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.



Thống kê số lượng các trang web phishing trong tuần theo nhà cung cấp dịch vụ



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

BỘ THÔNG TIN VÀ TRUYỀN THÔNG
CỤC AN TOÀN THÔNG TIN
TRUNG TÂM ỨNG CỨU KHẨN CẤP AN TOÀN KHÔNG GIAN MẠNG QUỐC GIA

Báo cáo tóm tắt
Tình hình an toàn thông tin đáng chú ý tuần 32 (từ 05/08 - 11/08/2019)

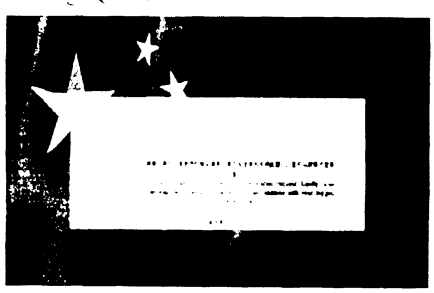
Số: 38 /BC-CATTT | *Hà Nội, ngày 13 tháng 08 năm 2019*

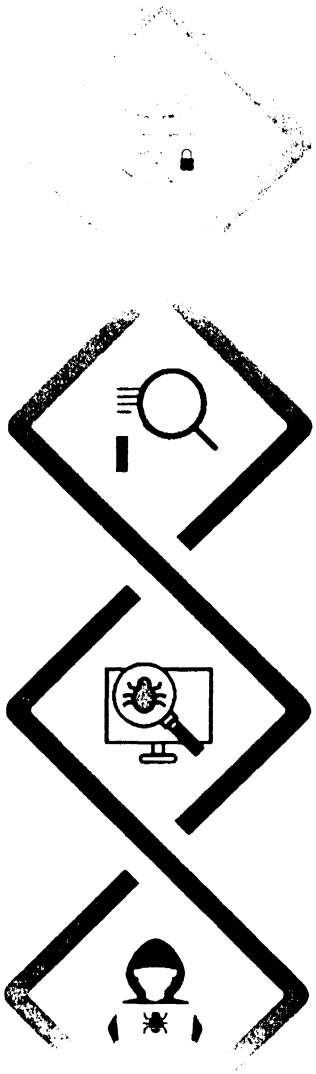
HOẠT ĐỘNG MẠNG LƯỚI NHÓM TẤN CÔNG MẠNG MAGECART

Trong tháng 7 2019, các nhà nghiên cứu bảo mật đã phát hiện và ngăn chặn 65.000 hành động nhằm mục tiêu đánh cắp thông tin thẻ tín dụng từ các trang web bán hàng trực tuyến. Theo thống kê, 53,5% thẻ tín dụng bị đánh cắp thông tin là của người mua hàng ở Hoa Kỳ. Canada đứng thứ 2 với tỉ lệ 15,7%, tiếp theo là Đức với tỉ lệ 6,8% và Hà Lan với tỉ lệ 6,4%.

NHÓM APT BITTER NHẮM MỤC TIÊU VÀO CHÍNH PHỦ TRUNG QUỐC

Theo các nhà nghiên cứu của Anomali đã xác định một trang web giả mạo được thiết kế giống như trang đăng nhập email của Bộ Ngoại giao Trung Quốc. Sau khi điều tra, họ cũng đã phát hiện hơn 40 trang web giả mạo và dường như nhắm mục tiêu vào chính phủ và các tổ chức khác ở Trung Quốc.





THỐNG KÊ NGUỒN TẤN CÔNG DDOS

Biểu đồ thống kê thiết bị theo công dịch vụ phổ biến

ĐIỂM YẾU, LỖ HỔNG AN TOÀN THÔNG TIN

Trong tuần, các tổ chức quốc tế đã công bố và cập nhật ít nhất 445 lỗ hổng, trong đó có 20 lỗ hổng mức cao, 98 lỗ hổng mức trung bình, 71 lỗ hổng mức thấp và 256 lỗ hổng chưa đánh giá. Trong đó có ít nhất 57 lỗ hổng cho phép chèn và thực thi mã

HƠN 14,3 TRIỆU NGƯỜI CHILE BỊ LỘ THÔNG TIN CÁ NHÂN

Thông tin cử tri của hơn 14.3 triệu người Chile (chiếm gần 80% toàn bộ dân số của đất nước này), đã bị lộ, lọt trên mạng. Các thông tin này được lưu trữ trong một cơ sở dữ liệu Elasticsearch (Elasticsearch - công cụ tìm kiếm trên nền tảng Apache Lucene).

1. Điểm tin đáng chú ý

1.1. Trong tháng 7/2019, các nhà nghiên cứu bảo mật đã phát hiện và ngăn chặn 65.000 hành động nhằm mục tiêu đánh cắp thông tin thẻ tín dụng từ các trang web bán hàng trực tuyến. Theo thống kê, 53.5% thẻ tín dụng bị đánh cắp thông tin là của người mua hàng ở Hoa Kỳ. Canada đứng thứ 2 với tỉ lệ 15.7%, tiếp theo là Đức với tỉ lệ 6.8% và Hà Lan với tỉ lệ 6.4%.

Các chuyên gia cho rằng hoạt động này do một mạng lưới có tên là Magecart gồm nhiều nhóm tấn công mạng thực hiện. Magecart thường sử dụng "web skimmers" (công cụ để lấy cắp thông tin thanh toán trên các trang web) để đánh cắp thông tin thẻ tín dụng của khách hàng. Mạng lưới này hoạt động mạnh từ đầu năm. Tháng 1/2019, một nhóm tội phạm mạng Magecart đã sử dụng một tập lệnh độc hại gây tổn hại cho hàng trăm trang web thương mại điện tử. Hai tháng sau, các nhà nghiên cứu phát hiện các đối tượng Magecart sử dụng cùng một skimmer tương tự với nhà cung cấp nền tảng web.

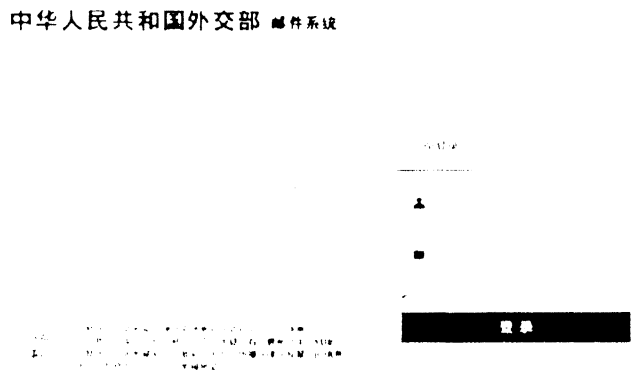
Trước sự phát triển không ngừng của các web skimmer, các cơ quan, tổ chức, doanh nghiệp có thể đóng góp vào việc chống lại các đối tượng tấn công này bằng cách gửi các báo cáo tới cơ quan chức năng và các doanh nghiệp nghiên cứu, phát triển sản phẩm, dịch vụ an toàn thông tin khi các trang web bị có dấu hiệu bị tấn công. Còn đối với người dùng, nên cẩn trọng khi sử dụng thông tin thẻ tín dụng trên các nền tảng trực tuyến. Ngoài ra, người dùng cần duy trì giải pháp phòng, chống phần mềm độc hại được cập nhật thường xuyên trên máy tính cũng như điện thoại thông minh dùng để mua hàng trực tuyến.

1.2. Thông tin cử tri của hơn 14.3 triệu người Chile (chiếm gần 80% toàn bộ dân số của đất nước này), đã bị lộ, lọt trên mạng. Các thông tin này được lưu trữ trong một cơ sở dữ liệu Elasticsearch (Elasticsearch - công cụ tìm kiếm trên nền tảng Apache Lucene). Cục An toàn thông tin đã cảnh báo về việc máy chủ của Elaticsearch bị tấn công nhằm mục đích phát tán phần mềm độc hại tại Báo cáo tóm tắt tình hình an toàn thông tin đáng chú ý tuần 30/2019.

Cơ sở dữ liệu bị lộ, lọt chứa tên, địa chỉ nhà, giới tính, tuổi và mã số thuế của 14.308.151 người dân. Các nhà nghiên cứu đã xác nhận tính chính xác của thông tin này với một số cá nhân có dữ liệu bị lộ, lọt. Người phát ngôn của cơ quan dịch vụ bầu cử Chile (Chile's Electoral Service) cũng đã xác nhận tính xác thực của dữ liệu, tuy nhiên, lại phủ nhận việc sở hữu máy chủ lưu trữ cơ sở dữ liệu bị lộ, lọt thông tin. Cơ quan này cho biết họ được giao nhiệm vụ theo luật của Chile để cập nhật dữ liệu và cung cấp giao diện thông qua đó cử tri có thể xác minh tính hợp lệ hoặc cập nhật thông tin cử tri của họ. Điều này có thể được thực hiện thông qua các ứng dụng di

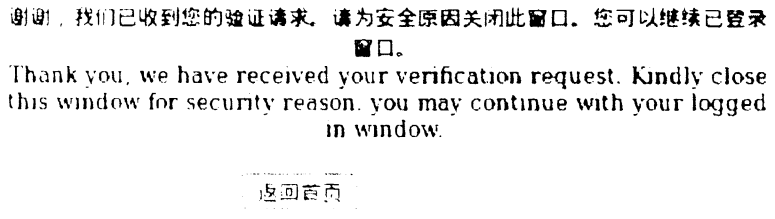
động hoặc trang web. Cơ quan dịch vụ bầu cử Chile cho rằng đối tượng đã khai thác thông tin này từ trang web và sau đó tập hợp nó vào một cơ sở dữ liệu và phát tán lên mạng.

1.3. Theo các nhà nghiên cứu của Anomali đã xác định một trang web giả mạo được thiết kế giống như trang đăng nhập email của Bộ Ngoại giao Trung Quốc. Sau khi điều tra, họ cũng đã phát hiện hơn 40 trang web giả mạo khác cũng nhằm mục tiêu vào chính phủ và các tổ chức khác ở Trung Quốc. Tất cả các trang web đều sử dụng chứng thư số của **Let's Encrypt** để vượt qua các cảnh báo của trình duyệt và có quy ước đặt tên, chủ yếu nhằm vào những trang đăng nhập tài khoản trực tuyến và xác thực tài khoản.

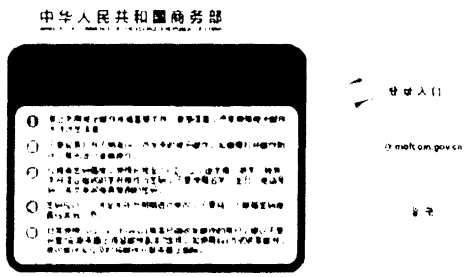


Hình 1 - Trang web lừa đảo nhắm mục tiêu Bộ Ngoại giao

Trang web giả mạo được thiết kế đặc biệt để giả mạo trang đăng nhập cho Bộ ngoại giao Trung Quốc nhằm đánh cắp thông tin email, khi người dùng nhập thông tin đăng nhập của họ.



Hình 2 - Thông báo sau khi người dùng đăng nhập vào trang web



Hình 3 - Trang web lừa đảo nhắm mục tiêu Bộ thương mại Trung Quốc

Ngoài ra, trong quá trình điều tra và phân tích những nhà nghiên cứu đã xác định 06 tên miền và hơn 40 tên miền con mạo danh các trang web của chính phủ và doanh nghiệp ở Trung quốc bao gồm:

- 04 cơ quan chính phủ Trung Quốc
- 06 doanh nghiệp nhà nước
- 01 tổ chức đấu giá có trụ sở tại Hồng Kông
- 02 nhà cung cấp dịch vụ email (NetEase Inc. và Gmail)

Mỗi trang web mạo danh đều chứa một cấu trúc đặt tên tương tự, có thể là dấu hiệu của cùng một nhóm tội phạm mạng thực hiện chiến dịch lừa đảo này: Cấu trúc đặt tên gồm:

- Một chuỗi ngẫu nhiên các chữ cái và số.
- Kết thúc với tên miền độc hại.
- Một hoặc hai ký tự "l" được đưa thêm vào Email.
- Tên miền hợp pháp của mục tiêu tấn công.
- Biến thể của các từ "acountvalidation" và "verify"

Thông tin chi tiết về các tên miền độc hại này xem chi tiết tại http://ti.khonggianmang.vn/

Việc giả mạo các trang web để thu thập thông tin tài khoản người dùng đã được đối tượng tấn công sử dụng từ lâu, tuy nhiên đến nay vẫn tiếp tục được tội phạm mạng ưa thích sử dụng, điều đó cho thấy vẫn còn hiệu quả do rất nhiều người dùng chưa có khả năng phân biệt được trang web chính thống và trang web giả mạo. Do vậy các cơ quan tổ chức cung cấp dịch vụ cho người dùng đặc biệt là những tổ chức cung cấp dịch vụ liên quan đến tài chính, ngân hàng bên cạnh việc chú trọng các biện pháp kỹ thuật cần phải có những biện pháp phi kỹ thuật để bảo vệ cũng như

hỗ trợ, nâng cao nhận thức cho người dùng sử dụng sản phẩm dịch vụ của mình trước các nguy cơ lừa đảo.

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 445 lỗ hổng, trong đó có 20 lỗ hổng mức cao, 98 lỗ hổng mức trung bình, 71 lỗ hổng mức thấp và 256 lỗ hổng chưa đánh giá. Trong đó có ít nhất 57 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 117 lỗ hổng trên phần mềm Cpanel; Nhóm 71 lỗ hổng trên Magento; Nhóm 03 lỗ hổng trên phần mềm Jira, 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	Cpanel	CVE-2017-18386 CVE-2017-18460 CVE-2017-18474	Nhóm 117 lỗ hổng trên Cpanel cho phép đối tượng tấn công chèn và thực thi mã lệnh độc hại qua nhiều thành phần khác nhau (PostgreSQL, SQLite, /scripts/maildir_converter, BoxTrapper API...). Việt Nam có ít nhất 210 máy chủ Cpanel đang công khai trên Internet. Cục ATTT cũng đã cảnh báo 249 lỗ hổng của Cpanel trong tuần 31.	Đã có thông tin xác nhận và bản vá
2	Magento	CVE-2019-7890 CVE-2019-7930 CVE-2019-7851	Nhóm 71 lỗ hổng trên Magento (nền tảng nguồn mở hỗ trợ xây dựng website thương mại điện tử) cho phép truy cập trái phép	Đã có thông tin xác nhận và bản vá

		...	vào hệ thống, khai thác lỗi file update để cài cắm mã độc trên hệ thống. Lỗ hổng CVE-2019-7930 có điểm CVSS là 9.0	
3	OpenEMR	CVE-2019-14529	Lỗ hổng trên OpenEMR cho phép đối tượng tấn công khai thác lỗi SQL Injection thông qua /forms/eye_mag/save.php. OpenEMR là phần mềm quản lý hồ sơ sử dụng trong lĩnh vực y tế, nếu ứng dụng này bị khai thác thì có thể gây ra các vụ lộ lọt thông tin của bệnh nhân tại các bệnh viện.	Đã có phương án khắc phục
4	D-Link	CVE-2019-6968 CVE-2019-6969	Nhóm 02 lỗ hổng trên firmware của thiết bị D-Link DVA-5592 20180823 cho phép khai thác lỗi XSS, truy cập trái phép vào thiết bị để lấy thông tin như mật khẩu Wi-Fi, số điện thoại (nếu sử dụng VoIP)	Đã có thông tin xác nhận và bản vá
5	Jira	CVE-2018-20826 CVE-2018-20827 CVE-2019-11581	Nhóm 03 lỗ hổng trên phần mềm quản lý dự án Jira cho phép đối tượng tấn công khai thác lỗi XSS, chèn và thực thi mã lệnh trên hệ thống. Có 22 máy chủ của Việt Nam đang public trên Internet có sử dụng Jira. Lỗ hổng CVE-2019-11581 đã được Cục ATTT cảnh báo trực tiếp đến 1 số đơn vị đang có máy chủ Jira bị ảnh	Đã có thông tin xác nhận bản vá.

			hưởng từ 23/7/2019.	
6	Cisco	CVE-2019-1971 CVE-2019-1910 CVE-2019-1918 ...	Nhóm 32 lỗ hổng trên một số sản phẩm ứng dụng của Cisco (NFVIS, IOS XR Software, Firepower Threat Defense software, IoT Field Network Director, Small Business 220 Series Smart Switches...) cho phép đối tượng tấn công thực hiện tấn công từ chối dịch vụ, khai thác lỗi XSS, CSRF, chèn và thực thi mã lệnh, 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.

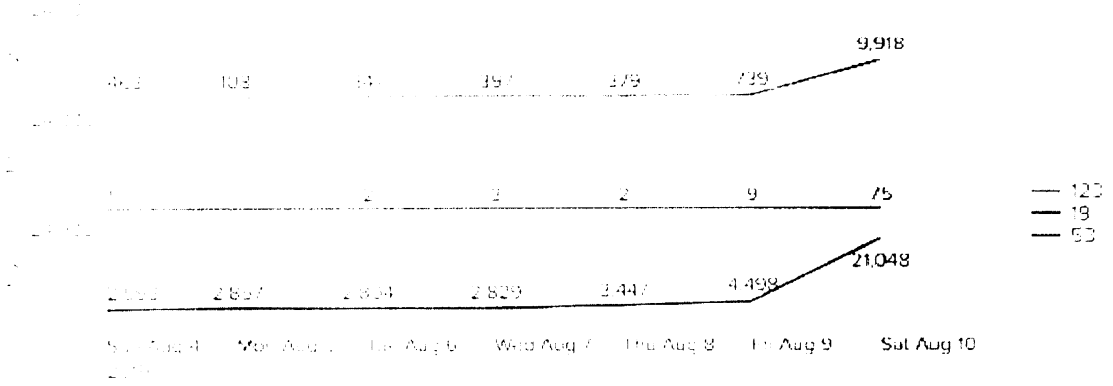
Tấn công từ chối dịch vụ có thể được thực hiện với nhiều kỹ thuật khác nhau, nhưng trong những năm gần đây phần lớn tin tặc huy động các thiết bị đang mở cổng dịch vụ sử dụng giao thức UDP để thực hiện tấn công. Các thiết bị này có thể bị huy động dễ dàng để thực hiện tấn công DRDoS (tấn công từ chối 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

Giao thức	Số lần khuếch đại băng thông
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 **52,518 (tăng so với tuần trước là 50,428)** 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.

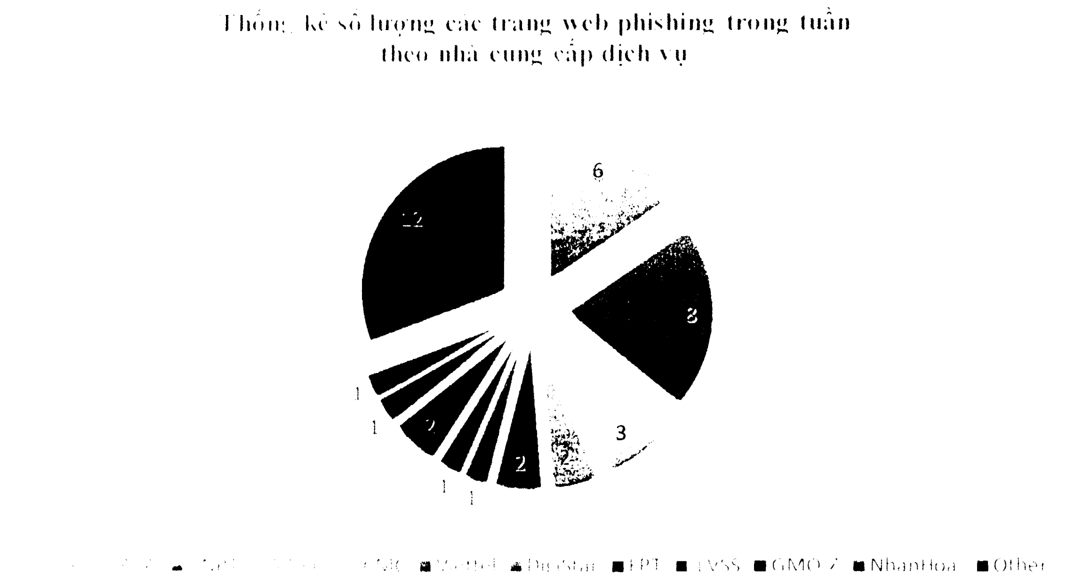
Biểu đồ thống kê thiết bị theo cổng dịch vụ phổ biến



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 466 trường hợp tấn công vào trang/cổng thông tin điện tử của Việt Nam: 09 trường hợp tấn công thay đổi giao diện, 39 trường hợp tấn công lừa đảo (Phishing), 419 trường hợp tấn công cài cắm mã độc.

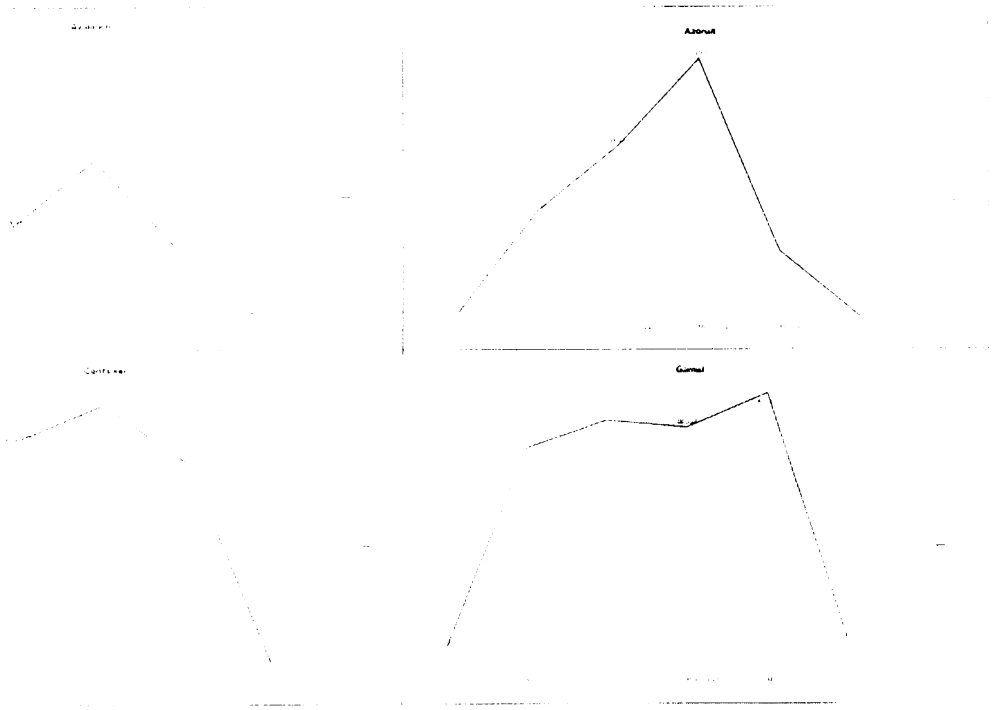


5. Hoạt động của mạng botnet, APT, mã độc tại Việt Nam

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:

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 có giảm so với tuần trước, có 306.155 lượt địa chỉ IP kết nối với máy chủ điều khiển (Tuần 31 là 687.285).

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

TT	Tên miền/IP
1	n.hmiblgoja.ru
2	mel.cloudcontentsmak.com
3	mokoaehaeihgiaheih.ru
4	realhotchickss.com
5	ajkeahkcueafuiaeuf.ru
6	pradanewstyle.com
7	bszotsjovih.com
8	strikotunrev.top
9	letstryitnowx.online
10	willem@alternativa.nl:444134
11	estellavw11@tango.whiskey.ezbunko.top:x4ivyga51f
12	camiam2@villager.co.uk:iluvme1

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