BỘ THÔNG TIN VÀ TRUYỀN THÔNG
CỤC AN TOÀN THÔNG TIN

CỘNG HÒA XÃ HỘI CHỦ NGHĨA VIỆT NAM
Độc lập - Tự do - Hạnh phúc

Số: /BC-CATTT

Hà Nội, ngày tháng 02 năm 2019

TÓM TẮT
Tình hình an toàn thông tin đáng chú ý trong tuần 08/2019
(từ ngày 18/02/2019 đến ngày 24/02/2019)

BẢNG TỔNG HỢP

1. Sân bay Sydney chuẩn bị mở một Trung tâm điều hành an toàn, an ninh mạng (SOC) để giảm thiểu rủi ro ngày càng tăng của các mối đe dọa vi phạm dữ liệu và thông tin. Giai đoạn đầu tiên của Trung tâm SOC dự kiến sẽ được hoàn thành vào tháng 4/2019.

2. Israel cung cấp một đường dây nóng (hotline) với mục đích cung cấp trợ giúp cho các cơ quan, tổ chức và người dân gặp phải vấn đề liên quan tới tấn công mạng. Cơ quan, tổ chức, doanh nghiệp và cá nhân có thể báo cáo về các điểm yếu, lỗ hổng an toàn thông tin đáng ngờ và nhận được giải pháp hỗ trợ thông qua đường dây nóng. Đây là mô hình đầu tiên trên thế giới về tổng đài an toàn thông tin, được tạo ra bởi Israel.

3. Trickbot - một loại Banking Trojan đã được sử dụng một thời gian khá dài để tấn công nhiều tổ chức ngân hàng, tài chính trên thế giới. Vào khoảng thời gian tháng 11 năm 2018 đã có nhiều phân tích đề cập đến biến thể mới của Trickbot đi kèm theo thành phần đánh cắp mật khẩu (pwgrab).

4. Báo cáo được xây dựng dựa trên các nguồn thông tin thu thập được từ hệ thống phân tích và chia sẻ nguy cơ tấn công mạng Việt Nam (https://ti.khonggianmang.vn). Thông tin chi tiết về Hệ thống tại *Phụ lục kèm theo*.

1. Điểm tin đáng chú ý

1.1. Sân bay Sydney đang chuẩn bị mở một Trung tâm điều hành an toàn, an ninh mạng (SOC) để giảm thiểu rủi ro ngày càng tăng của các mối đe dọa vi phạm dữ liệu và thông tin. Giai đoạn đầu tiên của Trung tâm SOC dự kiến sẽ được hoàn thành vào tháng 4/2019.

Điều này cho thấy chính phủ Australia ngày càng chú ý tới các vấn đề an toàn, an ninh mạng và coi các cuộc tấn công mạng là một mối đe dọa chính tới hoạt động của sân bay cùng với các mối đe dọa khác như tai nạn máy bay, khủng bố, biến đổi khí hậu và mối đe dọa chiến tranh.

Sân bay Sydney hiện đang hợp tác chặt chẽ với chính phủ Australia về an ninh mạng thông qua Trung tâm an ninh mạng chung (JCSC) và cũng đang làm việc với Trung tâm phân tích và chia sẻ thông tin hàng không (ISAC) về tình báo an toàn, an ninh mạng hàng không toàn cầu. Sân bay Sydney sẽ tiếp tục đầu tư vào công nghệ trong năm nay để tăng trải nghiệm của khách hàng cũng như khả năng phục hồi hệ thống và quản lý rủi ro mạng. Việc nâng cấp khả năng phục hồi của hệ thống và SOC ngày càng trở nên quan trọng khi sân bay tiếp tục chuyển sang sử dụng các quy trình tự động và kết nối với nhau.

1.2. Israel cung cấp một đường dây nóng (hotline) với mục đích cung cấp trợ giúp cho các cơ quan, tổ chức và người dẫn gặp phải vấn đề liên quan tới tấn công mạng. Các cơ quan, tổ chức, doanh nghiệp và cá nhân có thể báo cáo về các điểm yếu, lỗ hổng an toàn thông tin đáng ngờ và nhận được giải pháp hỗ trợ thông qua đường dây nóng. Đây là mô hình đầu tiên trên thế giới về tổng đài an toàn thông tin, được tạo ra bởi Israel.

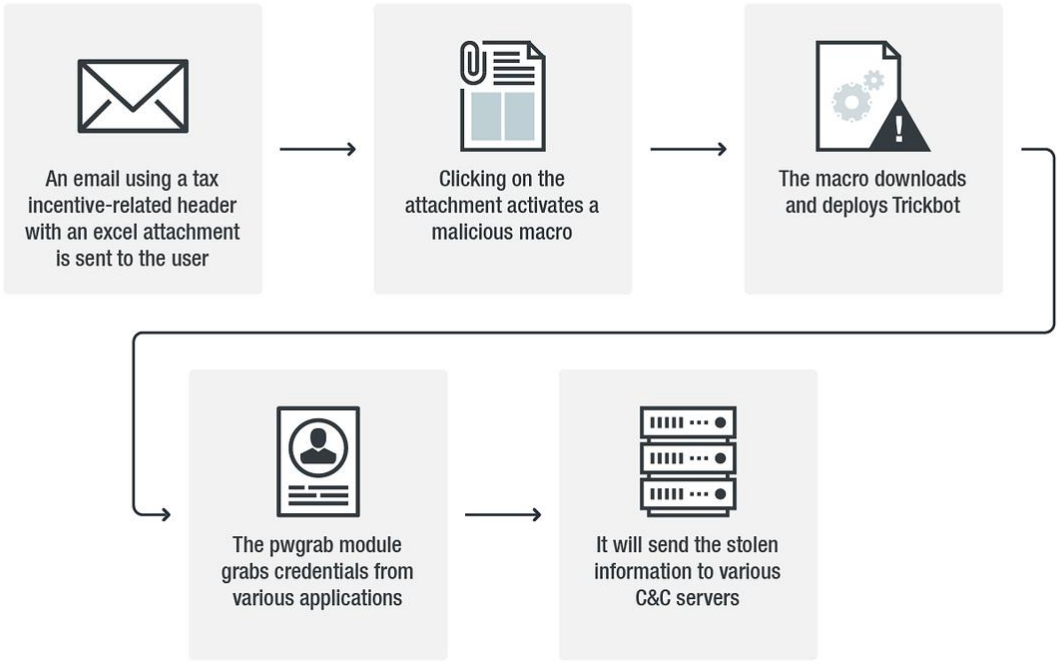
Mục đích hotline này là giảm thiểu thiệt hại nhanh nhất có thể, tìm hiểu về các mối đe dọa và phổ biến kiến thức liên quan đến bảo đảm an toàn thông tin. Một cuộc tấn công mạng có thể không chỉ giới hạn ở thiệt hại tài sản hoặc tài chính. Nó cũng có thể gây đe dọa đến tính mạng. Trong một số trường hợp cơ quan chức năng sẽ cử các nhóm chuyên gia đến hỗ trợ người dùng máy tính bị ảnh hưởng sau một vài giờ kể từ khi nhận được thông báo.

Hotline này hiện này nhận được khoảng 100 cuộc gọi hàng ngày. Khoảng 15% người gọi là "hacker mũ trắng" báo cáo về những điểm yếu, lỗ hổng trong các hệ thống của doanh nghiệp hoặc chính phủ và đề nghị xử lý trước khi các hệ thống này có thể bị tấn công.

1.3. Trickbot - một loại Banking Trojan đã được sử dụng một thời gian khá dài để tấn công nhiều tổ chức ngân hàng, tài chính trên thế giới. Vào khoảng thời gian tháng 11 năm 2018 đã có nhiều phân tích đề cập đến biến thể mới của Trickbot đi kèm theo thành phần đánh cắp mật khẩu (pwgrab), cho phép đánh cắp thông tin từ nhiều ứng dụng (như Microsoft Outlook, Filezilla, WinSCP, Google Chrome, Mozilla Firefox, Internet Explorer, Microsoft Edge). Vào cuối tháng 1 năm 2019 những báo cáo mới cho thấy thành phần mới này (pwgrab)

còn cho phép lấy thông tin đăng nhập từ xa và lấy thông tin xác thực trong cả những ứng dụng Putty, RDP, VNC.

Cách thức lây nhiễm của Trickbot:



Mã độc được gửi qua email ngụy trang dưới dạng một thông báo ưu đãi thuế từ công ty tài chính lớn. Trong email đính kèm file Excel có chưa chi tiết về ưu đãi thuế. Khi người dùng mở tập tin này thì Trickbot sau khi kích hoạt.

FW: 2018 EF Tax Incentive Billing

JD - Deloitte <@deloitteus.org>
1/29/2019 12:44 AM

To:

deloitte_tax_file28012019.xlsm
32.81 KB

Please see the attached Tax Incentive billing

Tax Senior | Business Tax Services
Deloitte Tax LLP
2000, Atlanta, GA 30303
www.deloitte.com

Please consider the environment before printing.

This message (including any attachments) contains confidential information intended for a specific individual and purpose, and is protected by law. If you are not the intended recipient, you should delete this message and any disclosure, copying, or distribution of this message, or the taking of any action based on it, by you is strictly prohibited.
v.E.1
Privacy Notice:This message is from Engineered Floors, LLC. The information contained in this message may be privileged and confidential and protected from disclosure. If the reader of this message is not the intended recipient, or an employee or agent responsible for delivering this message to the intended recipient, you are hereby notified that any dissemination, distribution or copying of this communication is strictly prohibited. If you have received this communication in error, please notify us immediately by replying to this message and deleting it from your computer.

Email chưa tệp đính kèm độc hại

```
.rdata:100C1FA4 aChromeHistory  db 'chrome history',0   ; DATA XREF: sub_100137F8+54↑r
.rdata:100C1FA4                                        ; sub_100137F8+6D↑r ...
.rdata:100C1FB3                 db    0
.rdata:100C1FB4 aChromePassword db 'chrome passwords',0 ; DATA XREF: sub_100137F8+1CB↑r
.rdata:100C1FB4                                        ; sub_100137F8+1EA↑r ...
.rdata:100C1FC5                 db    0
.rdata:100C1FC6                 db    0
.rdata:100C1FC7                 db    0
.rdata:100C1FC8 aFirefoxPasswor db 'firefox passwords',0 ; DATA XREF: sub_100137F8+40F↑r
.rdata:100C1FC8                                        ; sub_100137F8+430↑r ...
.rdata:100C1FDA                 db    0
.rdata:100C1FDB                 db    0
.rdata:100C1FDC aFirefoxHistory db 'firefox history',0  ; DATA XREF: sub_100137F8+667↑r
.rdata:100C1FDC                                        ; sub_100137F8+688↑r ...
.rdata:100C1FEC aIePasswords    db 'IE passwords',0     ; DATA XREF: sub_100137F8+89C↑r
.rdata:100C1FEC                                        ; sub_100137F8+8BB↑r ...
.rdata:100C1FF9                 db    0
.rdata:100C1FFA                 db    0
.rdata:100C1FFB                 db    0
.rdata:100C1FFC aIeHistory      db 'IE history',0       ; DATA XREF: sub_100137F8+A37↑r
.rdata:100C1FFC                                        ; sub_100137F8+A58↑r ...
.rdata:100C2007                 db    0
.rdata:100C2008 aEdgePasswords  db 'Edge passwords',0   ; DATA XREF: sub_100137F8+BC1↑r
.rdata:100C2008                                        ; sub_100137F8+BDA↑r ...
.rdata:100C2017                 align 4
.rdata:100C2018 aEdgeHistory    db 'Edge history',0     ; DATA XREF: sub_100137F8+D3F↑r
.rdata:100C2018                                        ; sub_100137F8+D5E↑r ...
.rdata:100C2025                 align 4
.rdata:100C2028 aPasswordsGrabA db 'Passwords grab: allocation error',0
.rdata:100C2028                                        ; DATA XREF: sub_100137F8+10B0↑r
.rdata:100C2028                                        ; sub_100137F8+10CF↑r ...
.rdata:100C2049                 align 4
.rdata:100C204C aBrowserPasswor db 'Browser passwords are empty',0
```

Mã nguồn trickbot đánh cắp thông tin từ một số Trình duyệt

Biến thể mới nhất của Trickbot bổ sung thêm ba tính năng mới là đánh cắp cả thông tin đăng nhập trong Virtual Network Computing (VNC), PuTTY và Remote Desktop Protocol (RDP).

Để trích xuất thông tin xác thực từ PuTTY, Trickbot sẽ lấy thông tin từ Registry Software\SimonTatham\Putty\Sessions để xác định những phiên đã lưu trong Putty, sau đó trích xuất thông tin về Hostname, Username và Khóa xác thực

```
  goto LABEL_181;
buf_to_buf(a1 - 544, (a1 - 1368));
*(a1 - 4) = 18;
v36 = buf_to_buf(a1 - 348, &String2);
*(a1 - 4) = 19;
v37 = 0;
*(a1 - 103) = xmmword_100E8670;          // Software\SimonTatham\Putty
*(a1 - 87) = 0x72666D79;
*(a1 - 83) = 0x597A5561;
*(a1 - 79) = 0x5E59;
*(a1 - 77) = 0;
do
  *(a1 + v37++ - 103) -= 5;
while ( v37 < 0x1A );
v38 = sub_1000FB40((a1 - 256), v36);
*(a1 - 4) = 20;
v39 = 0x23;
*(a1 - 56) = 0x46707F23;                 // \Sessions\
v40 = 0;
*(a1 - 52) = 0x4C4A5050;
*(a1 - 48) = 0x7F504D;
while ( 1 )
{
```

```
sub_100C8A28():
v2 = 0;
*(a1 - 36) = 0;
v4 = v3;
*(a1 - 428) = v3;
*(a1 - 324) = 0;
*(a1 - 320) = 0;
*(a1 - 316) = 0;
*(a1 - 4) = 0;
v5 = 0x5E;
*(a1 - 22) = 0x1330165E;                 // Hostname
v6 = 0;
*(a1 - 18) = 0x9022C15;
*(a1 - 14) = 0;
while ( 1 )
{
  *(a1 + v6 - 21) ^= v6 + v5;
  if ( ++v6 >= 8 )
    break;
  v5 = *(a1 - 22);
}
*(a1 - 13) = 0;
buf_to_buf(a1 - 180, (a1 - 21));
*(a1 - 4) = 1;
sub_1000E110((a1 - 180));
*(a1 - 4) = 0;
sub_1000E3C0(a1 - 180, 0, a2);
v7 = 0x72;
*(a1 - 22) = 0x17012772;                 // Username
*(a1 - 18) = 0x1F133C00;
v8 = 0;
*(a1 - 14) = 23;
```

Đoạn mã lấy thông tin xác thực trên Putty

Gửi thông tin xác thực RDP đến máy chủ điều khiển

Những tính năng mới cập nhật vào Trickbot cho thấy đối tượng tấn công ngày càng đầu tư và phát triển mã độc này, không hề dừng lại sau những lợi ích thu được. của hò mà ngày càng cải thiện nó, làm cho nó ngày càng độc hại và nguy hiểm hơn.

Người dùng nên chú ý đến những email spam, để ý đến những người gửi đáng ngờ và họ cũng không nên mở các tệp đính kèm theo email trừ khi họ chắc chắn rằng đó là những nguồn hợp pháp.

Thông tin kỹ thuật tham khảo thêm tại:

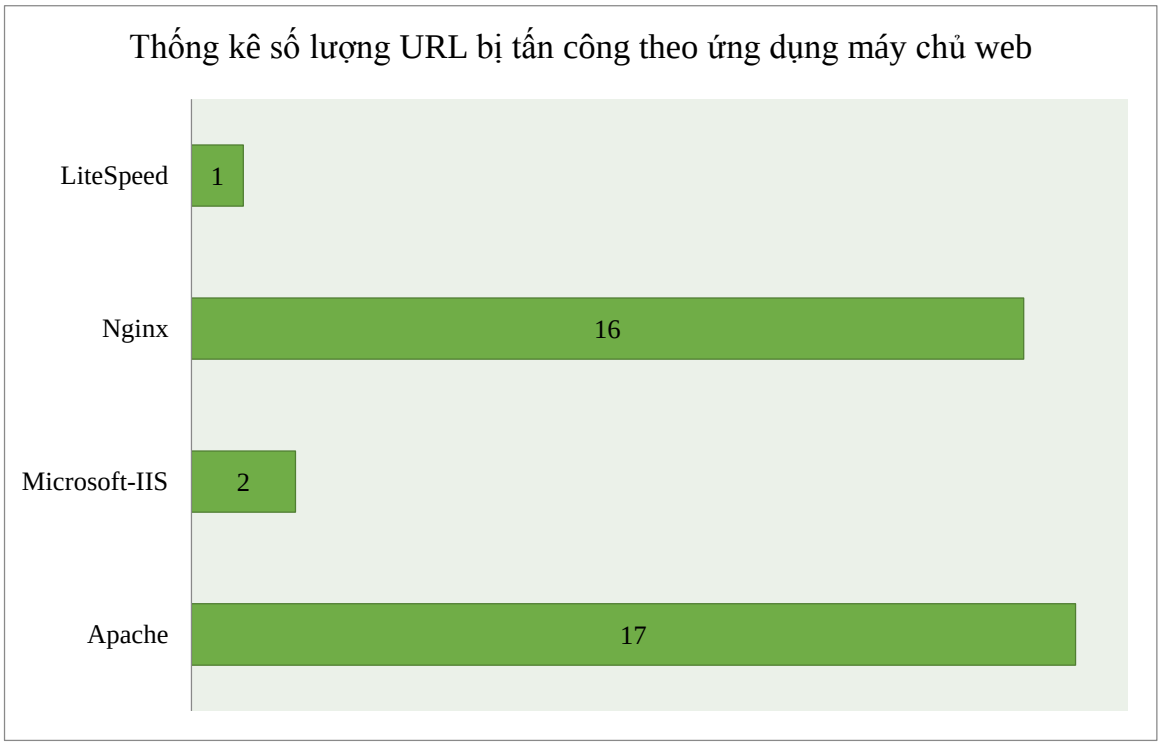
https://ti.khonggianmang.vn/dashboard/news/p/ma-doc-ngan-hang-trickbot-cap-nhat-them-tin/

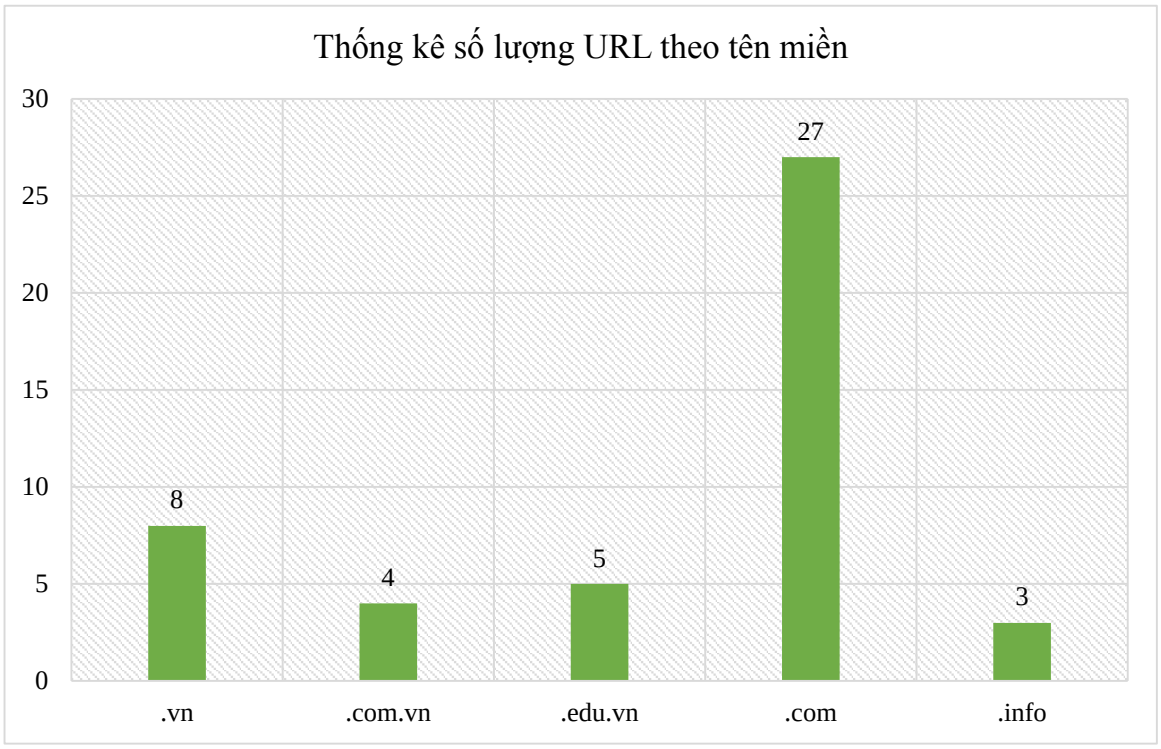
2. Tình hình tấn công gây nguy hại trên các trang web tại Việt Nam

Qua theo dõi, trích xuất thông tin từ hệ thống kỹ thuật thời gian qua, Cục ATTT nhận thấy trên không gian mạng đang tồn tại nhiều trang web Việt Nam (bao gồm cả những trang web sử dụng dịch vụ máy chủ nước ngoài) bị tấn công, lợi dụng để thực hiện các hành vi gây mất an toàn thông tin như: phát tán thư rác; tấn công từ chối dịch vụ; cài đặt và phát tán các loại mã độc (gần đây nhất là cài đặt và phát tán mã độc để đào tiền ảo); lưu trữ các mã khai thác điểm yếu lỗ hổng một cách tự động (như lỗ hổng trên trình duyệt hay các thành phần mở rộng của trình duyệt mà người dùng sử dụng .v.v…).

Trong tuần, Cục ATTT ghi nhận có ít nhất **47** đường dẫn (URL) trên các trang web tại Việt Nam bị tấn công, lợi dụng để thực hiện các hành vi gây mất

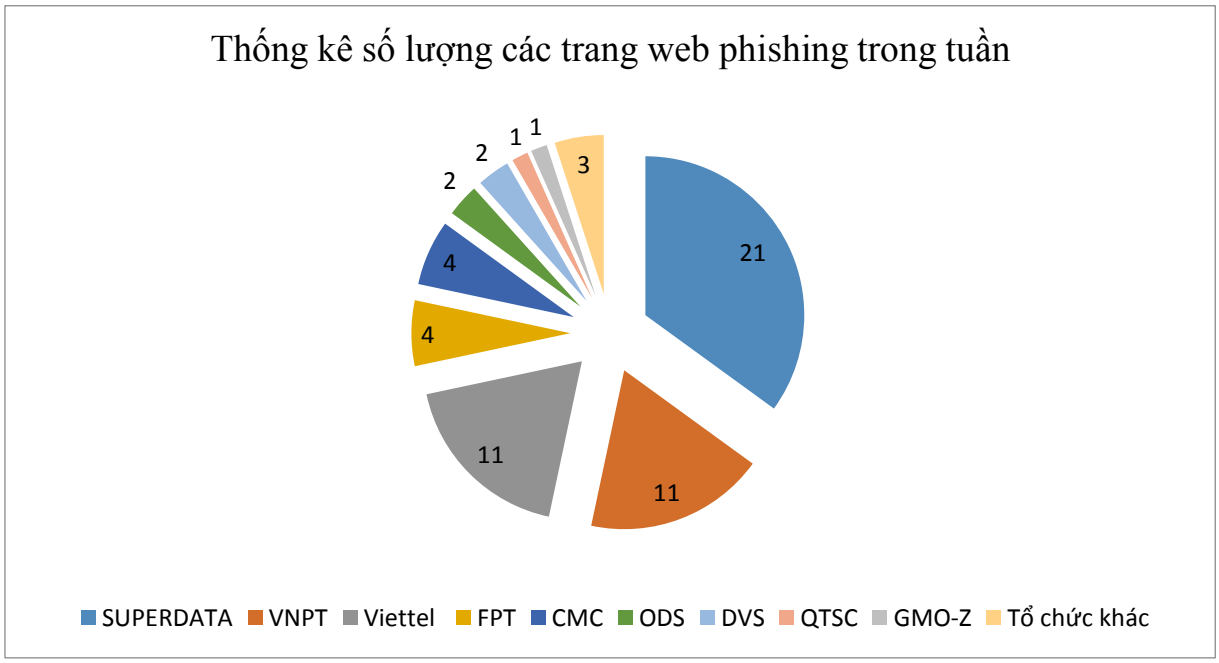
an toàn thông tin. Trong đó, thống kê, phân loại các đường dẫn này theo loại ứng dụng máy chủ web (IIS, Apache …) và nhà cung cấp cụ thể như sau:



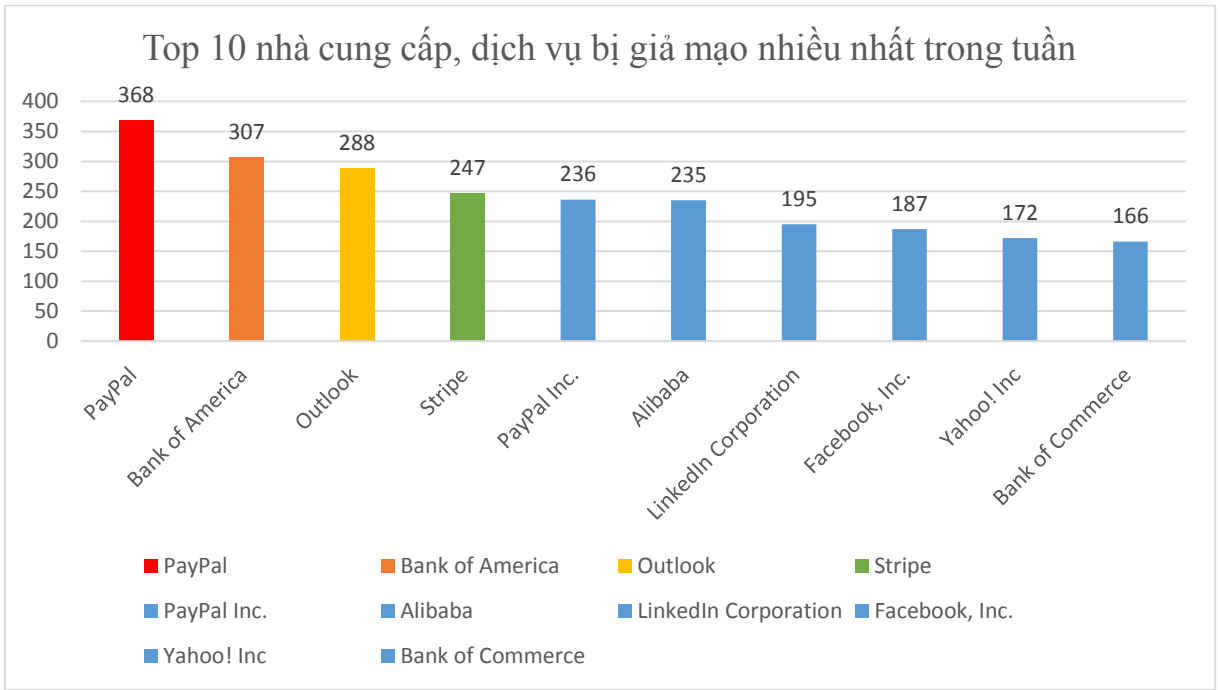


3. Tình hình tấn công lừa đảo (Phishing) trong tuần

3.1. Qua thu thập, theo dõi, trích xuất từ hệ thống kỹ thuật, Cục ATTT còn ghi nhận có ít nhất **62** trang web đặt tại Việt Nam bị lợi dụng để thực hiện tấn công Phishing trong tuần.



3.2. Trên thế giới có nhiều các trang web giả mạo các tổ chức, doanh nghiệp, nhà cung cấp, dịch vụ lớn như: Các mạng xã hội, ngân hàng, thư điện tử ..v.v…



Việt Nam có nhiều người dùng các dịch vụ, ứng dụng nước ngoài (cả miễn phí và có phí) như các mạng xã hội, Dropbox, Paypal ..v.v… vì vậy người

dùng cần phải hết sức cảnh giác với những trang web giả mạo để ăn trộm tài khoản.

4. Lỗ hổng/điểm yếu an toàn thông tin trong tuần

4.1. Trong tuần, các tổ chức quốc tế đã công bố và cập nhật ít nhất 255 lỗ hổng, trong đó có 31 lỗ hổng mức cao, 118 lỗ hổng mức trung bình, 14 lỗ hổng mức thấp và 92 lỗ hổng chưa đánh giá; 05 lỗ hổng đã có mã khai thác.

4.2. Hệ thống kỹ thuật của Cục An toàn thông tin 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 13 lỗ hổng trên một số sản phẩm, ứng dụng của Cisco, nhóm 29 lỗ hổng trên trình duyệt Chrome ...v.v.

4.3. Chi tiết về thông tin 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-2018-15380 CVE-2019-1664 CVE-2019-1700 ...	Nhóm 13 lỗ hổng trên một số sản phẩm, ứng dụng của Cisco (HyperFlex Software, Firepower 9000, Network Convergence System 1000 Series, Cisco Prime Collaboration Assurance...) cho phép đối tượng tấn công khai thác lỗi XSS chuyển hướng người dùng đến trang web độc hại, thu thập thông tin trên hệ thống đích, một số lỗ hổng cho phép thực thi lệnh với quyền người dùng cao nhất trên hệ thống	Đã có thông tin xác thực và bản vá
2	D-Link	CVE-2019-8392	Lỗ hổng phát hiện trên các thiết bị D-Link DIR-823G phiên bản firmware 1.02B03 cho phép kẻ tấn công từ xa kích hoạt chế độ Wi-Fi Guest thông qua API SetWLanRadioSinstall HNAP.	Chưa có thông tin xác nhận và bản vá

3	Google Chrome	CVE-2019-5754 CVE-2019-5755 CVE-2019-5783 ...	Nhóm 29 lỗ hổng trên Google Chrome cho phép đối tượng tấn công dựa trên 1 trang HTML hoặc file PDF tự tạo để thu thập thông tin, chèn và thực thi mã lệnh, tấn công leo thang.	Chưa có bản vá
4	IBM	CVE-2018-1701 CVE-2018-1727 CVE-2017-1695 CVE-2019-4059	Nhóm 04 lỗ hổng trên một số sản phẩm, ứng dụng của IBM (InfoSphere Information Server, Rational ClearCase) cho phép đối tượng tấn công thực hiện một số hình thức tấn công gồm: giải mã dữ liệu (do sử dụng giải thuật mã hóa yếu), thu thập thông tin quan trọng, bao gồm cả cơ sở dữ liệu lưu trữ mật khẩu thông qua các connector.	Đã có thông tin xác nhận
5	Cisco	CVE-2018-15380 CVE-2019-1664 CVE-2019-1700 ...	Nhóm 13 lỗ hổng trên một số sản phẩm, ứng dụng của Cisco (HyperFlex Software, Firepower 9000, Network Convergence System 1000 Series, Cisco Prime Collaboration Assurance...) cho phép đối tượng tấn công khai thác lỗi XSS chuyển hướng người dùng đến trang web độc hại, thu thập thông tin trên hệ thống đích, một số lỗ hổng cho phép thực thi lệnh với quyền người dùng cao nhất trên hệ thống	Đã có thông tin xác thực và bản vá

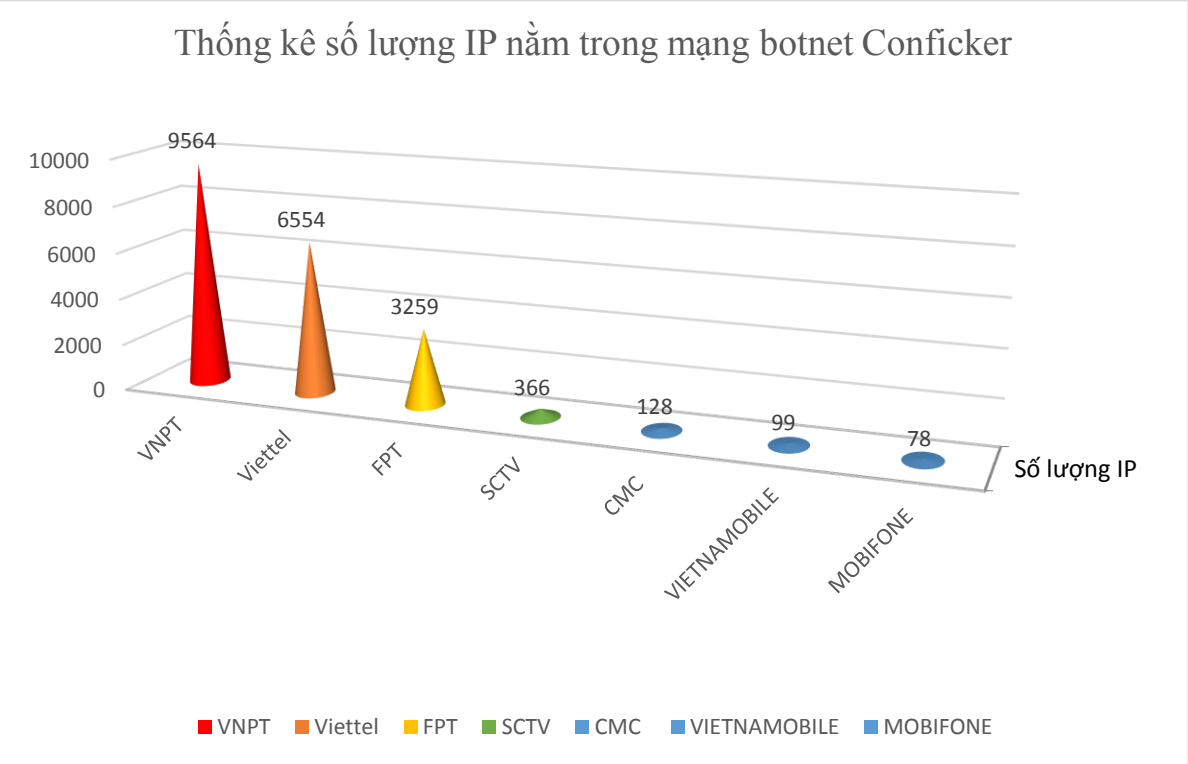
5. Hoạt động một số mạng botnet, APT, mã độc tại Việt Nam

5.1. Mạng botnet Conficker

Mạng botnet Conficker được phát hiện từ tháng 10/2008. Mã độc này được thiết kế nhằm vào hệ điều hành Microsoft Windows. Khi mã độc này lây nhiễm vào một máy tính, thì máy tính này tham gia vào mạng botnet và có thể bị điều khiển để gửi thư rác (spam) và tấn công các hệ thống khác. Những máy tính

bị lây nhiễm đều không truy cập được các website liên quan đến phần mềm diệt virus hay dịch vụ cập nhật của hệ Windows (Windows Update).

Mặc dù mạng botnet Conficker xuất hiện từ năm 2008, lợi dụng lỗ hổng cũ (MS 08-067), đã có bản vá bảo mật, tuy nhiên tại Việt Nam, số lượng máy tính nằm trong mạng botnet Conficker vẫn còn rất nhiều trong tuần mà Cục An toàn thông tin đang theo dõi.



5.2. Danh sách IP/tên miền máy chủ điều khiển của mạng botnet Conficker

TT	Tên miền/IP
1	104.244.14.252
2	104.244.14.253
3	38.229.141.123
4	38.229.145.115
5	38.229.156.73
6	38.229.170.101
7	38.229.173.187
8	38.229.179.247
9	38.229.134.237
10	38.229.144.129

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

TT	Tên miền/IP
1	plpanaifheaighai.com
2	n.hmiblgoja.ru
3	ajkeahkcueafuiaeuf.ru
4	mokoaehaeihgiaheih.ru
5	mel.cloudcontentsmak.com
6	iuefgauiaiduihgs.com
7	43trfdsds.com
8	strikotunrev.top
9	bszotsjovih.com
10	d3s1.me

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 An toàn thông tin khuyến nghị:

- 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 2*, các cơ quan tổ chức cần phải thường xuyên kiểm tra, rà soát máy chủ web để kịp thời phát hiện và cập nhật các điểm yếu, lỗ hổng trên các máy chủ web thuộc cơ quan, tổ chức mình

- Người dùng cần phải hết sức cảnh giác với những trang web giả mạo để ăn trộm tài khoản, đặc biệt là các trang web giả mạo các ứng dụng, dịch vụ phổ biến như đã nêu trong *mục 3.2* báo cáo này.

- Theo dõi và cập nhật bản vá cho các lỗ hổng, đặc biệt là lỗ hổng nêu tại *mục 4.3* báo cáo này.

- Chủ động kiểm tra, rà soát, bóc gỡ mã độc ra khỏi hệ thống mạng. Cục An toàn 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 An toàn thông tin theo thông tin bên dưới để phối hợp thực hiện.

- 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 An toàn thông tin đã chia sẻ, đặc biệt là các tên miền đã nêu trong *mục 5.2 và 5.3* báo cáo này.

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./.

Nơi nhận:
- Bộ trưởng và các Thứ trưởng (để b/c);
- Thư ký Lãnh đạo Bộ;
- Đơn vị chuyên trách về CNTT các bộ, ngành;
- Sở TT&TT các tỉnh, thành phố trực thuộc TW;
- Cục KSTTHC, Văn phòng Chính phủ;
- Vụ Khoa giáo - Văn xã, Văn phòng Chính phủ;
- Trung tâm CNTT, Văn phòng Trung ương Đảng;
- Trung tâm CNTT, Văn phòng Quốc Hội; (email)
- Trung tâm CNTT, Văn phòng Chủ tịch nước;
- Các Tập đoàn kinh tế; Tổng công ty nhà nước; Tổ chức tài chính và Ngân hàng;
- Cơ quan, đơn vị thuộc Bộ;
- Lãnh đạo Cục;
- Lưu: VT, NCSC.

KT. CỤC TRƯỞNG
PHÓ CỤC TRƯỞNG

Nguyễn Huy Dũng

PHỤ LỤC

Hệ thống phân tích và chia sẻ nguy cơ tấn công mạng Việt Nam

https://ti.khonggianmang.vn

HỆ THỐNG PHÂN TÍCH VÀ CHIA SẺ NGUY CƠ TẤN CÔNG MẠNG VIỆT NAM

Vietnam Threat Intelligence Portal

GIỚI THIỆU VỀ HỆ THỐNG

Hệ thống phân tích và chia sẻ nguy cơ tấn công mạng Việt Nam là hệ thống cho phép thu thập, phân tích và chia sẻ thông tin trực tiếp về dấu hiệu, nguy cơ và cuộc tấn công mạng đang xảy ra trên hệ thống của các cơ quan, đơn vị. Mục tiêu của hệ thống nhằm tăng cường việc kết nối chia sẻ thông tin giữa các cơ quan, đơn vị, tổ chức.

ĐIỂM NỔI BẬT CỦA HỆ THỐNG

Khi truy cập vào hệ thống, các cơ quan, đơn vị sẽ được chia sẻ các thông tin theo thời gian thực về: các dấu hiệu, hình thức tấn công mạng trên hệ thống thông tin của mình được Cục An toàn thông tin tổng hợp, phân tích và xử lý từ nhiều tổ chức trên thế giới.

- **Cập nhật liên tục nguy cơ tấn công mạng:** Cập nhật danh sách các máy chủ điều khiển C&C, IP, Hash độc hại (APT, Botnet, Phishing, Ransomeware...) thường được sử dụng để tấn công vào Việt Nam.
- **Giám sát và cảnh báo sớm tấn công mạng:** Giám sát và cảnh báo sớm các tấn công vào hệ thống của tổ chức và các kết nối bất thường từ hệ thống mạng ra ngoài. Đánh giá định kỳ mức độ an toàn thông tin của hệ thống.

THÔNG TIN LIÊN HỆ

Email: ais@mic.gov.vn | Website: Khonggianmang.vn
Phone: +84 24 3209 6789 | Fax: +84 24 3209 6789
Address: Tầng 8 - 115 Trần Duy Hưng - Cầu Giấy - Hà Nội

BEST SERVICES

THÔNG TIN CẬP NHẬT

Hệ thống liên tục cập nhật và chia sẻ các thông tin về nguy cơ tấn công mạng đối với Việt Nam.

DỮ LIỆU ĐA DẠNG

Dữ liệu được tổng hợp từ các tổ chức Quốc tế, Việt Nam, từ các sensor, honeypot,...

CẢNH BÁO TỨC THÌ

Hệ thống cảnh báo sớm các tấn công và cảnh báo các kết nối bất thường từ hệ thống mạng tổ chức.

CÁC NỘI DUNG CỦA DỊCH VỤ

HOẠT ĐỘNG CỦA CHÚNG TÔI

Cảnh báo sớm ATTT

Hỗ trợ các tổ chức cảnh báo sớm các nguy cơ tấn công mạng.

Giám sát ATTT

Thực hiện cung cấp dịch vụ giám sát ATTT từ xa và tổng thể.

Đánh giá ATTT

Cung cấp dịch vụ đánh giá ATTT từ Ứng dụng, Hạ tầng, Kiến trúc...

Xử lý tấn công mạng

Hỗ trợ xử lý tấn công mạng cục bộ và trên diện rộng cho các tổ chức.

ORGANIZATION
Dành cho Tổ chức

- Danh sách máy chủ điều khiển độc hại.
- Danh sách IP độc hại.
- Danh sách mã hash độc hại.
- Danh sách website lừa đảo.
- Thông tin ATTT cập nhật.
- Báo cáo tổng hợp hàng tuần.

GOVERMENT
Dành cho cơ quan Chính phủ

- Đầy đủ thông tin của tài khoản Organization.
- Cập nhật điểm yếu, lỗ hổng nguy hiểm và phổ biến đối với Việt Nam.
- Giám sát tình trạng Up/Down của hệ thống.
- Giám sát và cảnh báo về mã độc/ backlink trên Website.
- Cảnh báo các tấn công mạng vào hệ thống công khai của tổ chức.
- Cảnh báo các kết nối bất thường, đáng ngờ từ hệ thống của tổ chức.
- Cảnh báo tức thì qua Email.
- Hỗ trợ kỹ thuật qua Email

ENTERPRISE
Dành cho Doanh nghiệp

- Đầy đủ thông tin của tài khoản Goverment.
- Danh sách domain độc hại C&C được sử dụng tấn công APT vào Việt Nam.
- Danh sách IP, Hash sử dụng tấn công có chủ đích APT vào Việt Nam.
- Cập nhật các thông tin có liên quan đến tổ chức, website giả mạo tổ chức...nếu có.
- Cập nhật các tin tức, phân tích kỹ thuật mới nhất về tấn công có chủ đích APT.
- Đánh giá các điểm yếu, lỗ hổng bảo mật định kỳ đối với các hệ thống công khai (IP và Domain) của tổ chức.
- Cảnh báo tức thì qua SMS.
- Hỗ trợ kỹ thuật qua Email.
- Hỗ trợ kỹ thuật Hotline.

LIÊN HỆ ĐĂNG KÝ SỬ DỤNG:

Email: ais@mic.gov.vn | **Website:** Khonggianmang.vn | **Phone:** +84 24 3209 6789
Address: 115 - Trần Duy Hưng - Cầu Giấy - Hà Nội