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: **03**/BC-CATTT

Hà Nội, ngày 15 tháng 01 năm 2019

TÓM TẮT
Tình hình an toàn thông tin đáng chú ý trong tuần 02/2019
(từ ngày 07/01/2019 đến ngày 13/01/2019)

BẢNG TỔNG HỢP

1. Ngày 10/01/2019, Ủy ban điều tra tấn công mạng vào Hệ thống SingHealth của Singapore (viết tắt là COI, được thành lập vào tháng 7/2018) đã công bố một Báo cáo cho thấy bên cạnh các điểm yếu an toàn thông tin của hệ thống thì nhận thức về bảo đảm an toàn thông tin của nhân sự cũng là một trong những nguyên nhân chủ yếu dẫn tới việc vi phạm dữ liệu.

2. Trong một nghiên cứu với dữ liệu của khoảng 5 triệu mật khẩu bị lộ, lọt từ những vụ vi phạm dữ liệu trong thời gian gần đây, SplashData đã công bố một danh sách những mật khẩu kém an toàn nhất năm 2018.

3. . Chuyên gia của FireEye đã phát hiện một chiến dịch tấn công tên miền DNS Hijacking vào nhiều tổ chức ở khu vực Trung Đông, Bắc Mỹ và Châu Âu. Các tổ chức bị ảnh hưởng gồm cơ quan chính phủ, nhà cung cấp dịch vụ viễn thông, hạ tầng Internet và tổ chức thương mại. Đây là chiến dịch tấn công với quy mô lớn chưa từng thấy trước đây.

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. Ngày 10/01/2019, Ủy ban điều tra tấn công mạng vào Hệ thống SingHealth của Singapore (viết tắt là COI, được thành lập vào tháng 7/2018) đã công bố một Báo cáo cho thấy bên cạnh các điểm yếu an toàn thông tin của hệ thống thì nhận thức về bảo đảm an toàn thông tin của nhân sự cũng là một trong những nguyên nhân chủ yếu dẫn tới việc vi phạm dữ liệu.

COI cho biết đối tượng tấn công lần đầu tiến hành thử xâm nhập hệ thống mạng của SingHealth vào tháng 8/2017. Đến Tháng 12/2017 thì dữ liệu trên hệ thống bị vi phạm kéo dài đến tháng 6/2018. Cuộc tấn công mạng lần đầu tiên bị quản trị viên CNTT của IHiS chú ý là khi phát hiện có đăng nhập trái phép không thành công vào cơ sở dữ liệu của Trình quản lý lâm sàng (SCM), tuy nhiên quản trị viên đã không tiếp tục theo dõi, giám sát hoạt động đáng ngờ vì cho rằng nỗ lực xâm nhập của đối tượng đã thất bại và không thực hiện nữa. Điều này cho thấy, nhân sự chính có vai trò trong việc phản ứng và báo cáo về dấu hiệu tấn công mạng đã không hành động kịp thời, phù hợp theo đúng chính sách bảo đảm an toàn thông tin của SingHealth và đã bỏ lỡ cơ hội để ngăn chặn tấn công đi sâu hơn, cụ thể là sự vụ vi phạm dữ liệu.

COI đã đưa ra 16 khuyến nghị trong đó 7 khuyến nghị ưu tiên để cải thiện kế hoạch, phản ứng đối với tấn công mạng và đề xuất áp dụng cho cả việc bảo vệ cơ sở dữ liệu cá nhân khác của chính phủ .

1.2. SpashData (một doanh nghiệp phần mềm chuyên phát triển trình quản lý mật khẩu) cho biết, rất nhiều người dùng hiện nay vẫn đang có thói quen đặt mật khẩu khá dễ đoán, bất chấp những cảnh báo, khuyến nghị về nguy cơ mất an toàn thông tin. Những mật khẩu này luôn đứng đầu trong cơ sở dữ liệu của các công cụ tấn công dò tìm mật khẩu.

Trong một nghiên cứu với dữ liệu của khoảng 5 triệu mật khẩu bị lộ, lọt từ những vụ vi phạm dữ liệu trong thời gian gần đây, SplashData đã công bố một danh sách những mật khẩu kém an toàn nhất năm 2018, theo đó 10% mật khẩu (trong 5 triệu mật khẩu bị lộ lọt) đã sử dụng ít nhất một trong số 25 mật khẩu phổ biến sau:

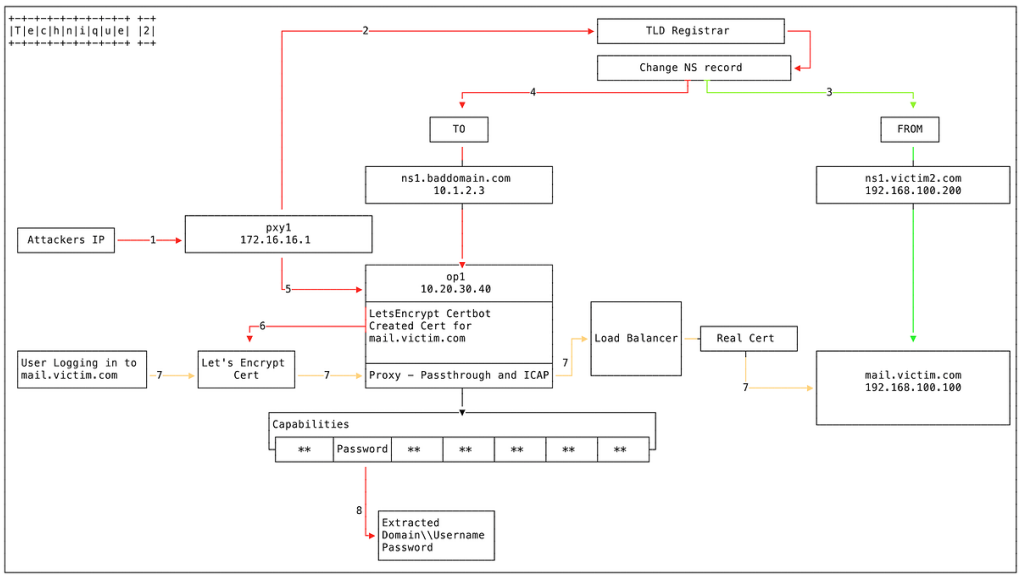
TT	Mật khẩu	TT	Mật khẩu
1	123456	13	welcome
2	password	14	666666
3	123456789	15	abc123
4	12345678	16	football
5	12345	17	123123
6	111111	18	monkey
7	1234567	19	654321
8	sunshine	20	!@#$%^&*
9	qwerty	21	charlie
10	iloveyou	22	aa123456 w
11	princess	23	donald
12	admin	24	password1
		25	qwerty123

1.3. Chuyên gia của FireEye đã phát hiện một chiến dịch tấn công tên miền DNS Hijacking vào nhiều tổ chức ở khu vực Trung Đông, Bắc Mỹ và Châu Âu. Các tổ chức bị ảnh hưởng gồm cơ quan chính phủ, nhà cung cấp dịch vụ viễn thông, hạ tầng Internet và tổ chức thương mại. Đây là chiến dịch tấn công với quy mô lớn chưa từng thấy trước đây.

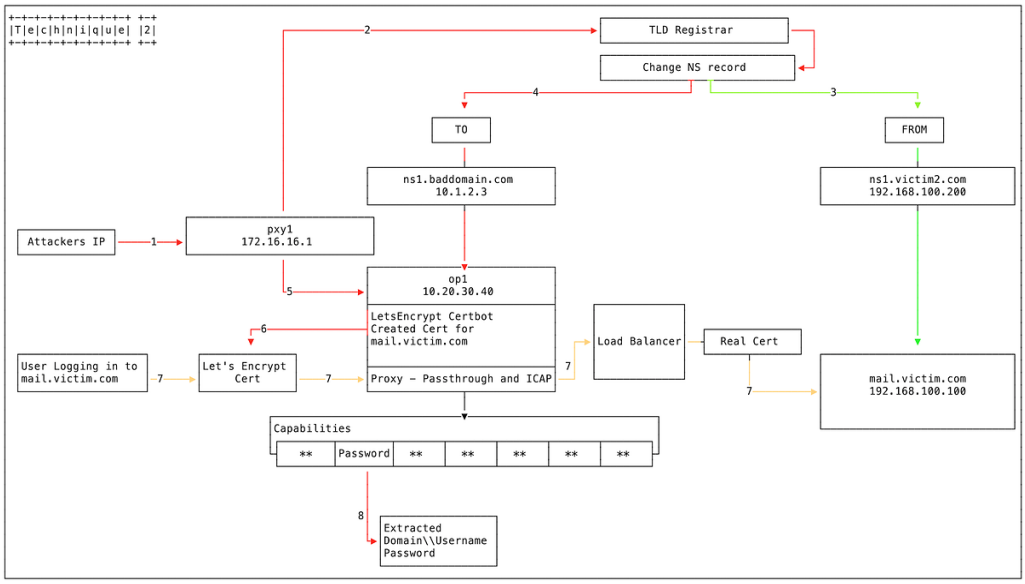
FireEye đã theo dõi hoạt động này trong nhiều tháng, xây dựng biểu đồ để phân tích hoạt động, kỹ thuật và quy trình triển khai của đối tượng tấn công, đồng thời cũng đã làm việc với những tổ chức nạn nhân bị tấn công, cơ quan an ninh và cơ quan chính phủ ở các khu vực để giảm thiểu tác động và ngăn chặn tấn công tiếp theo.

Chiến dịch tấn công này có thể sử dụng kỹ thuật tấn công truyền thống, trong phân tích của FireEye, đề chập ít nhất đến 3 cách thực hiện để thay đổi bản ghi DNS:

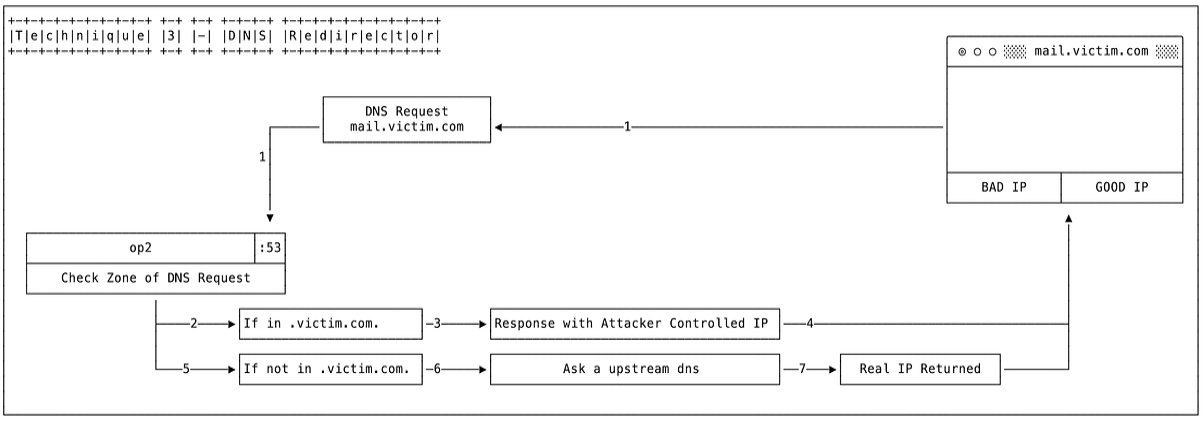
- Kỹ thuật 1: Thay đổi bản ghi A. Đối tượng tấn công thay đổi thông tin bản ghi A trên hệ thống quản lý tên miền của nhà cung cấp dịch vụ và tạo chứng chỉ Let's Encrypt certificate (chứng chỉ do Let’s Encrypt cung cấp miễn phí, các tên miền sử dụng chứng chỉ này không bị hiển thị cảnh báo trên trình duyệt như chứng chỉ tự tạo ra) cho tên miền mục tiêu để xác thực.



- Kỹ thuật 2: Thay đổi bản ghi NS. Đối tượng tấn công có thể thay đổi bản ghi NS đến địa chỉ IP của máy chủ DNS giả mạo, việc thay đổi có thể thực hiện thông qua hệ thống của nhà đăng ký tên miền hoặc ccTLD (nhà quản lý tên miền cấp quốc gia). Sau đó cập nhật bản ghi A với tên miền mục tiêu thông qua máy chủ DNS giả mạo, và tạo chứng chỉ Let's Encrypt certificate cho tên miền mục tiêu.



- Kỹ thuật 3: DNS Redirector. Kết hợp cả 2 kỹ thuật trên.

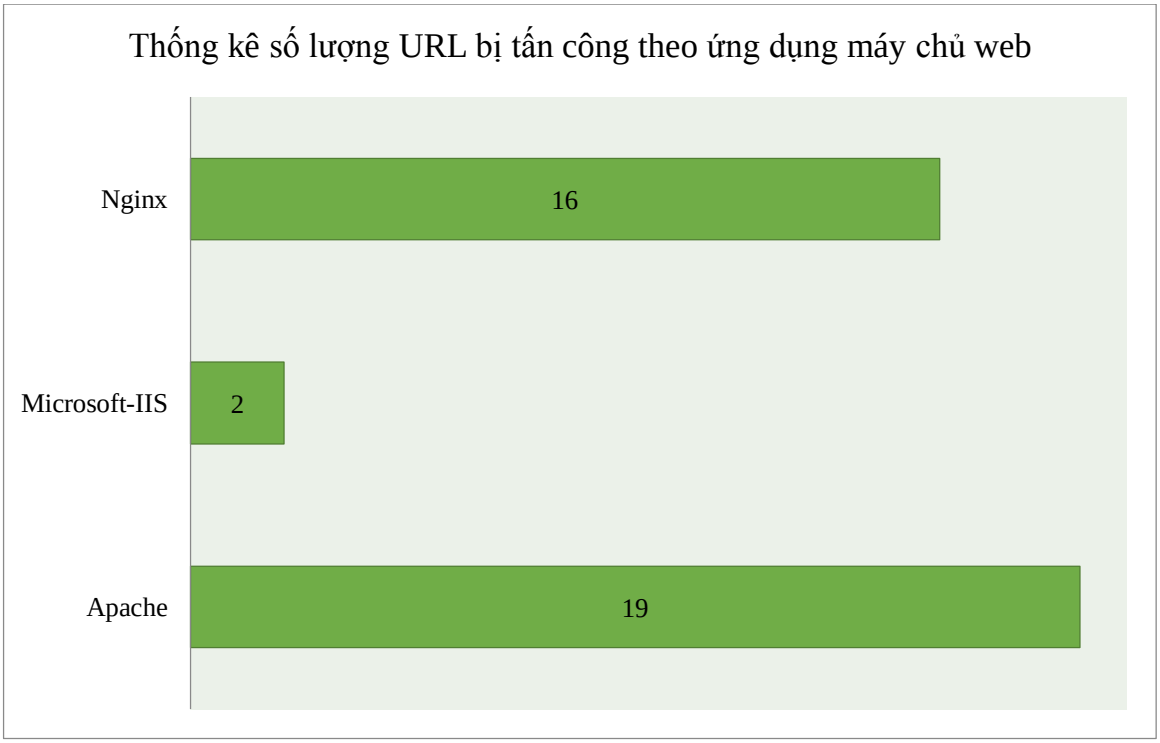


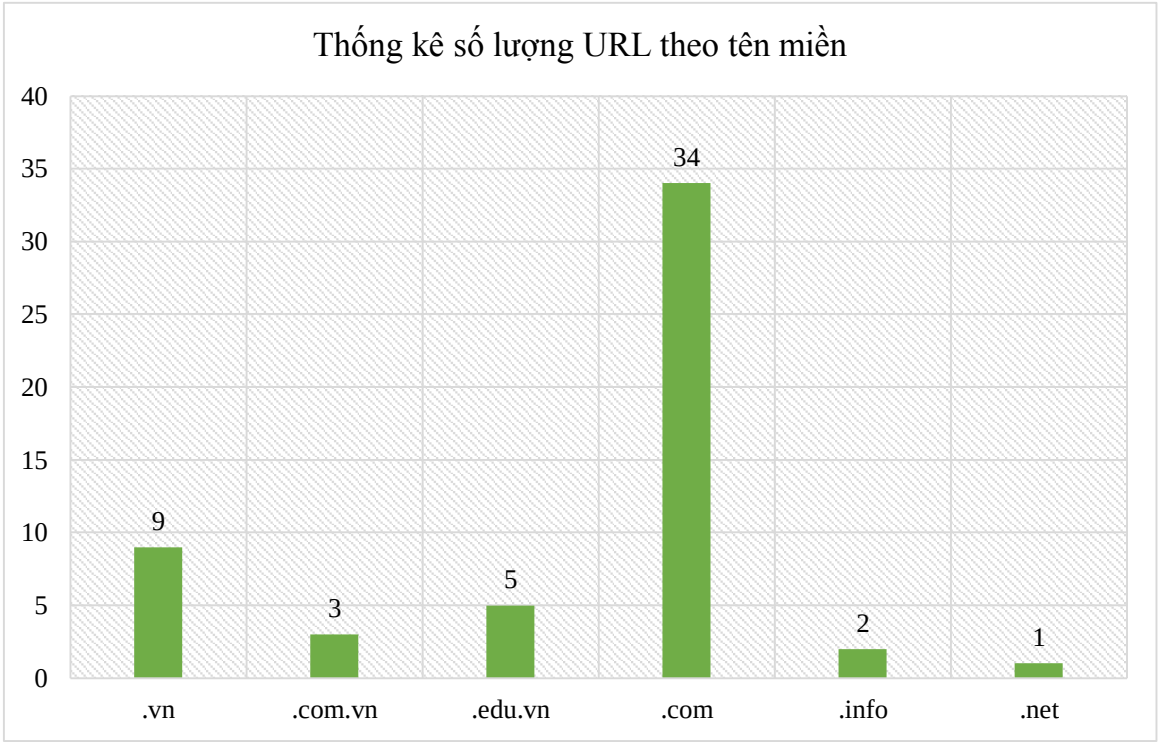
Theo FireEye, đây là chiến dịch tấn công với quy mô lớn chưa từng thấy trước đây; đối tượng tấn công sẽ tiếp tục thực hiện ở những khu vực và quốc gia khác. Đặc biệt khi được kết hợp với những hình thức tấn công khác sẽ gây ra thiệt hại khó có thể lường trước được. Do vậy cơ quan tổ chức có máy chủ DNS, nhà quản lý tên miền, tổ chức cung cấp dịch vụ cần phải siết chặt hơn các biện pháp để giảm thiểu các và sớm phát hiện tấn công có thể xảy ra.

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…).

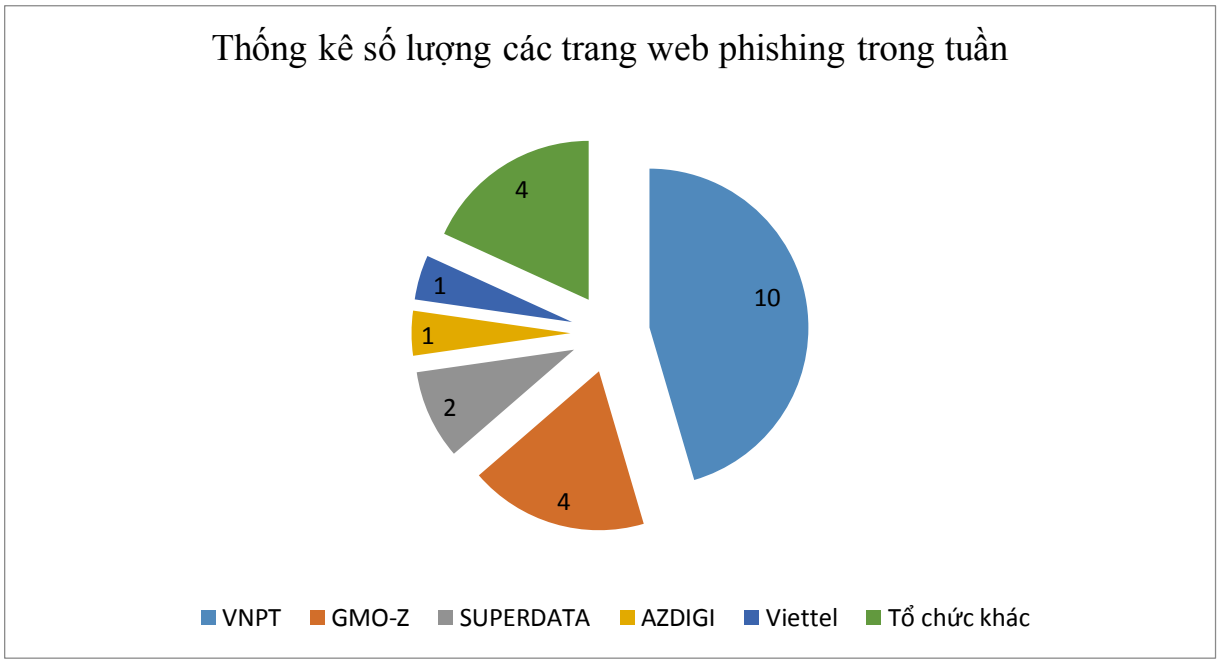
Trong tuần, Cục ATTT ghi nhận có ít nhất **54** đường dẫn (URL) trên các trang web tại Việt Nam bị tấn công, lợi dụng để thực hiện các hành vi gây mất an toàn thông tin. Trong đó, thống kê, phân loại các đường dẫn này theo loại ứng dụng máy chủ web (IIS, Apache …) và nhà cung cấp cụ thể như sau:



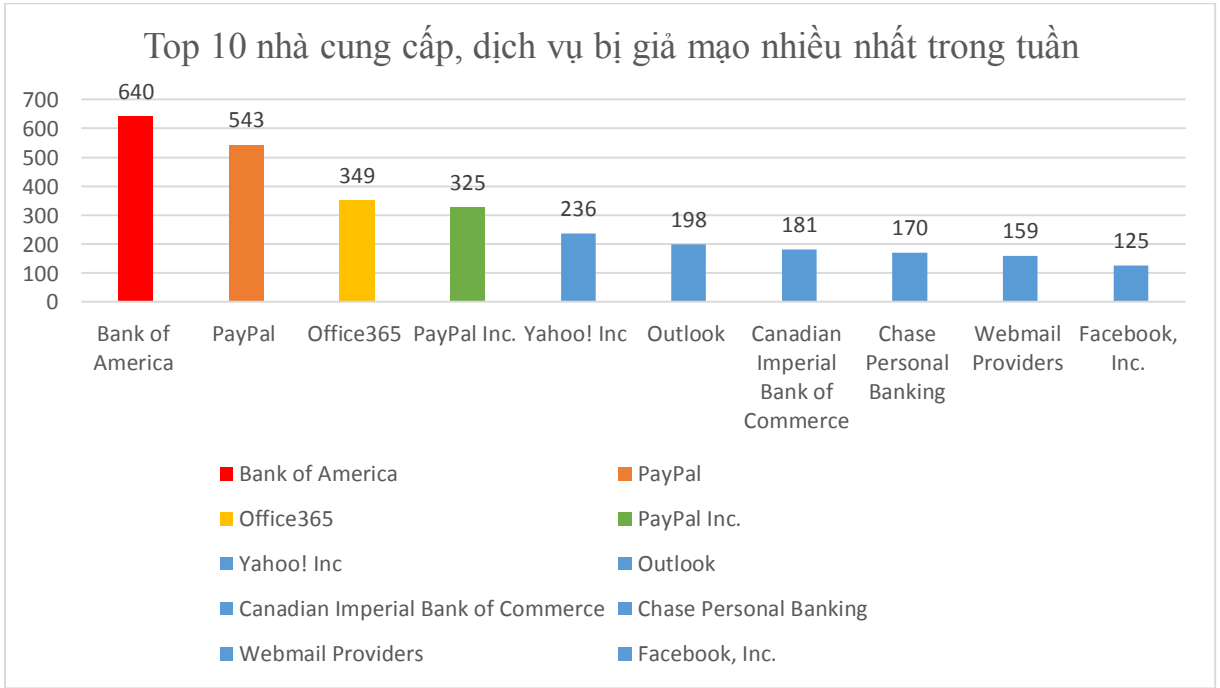


3. Tình hình tấn công lừa đảo (Phishing) trong tuần

3.1. Qua thu thập, theo dõi, trích xuất từ hệ thống kỹ thuật, Cục ATTT còn ghi nhận có ít nhất **22** 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 399 lỗ hổng, trong đó có ít nhất 32 lỗ hổng cho phép chèn và thực thi mã lệnh, 10 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 **08** 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 48 lỗ hổng trên một số sản phẩm, ứng dụng của Microsoft; Nhóm 53 lỗ hổng trên một số sản phẩm, ứng dụng Apple ..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	Microsoft	CVE-2019-0565 CVE-2019-0586 CVE-2019-0539 …	Nhóm 48 lỗ hổng trên một số sản phẩm, ứng dụng của Microsoft (Edge, Internet Explorer ASP.NET, Office, Exchange, SharePoint, Skype, Visual Studio, Windows kernel...) cho phép đối tượng tấn công thực hiện nhiều hình thức tấn công khác nhau: tấn công từ chối dịch vụ, thu thập thông tin, XSS, chèn và thực thi mã lệnh, tấn công leo thang.	Đã có thông tin xác nhận và bản vá
2	IBM	CVE-2018-1859 CVE-2018-1932 CVE-2018-1888	Nhóm 07 lỗ hổng trên một số sản phẩm, ứng dụng của IBM (IBM API Connect, IBM i Access for Windows, Jazz Reporting Service, IBM Spectrum Scale) cho phép đối tượng tấn công thực hiện khai thác lỗi XSS, thu thập thông tin, tấn công leo thang, chèn và thực thi mã lệnh thông qua DLL độc hại.	Đã có thông tin xác nhận và bản vá
3	Apple	CVE-2018-4043 CVE-2017-2411	Nhóm 53 lỗ hổng trên một số sản phẩm, ứng dụng	Đã có thông tin

		CVE-2018-4257 ...	Apple (Clean My Mac X, iOS, macOS High Sierra, tvOS, iTunes, iCloud, watchOS, Safari, SwiftNIO) cho phép đối tượng tấn công thực hiện: thu thập thông tin, khai thác lỗi tràn bộ đệm và tấn công leo thang	xác nhận và bản vá Một số lỗ hổng đã có mã khai thác
4	Aterm	CVE-2018-0634 CVE-2018-0640 CVE-2018-0637	Nhóm 17 lỗ hổng trong dòng Camera Aterm HC100RC của NEC cho phép đối tượng tấn công chèn và thực thi lệnh của hệ điều hành qua nhiều thành phần khác nhau, khai thác lỗi tràn bộ đệm.	Đã có thông tin xác nhận và bản vá
5	Cisco	CVE-2018-15464 CVE-2018-15453 CVE-2018-0461 …	Nhóm 17 lỗ hổng trên một số sản phẩm, ứng dụng của Cisco cho phép đối tượng tấn công thực hiện tấn công từ chối dịch vụ, thu thập thông tin nhạy cảm, xem thông tin xác thực ở dạng không mã hóa, tấn công XSS, một số lỗi cho phép chèn và thực thi đoạn mã độc hại.	Đã có thông tin xác nhận và bản vá
6	D-link	CVE-2018-20675 CVE-2018-20674	Nhóm 02 lỗ hổng trên một số dòng sản phẩm của D-Link cho phép đối tượng tấn công thực hiện vuwojt qua cơ chế xác thực để thực thi lệnh độc hại.	Chưa có thông tin xác nhận và bản vá
7	Google - Chrome	CVE-2018-20070 CVE-2018-6167 CVE-2017-15428 …	Nhóm 84 lỗ hổng trên trình duyệt Chrome cho phép đối tượng tấn công thực hiện thu thập thông tin nhạy cảm, vi phạm chính sách cùng nguồn, khai thác lỗi tràn bộ đệm, chèn và thực thi mã lệnh tùy ý.	Đã có thông tin xác nhận và bản vá
8	Imperva	CVE-2018-5412 CVE-2018-5413 CVE-2018-5403	Nhóm 03 lỗ hổng trên một số sản phẩm của Imperva (Imperva SecureSphere,	Chưa có thông tin xác nhận

			Imperva SecureSphere gateway) cho phép thực hiện tấn công leo thang (thông qua việc thêm khóa xác thực SSH), chèn và thực thi mã lệnh	và bản vá Đã có mã khai thác

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

5.1. Mạng botnet Andromeda

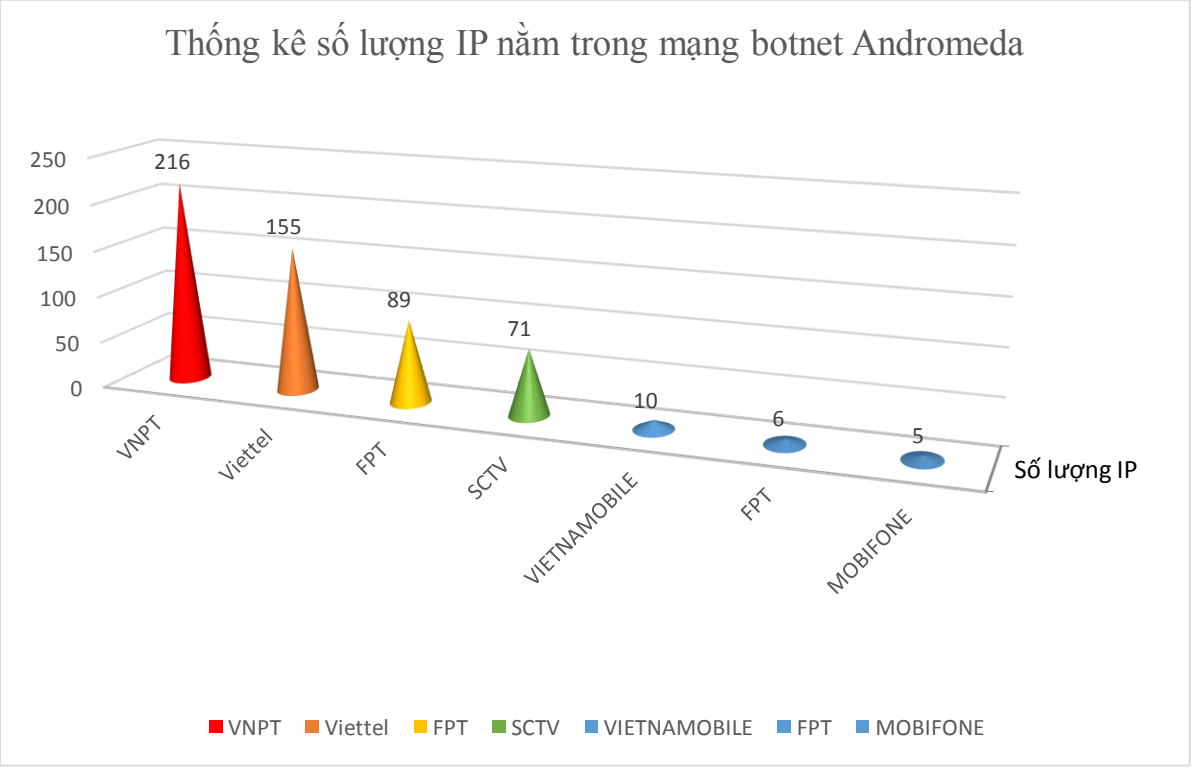
Botnet Andromeda, còn được gọi là Win32/Gamarue đã bắt đầu xuất hiện và lây nhiễm vào các máy tính từ năm 2011. Đối tượng chính của cuộc tấn công mã độc này là các doanh nghiệp sử dụng thẻ thanh toán.

Mục đích chính của Andromeda botnet là để phát tán các dòng mã độc khác nhằm phục vụ các cuộc tấn công phần mềm độc hại toàn cầu. Mạng botnet Andromeda bao gồm và có liên quan đến ít nhất 80 họ phần mềm độc hại, trong đó chủ yếu là họ mã độc Point of Sale (POS), ví dụ như GamaPOS. Trong sáu tháng cuối năm 2017, nó đã bị phát hiện lây nhiễm khoảng hơn 1 triệu máy tính mỗi tháng.

Mã độc Andromeda có các chức năng chính như: Keylogging; Rootkit; Truy cập từ xa ẩn; Thu thập thông tin đăng nhập từ trình duyệt.

Các tổ chức quốc tế cũng đã hợp tác với nhau để ngăn chặn các máy chủ và khoảng 1500 tên miền độc hại được sử dụng để phát tán và kiểm soát mạng botnet này.

Tại Việt Nam, số lượng máy tính nằm trong mạng botnet Andromeda 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 Andromeda

TT	Tên miền/IP
1	and30.blabladomdom.com
2	produkktc.com
3	dghfhfgjfhjghj6699.net
4	and31.amainwrorldnancy4.com
5	and28.aviationdreamflightering1.com
6	and12.thesuchivestfishmarketeat111.com
7	and9.themainnotmainstreet2.com
8	and10.uzuzuseubumaandro1.com
9	last-time.ru
10	and19.amainwrorldnancy1.com

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

TT	Tên miền/IP
1	www.iuqerfsodp9ifjaposdfjhgosurijfaewrwergwea.com
2	www.cityofangelsmagazine.com
3	dqrzxapnw.info
4	caarmelcollege.org
5	osheoufhusheoghuesdl.com
6	msjbsiq.com
7	6ae79845b2.pw
8	www.corpnox-technologie.fr
9	nlcfoundation.org
10	ahmedfahmy.name

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 *mục 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;
- 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.

(email)

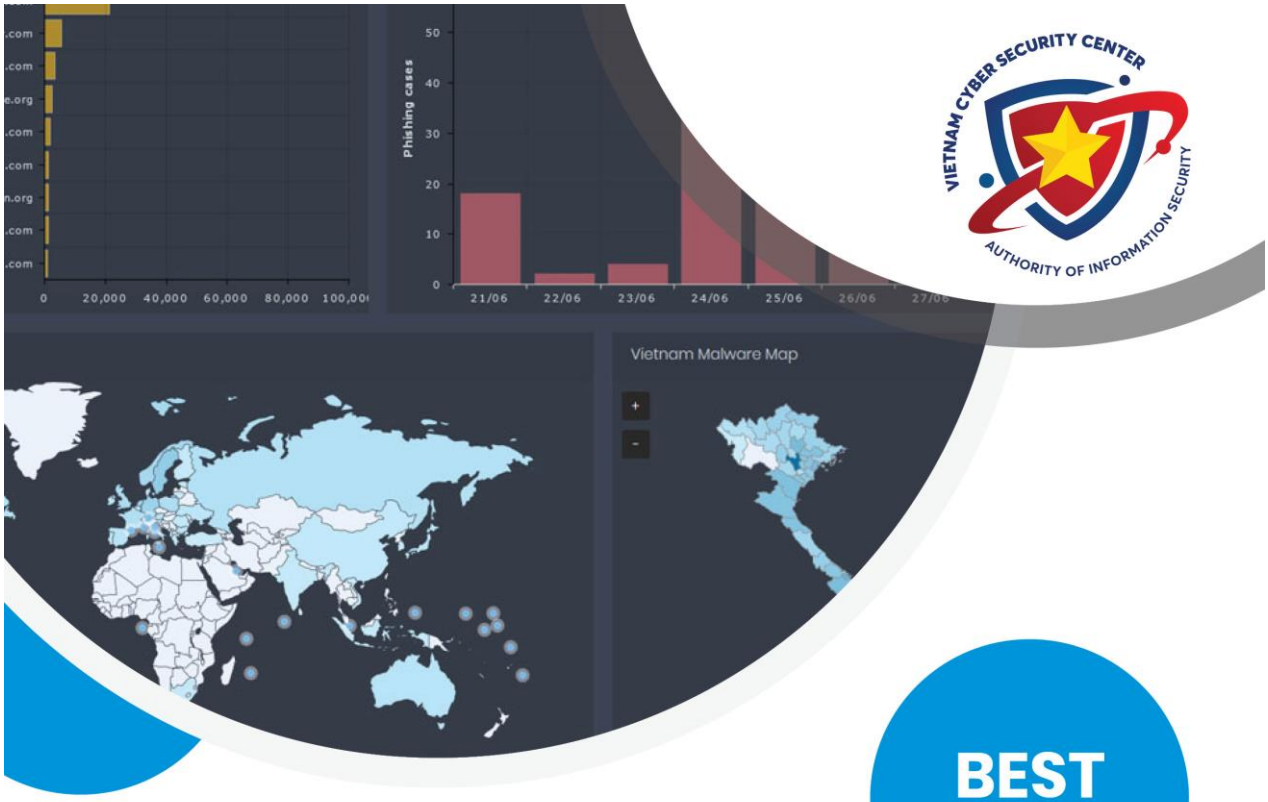
KT. CỤC TRƯỞNG
PHÓ CỤC TRƯỞNG

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

BEST SERVICES

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

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