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 29 (từ 15/07 - 21/07/2019)

Số: /BC-CATTT *Hà Nội, ngày 23 tháng 07 năm 2019*

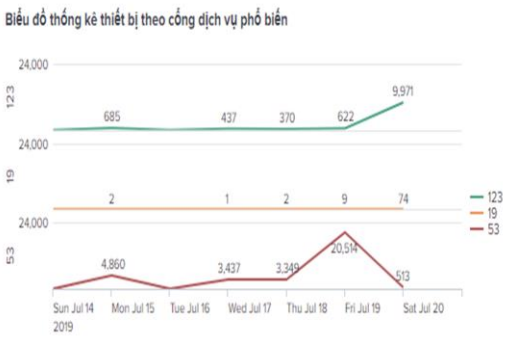
HỘI NGHỊ THƯỜNG NIÊN THỊ TRƯỞNG HOA KỲ

Tại cuộc họp thường niên của Hội nghị thị trưởng Hoa Kỳ, hơn 225 thị trưởng đã ủng hộ nghị quyết không trả tiền chuộc cho đối tượng tấn công mạng trong các cuộc tấn công bằng mã độc tống tiền Ransomware. Nghị quyết với tiêu đề "Phản đối thanh toán cho các đối tượng tấn công tống tiền - Opposing Payment To Ransomeware Attack Perpetrators".

PHẦN MỀM GIÁN ĐIỆP MỚI EVILGNOME TRÊN LINUX DESKTOP

Nhóm chuyên gia bảo mật của Intezer Labs gần đây đã phát hiện ra backdoor Linux mới- EvilGnome chưa bị bất kỳ sản phẩm phòng chống mã độc nào phát hiện.

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 346 lỗ hổng, trong đó có 61 lỗ hổng mức cao, 101 lỗ hổng mức trung bình, 28 lỗ hổng mức thấp và 156 lỗ hổng chưa đánh giá. Trong đó có ít nhất 28 lỗ hổng cho phép chèn và thực thi mã lệnh.

HÃNG HÀNG KHÔNG QUỐC TẾ BRITISH AIRWAYS VI PHẠM DỮ LIỆU THÔNG TIN

Hãng hàng không quốc tế British Airways của Anh đối mặt với mức phạt kỷ lục 183 triệu bảng vì vi phạm dữ liệu theo thông tin từ Văn phòng Ủy ban thông tin (ICO). ICO cho biết đây là hình phạt lớn nhất mà họ đã đưa ra và là lần đầu tiên được công khai.

1. Điểm tin đáng chú ý

1.1. Tại cuộc họp thường niên của Hội nghị thị trưởng Hoa Kỳ, hơn 225 thị trưởng đã ủng hộ nghị quyết không trả tiền chuộc cho đối tượng tấn công mạng trong các cuộc tấn công bằng mã độc tống tiền Ransomware. Nghị quyết với tiêu đề "Phản đối thanh toán cho các đối tượng tấn công tống tiền - Opposing Payment To Ransomeware Attack Perpetrators".

Nghị quyết được đưa ra sau khi gần 20 thành phố bị tấn công bằng mã độc tống tiền ransomware trong năm nay. Một số thành phố như Lake City, Florida đã thanh toán khoảng 43 bitcoin cho một đối tượng tấn công để lấy lại quyền truy cập vào hệ thống điện thoại và thư điện tử. Một cuộc tấn công gần đây nhất vào thành phố Baltimore hồi tháng 5 thông qua 1 email lừa đảo, đã khiến các hệ thống thiết yếu của thành phố này bị ngưng trệ. Đối tượng tấn công yêu cầu 13 bitcoin (khoảng 76.280 USD vào thời điểm đó). Tuy nhiên, lãnh đạo thành phố này được cho rằng đã không trả tiền chuộc theo yêu cầu với quan điểm là việc trả tiền chuộc chỉ mang lại động lực cho nhiều người tham gia vào loại hành vi bất hợp pháp này. Ước tính rằng cuộc tấn công đã tiêu tốn của thành phố ít nhất 18 triệu USD.

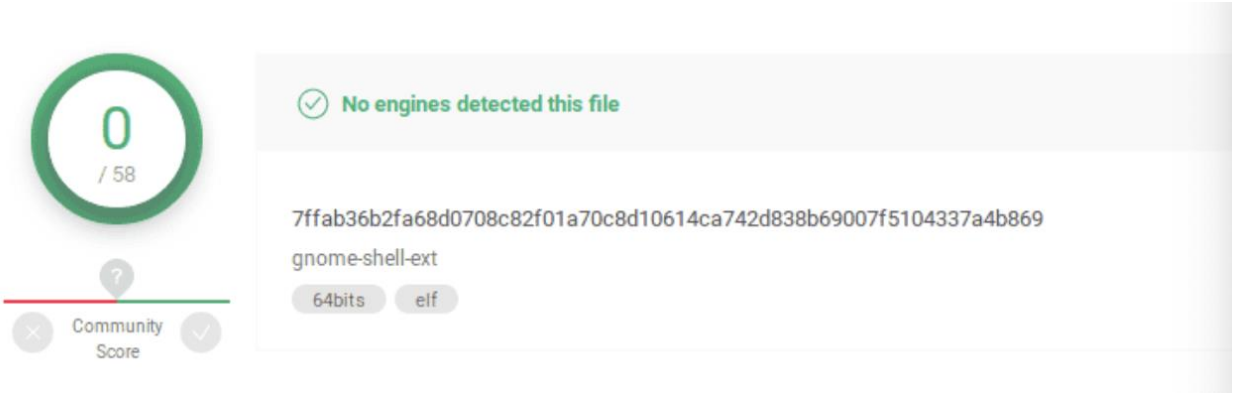
1.2. Hãng hàng không quốc tế British Airways của Anh đối mặt với mức phạt kỷ lục 183 triệu bảng vì vi phạm dữ liệu theo thông tin từ Văn phòn Ủy ban thông tin (ICO). ICO cho biết đây là hình phạt lớn nhất mà họ đã đưa ra và là lần đầu tiên được công khai. Mức phạt này áp dụng với British Airways do vụ việc xảy ra vào năm 2018, khi người dùng trang web của British Airways bị chuyển hướng đến một trang web lừa đảo. Thông qua trang web giả mạo này, thông tin chi tiết về khoảng 500.000 khách hàng đã bị đối tượng tấn công thu thập (***tham khảo thêm tại báo cáo tình hình an toàn thông tin đáng chú ý trong tuần 36/2018***).

Hình phạt áp dụng đối với British Airways là hình phạt đầu tiên được công khai kể từ khi Quy định bảo vệ dữ liệu chung (GDPR) của EU có hiệu lực. Theo GDPR mức phạt tối đa đối với các vụ việc liên quan tới vi phạm dữ liệu có thể lên đến 4% doanh thu toàn cầu. Mức phạt áp dụng với British Airways đang là 1.5% doanh thu trên toàn thế giới trong năm 2017 của hãng hàng không này, thấp hơn khá nhiều mức tối đa có thể áp dụng.

1.3. Nhóm chuyên gia bảo mật của Intezer Labs gần đây đã phát hiện ra backdoor Linux mới - EvilGnome đang trong giai đoạn phát triển và thử nghiệm nhưng đã bao gồm một số mô-đun độc hại theo dõi người dùng hệ điều hành Linux. Mã độc hại chưa bị bất kỳ sản phẩm phòng chống mã độc nào phát hiện.

Phần mềm độc hại này có tên EvilGnome, được thiết kế để chụp ảnh màn hình máy tính, đánh cắp tệp tin, ghi lại âm thanh từ micro của người dùng cũng như tải xuống và thực hiện các mô-đun độc hại khác.

Theo Interzer Labs thì mẫu mã độc tìm thấy trên VirusTotal có chức năng keylogger chưa hoàn chỉnh, và có thể do nhà phát triển tải lên nhầm.




```
paul@ubuntu:~$ ./spy-agent-setup-linux.run --info
Identification: setup files...
Target directory: spy-agent
Uncompressed size: 248 KB
Compression: gzip
Date of packaging: Thu Jul 4 12:51:00 MSK 2019
Built with Makeself version 2.3.0 on
Build command was: /usr/bin/makeself \
    "--notemp" \
    "/media/data/work/Rostov/spy/spy-source/spy-agent/../../spy-build/Linux/spy-agent" \
    "/media/data/work/Rostov/spy/spy-source/spy-agent/../../spy-binary/Linux/spy-agent-setup-linux.run"
    "setup files..." \
    "./setup.sh"
Script run after extraction:
    ./setup.sh
directory spy-agent is permanent
```

EvilGnome giả mạo gói phần mềm Gnome - chương trình cung cấp giao diện cho các hệ điều hành Linux. EvilGnome được phân phối dưới dạng một tập tin shell gnome-shell-ext.sh (tạo bằng makeself) và tạo cronjob để chạy theo phút.

Phần mềm độc hại này sử dụng các mô-đun để thực thi. Thành phần gián điệp của EvilGnome gồm 05 mô-đun độc hại gọi là Shooters như sau:

- ShooterSound: mô-đun này sử dụng PulseAudio để thu âm thanh từ micro của người dùng và tải dữ liệu lên máy chủ điều khiển (C&C).

- ShooterImage: mô-đun này sử dụng thư viện mã nguồn mở Cairo để chụp ảnh màn hình và tải chúng lên máy chủ C&C. Mô-đun này hoạt động bằng cách mở kết nối đến Xorg Display Server.

- ShooterFile: mô-đun này sử dụng danh sách bộ lọc để quét hệ thống tệp tin để tìm file mới được tạo và tải chúng lên máy chủ C&C.

- ShooterPing: mô-đun nhận các lệnh mới từ máy chủ C&C, như tải xuống và thực thi mã độc mới, đặt các bộ lọc mới để quét tệp, tải xuống và đặt cấu hình thời

gian chạy mới, lọc dữ liệu đầu ra để đưa lên máy chủ C&C hay dừng việc thực thi mô-đun khác.

- ShooterKey: mô-đun này không được thực hiện và không được sử dụng, rất có thể là mô-đun keylogging chưa hoàn thiện.

Đáng chú ý, tất cả toàn bộ mô-đun trên đều mã hóa dữ liệu đầu ra và giải mã các lệnh nhận được từ máy chủ C&C bằng khoá RC5 "sdg62_AS.sa $ die3", sử dụng phiên bản sửa đổi của thư viện nguồn mở của Nga.

Ngoài ra, các nhà nghiên cứu cũng tìm thấy mối liên hệ giữa EvilGnome và Gamaredon Group, một nhóm tấn công mạng của Nga đã hoạt động ít nhất từ năm 2013 và đã nhằm vào nhiều cá nhân làm việc với chính phủ Ukraine. Dưới đây là một số điểm tương đồng giữa EvilGnome và Gamaredon Group:

- Sử dụng cùng một nhà cung cấp dịch vụ lưu trữ;

- EvilGnome cũng hoạt động trên địa chỉ IP từng được kiểm soát bởi nhóm Gamaredon hai tháng trước.

- EvilGnome cũng đang sử dụng tên miền '.space' giống như Nhóm Gamaredon.

- EvilGnome sử dụng các kỹ thuật và mô-đun, giống như việc sử dụng SFX, lập lịch tác vụ và triển khai các công cụ đánh cắp thông tin tương tự Gamaredon Group.

Các nhà nghiên cứu cũng khuyên người dùng, quản trị viên nên kiểm tra hệ thống của mình có bị nhiễm phần mềm gián điệp EvilGnome bằng cách tìm thực thi **"gnome-shell-ext" trong thư mục "~ / .cache / gnome-software / gnome-shell-extend"**.

Ngoài ra, do các sản phẩm chống vi-rút và bảo mật hiện không phát hiện được phần mềm độc hại EvilGnome, các nhà nghiên cứu khuyên các quản trị viên Linux có liên quan nên chặn các địa chỉ điều khiển đã được chỉ ra.

Thông tin kỹ thuật về mã độc EvilGnome tham khảo thêm tại:

https://ti.khonggianmang.vn/dashboard/news/p/Phan-mem-gian-diep-moi-EvilGnome-tren-Linux-Desktop/

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 346 lỗ hổng, trong đó có 61 lỗ hổng mức cao, 101 lỗ hổng mức trung bình, 28 lỗ hổng mức thấp

và 156 lỗ hổng chưa đánh giá. Trong đó có ít nhất 28 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 77 lỗ hổng trong một số sản phẩm của Microsoft; Nhóm 11 lỗ hổng trên sản phẩm, phần mềm Adobe; Nhóm 08 lỗ hổng trên sản phẩm của Cisco, nhóm 03 lỗ hổng trên plugin của 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	Microsoft	CVE-2019-1001 CVE-2019-1092 CVE-2019-1104 ….	Nhóm 77 lỗ hổng trên một số sản phẩm, phần mềm của Microsoft (Chakracore, Edge, Office, IE, Windows 10, Windows 7, Windows Server 2012...) cho phép đối tượng tấn công chèn và thực thi mã lệnh từ xa, tấn công leo thang.	Đã có thông tin xác nhận và bản vá
2	Adobe	CVE-2019-7850 CVE-2019-7843 CVE-2019-7847 …..	Nhóm 11 lỗ hổng trên một số sản phẩm của Adobe (Campaign Classic, Bridge CC Dreamweaver, Experience Manager) cho phép đối tượng tấn công chèn và thực thi lệnh độc hại, thu thập thông tin nhạy cảm	Đã có thông tin xác nhận và bản vá
3	Centos Webpanel	CVE-2019-13359 CVE-2019-13383 CVE-2019-13605 ...	Nhóm 08 lỗ hổng trên CentOS Web Panel cho phép nwgoiwf dùng tải tập tin tùy ý lên thư mục /tmp, truy cập trái phép vào hệ thống với quyền của người dùng thông	Chưa có thông tin xác nhận và bản vá

			thường mà không cần xác thực, tìm kiếm người dùng có trên hệ thống.	
4	IBM	CVE-2019-4194 CVE-2019-4430 CVE-2018-2021	Nhóm 07 lỗ hổng trên một số sản phẩm của IBM (IBM Campaign, QRadar SIEM, IBM Jazz, IBM Maximo Asset Management) cho phép đối tượng tấn công khai thác lỗi Path Traverse để truy cập trái phép vào tập tin trên hệ thống, lỗi XSS thực thi các đoạn mã Java, thu thập thông tin nhạy cảm,	Đã có thông tin xác nhận và bản vá
5	Cisco	CVE-2019-1873 CVE-2019-1932 CVE-2019-1921 ...	Nhóm 08 lỗ hổng trên một số sản phẩm, ứng dụng của Cisco (IOS Access Points, Small Business Switches, FindIT Network Management Software, Identity Services Engine, Industrial Network Director) cho phép đối tượng tấn công truy cập vào giao diện console của thiết bị với quyền Root, khai thác lỗi SQL InjectionCentOS Web Panel, XSS, chuyển hướng người dùng đến trang web độc hại, một số lỗi cho phép thực thi hàng động trái phép thông qua REST APT,	Đã có thông tin xác nhận và bản vá
6	Tp-link	CVE-2019-13613	02 Lỗ hổng trên thiết bị TP-Link Wireless Router Archer Router và TP-Link Archer C1200 cho phép khai thác lỗi	Chưa có thông tin xác nhận và bản vá

			tràn bộ đệm để thực thi ma lệnh.	
7	Wordpress	CVE-2019-1010104 CVE-2019-13569 CVE-2019-12934	Nhóm 03 lỗ hổng trên một số plugin của Wordpress (TechyTalk Quick Chat, Email Subscribers & Newsletters, wp-code-highlightjs) cho phép khai thác lỗi SQL Injection, XSS.	Chưa có thông tin xác nhận và bản vá

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

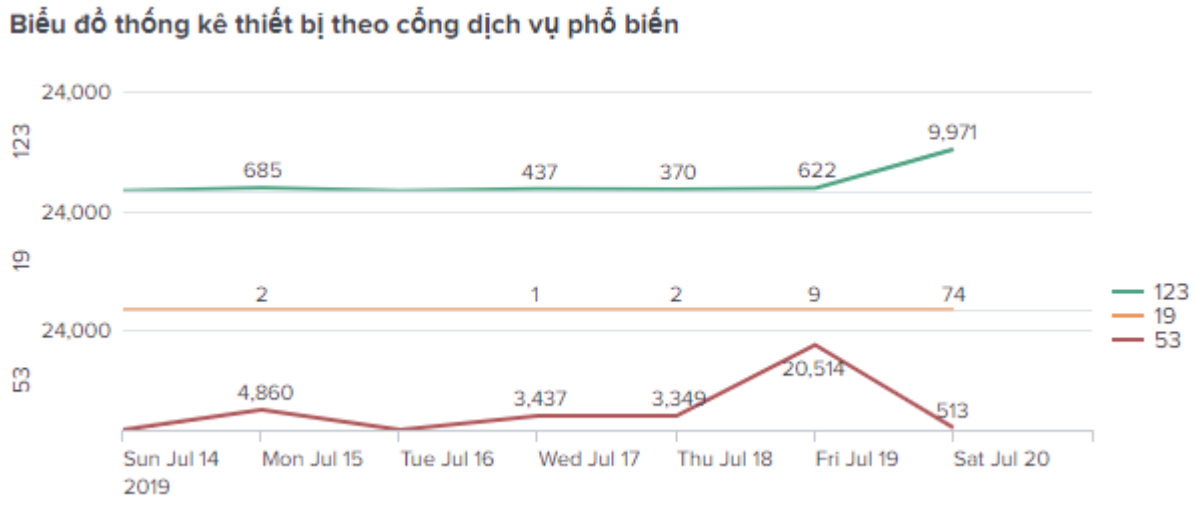
Tấn công từ chối dịch vụ là hình thức tấn công đã có từ lâu, và hiện tại vẫn được đối tượng tấn công ưa thích sử dụng để thực hiện các ý đồ xấu. Tấn công từ chối dịch vụ về cơ bản không nguy hiểm nhưng lại gây ảnh hưởng đến hoạt động của hệ thống, gây thiệt hại về kinh tế cho tổ chức bị tấn công.

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

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

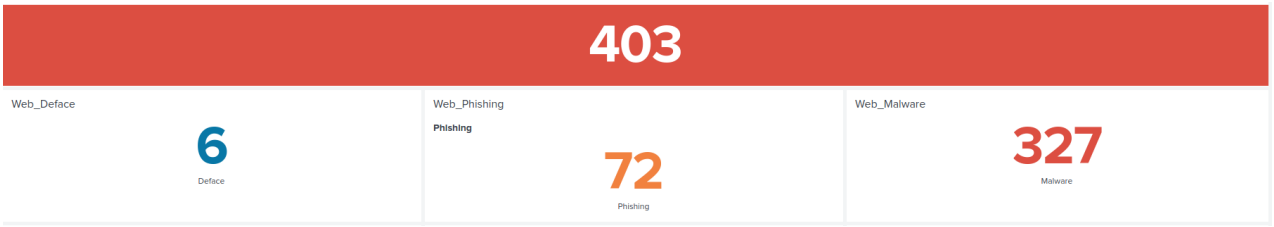
Tại Việt Nam, có rất nhiều máy chủ, thiết bị có thể trở thành nguồn phát tán tấn công DRDoS. Trong tuần có **44,927 (tăng so với tuần trước là 34,915)** thiết bị có khả năng bị huy động và trở thành nguồn tấn công DRDoS. Các thiết bị này đang mở sử dụng các dịch vụ NTP (123), DNS (53), Chargen (19). Dưới đây là biểu đồ thống kê thiết bị theo cổng dịch vụ phổ biến trong tuần.

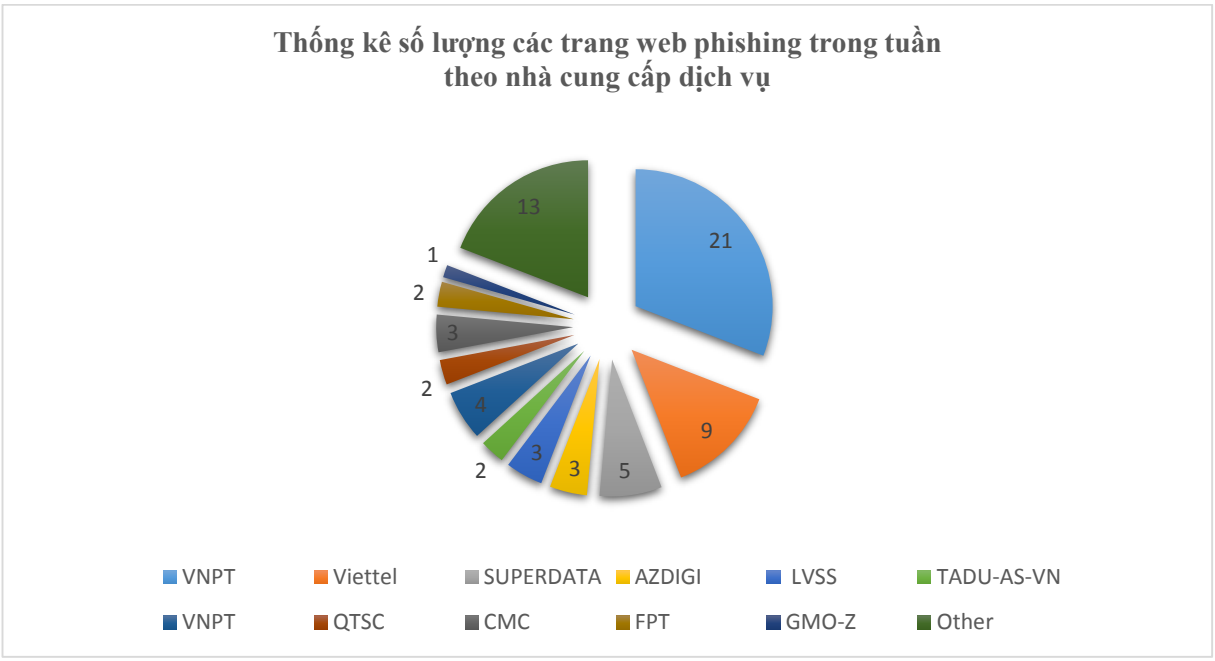


4. Tấn công vào Cổng TTĐT/ứng dụng web của Việt Nam

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 403 trường hợp tấn công vào trang/cổng thông tin điện tử của Việt Nam: 06 trường hợp tấn công thay đổi giao diện, 72 trường hợp tấn công lừa đảo (Phishing), 327 trường hợp tấn công cài cắm mã độc.

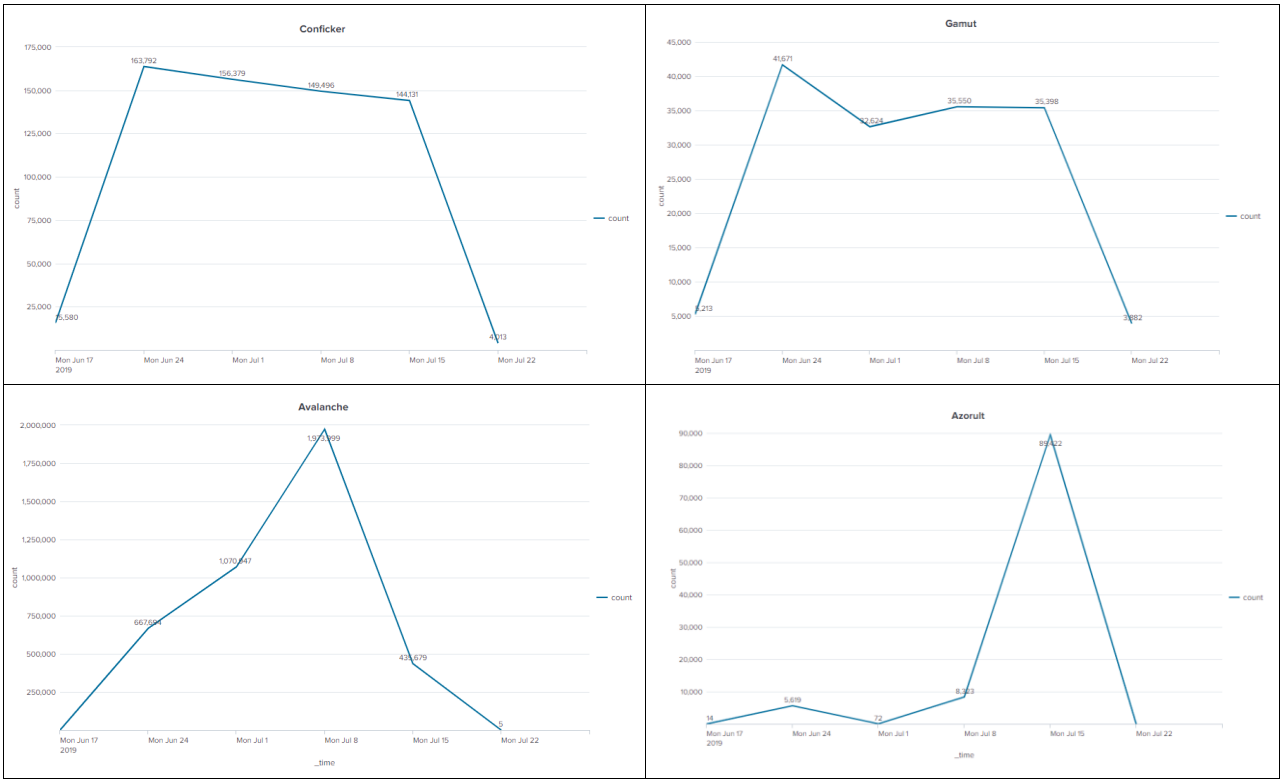




5. Hoạt động của mạng botnet, APT, mã độc tại Việt Nam

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 tuy nhiên có giảm so với tuần trước, có 435.679 lượt địa chỉ IP kết nối với máy chủ điều khiển (Tuần 28 là 565.309).

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	mokoaehaeihgiaheih.ru
3	produkktc.com
4	mel.cloudcontentsmak.com
5	and30.blabladomdom.com
6	ajkeahkcueafuiaeuf.ru
7	dghfhfgjfhjghj6699.net
8	and28.aviationdreamflightering1.com
9	https://realhotchickss.com/xefyzznumsa
10	bszotsjovih.com
11	and31.amainwrorldnancy4.com
12	and12.thesuchivestfishmarketeat111.com

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