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 4 năm 2019

TÓM TẮT
Tình hình an toàn thông tin đáng chú ý trong tuần 13/2019
(từ ngày 25/3/2019 đến ngày 31/3/2019)

BẢNG TỔNG HỢP

1. Ngày 01/4/2019, Trung tâm Giám sát an toàn không gian mạng quốc gia (NCSC) phối hợp cùng Công ty Group-IB (Nga) và Công ty CyberLab (Việt Nam) tổ chức khóa đào tạo kỹ thuật nhằm mục đích tăng cường khả năng phân tích mã độc dành riêng cho cán bộ vận hành các hệ thống thông tin thuộc lĩnh vực tài chính, ngân hàng.

2. Theo TechJury, 43% các cuộc tấn công mạng là nhằm vào các doanh nghiệp vừa và nhỏ; 91% các cuộc tấn công mạng được bắt đầu bằng một email lừa đảo; 85% các tệp đính kèm được gửi qua email hàng ngày đều có nguy cơ gây mất ATTT cho người nhận; 38% tệp đính kèm độc hại được che dấu dưới dạng một loại tập tin văn bản; chi phí toàn cầu của hoạt động tấn công mạng dự kiến sẽ đạt 6 nghìn tỷ USD vào năm 2021.

3. hãng bảo mật Palo Alto đã phát hiện ra một biến thể mới của botnet nổi tiếng trong lĩnh vực IoT là Mirai. Mirai được biết đến với việc được sử dụng trong các cuộc tấn công DDoS lớn ở mức độ chưa từng có trong năm 2016.

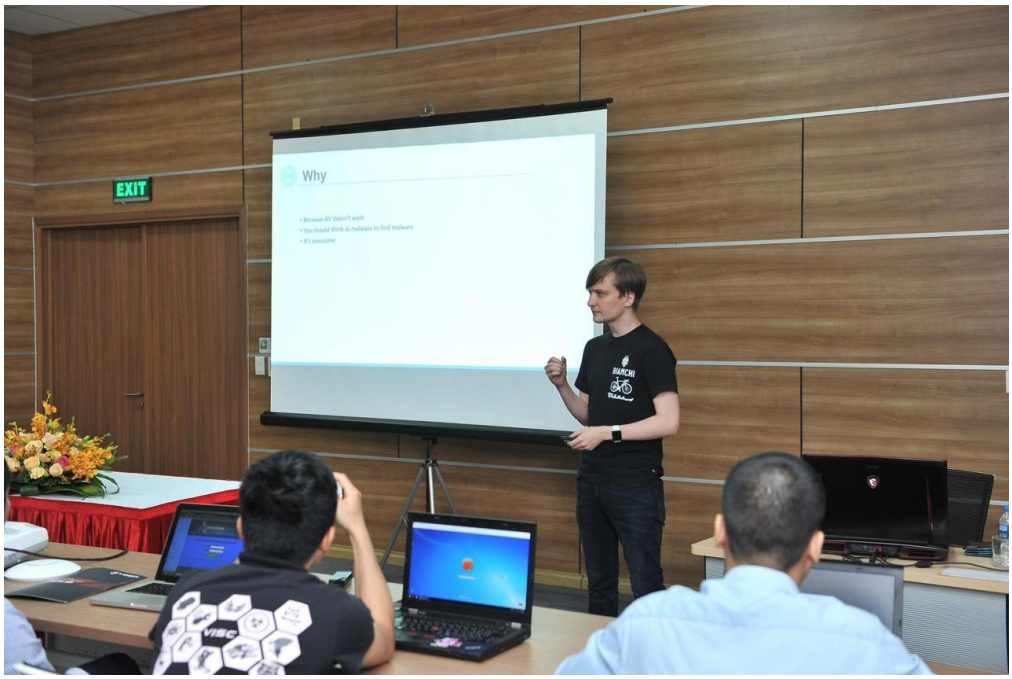
4. Báo cáo được xây dựng dựa trên các nguồn thông tin thu thập được từ hệ thống phân tích và chia sẻ nguy cơ tấn công mạng Việt Nam (https://ti.khonggianmang.vn). Thông tin chi tiết về Hệ thống tại *Phụ lục kèm theo*.

1. Điểm tin đáng chú ý

1.1. Ngày 01/4/2019, Trung tâm Giám sát an toàn không gian mạng quốc gia (NCSC) phối hợp cùng Công ty Group-IB (Nga) và Công ty CyberLab (Việt Nam) tổ chức khóa đào tạo kỹ thuật nhằm mục đích tăng cường khả năng phân tích mã độc dành riêng cho cán bộ vận hành các hệ thống thông tin thuộc lĩnh vực tài chính ngân hàng.

Lớp học giới hạn số lượng học viên với 16 học viên đến từ 12 ngân hàng, tổ chức tài chính lớn của Việt Nam (BIDV, Agribank, Vietinbank, Vietcombank, MBBank, Techcombank, LienVietPost bank, VIB, VPBank, TPBank, Sacombank, NAPAS…) tham dự.

Nội dung khóa học được thiết kế riêng cho các tổ chức tài chính ngân hàng với các kỹ thuật, kỹ năng phân tích các loại mã độc phổ biến thường được sử dụng để tấn công vào các hệ thống tài chính. Bên cạnh các kiến thức lý thuyết làm nền tảng thì thời lượng chính của khóa học sẽ được chuyên gia người Nga của Group-IB tập trung vào các bài thực hành kỹ thuật. Ngoài ra, trong khóa học cũng sẽ cùng nhau phân tích, thảo luận một số chiến dịch tấn công được thực hiện bởi nhóm APT Lazarus Group (aka. Hidden Cobra) vào ngân hàng trong thời gian gần đây.



Giảng viên chính của khóa học là ông Vitaliy Trifonov, chuyên gia forensics và phân tích mã độc của Group-IB, với nhiều năm kinh nghiệm trong lĩnh vực phân tích mã độc và reverse engineering. Vitaliy Trifonov đã phân tích hàng nghìn mẫu mã độc và đào tạo cho các chuyên gia tất cả các cấp độ thuộc nhiều tổ chức tài chính trên toàn cầu. Bên cạnh đó, Vitaliy Trifonov đã trực tiếp tham gia các hoạt động phản ứng sự cố và điều tra đối với các tấn công APT nhắm tới các tổ chức tài chính (một số nhóm APT như Anunak/Carbanak, Buhtrap, Lurk, Cobalt, Fin7, Moneytaker, Lazarus…).

1.2. Tổng hợp các thống kê về an toàn thông tin mạng trong những năm vừa qua của TechJury - một nhóm chuyên gia về đánh giá sản phẩm CNTT.

Theo TechJury, 43% các cuộc tấn công mạng là nhằm vào các doanh nghiệp vừa và nhỏ; 91% các cuộc tấn công mạng được bắt đầu bằng một email lừa đảo; 85% các tệp đính kèm được gửi qua email hàng ngày đều có nguy cơ gây mất ATTT cho người nhận; 38% tệp đính kèm độc hại được che dấu dưới dạng một loại tập tin văn bản; chi phí toàn cầu của hoạt động tấn công mạng dự kiến sẽ đạt 6 nghìn tỷ USD vào năm 2021. Thông kê chi tiết:

- Trong hầu hết các trường hợp, các cơ quan, tổ chức phải mất khoảng 6 tháng để phát hiện các vi phạm dữ liệu. *(Nguồn: ZD Net)*

- Có 8854 vụ vi phạm dữ liệu được ghi nhận từ ngày 01/01/2005 đến ngày 18/4/2018. *(Nguồn: Identity Theft Resource Center)*

- Năm 2017, 61% nạn nhân của các vụ vi phạm dữ liệu là các tổ chức, doanh nghiệp có ít hơn 1000 nhân viên. *(Nguồn: Verizon)*

- 43% các cuộc tấn công mạng có mục tiêu là các doanh nghiệp nhỏ. *(Nguồn: Small Business Trends)*

- Các cuộc tấn công IoT đã tăng 600% trong năm 2017. *(Nguồn: Symantec)*

- 31% các tổ chức đã trải qua các cuộc tấn công mạng vào cơ sở hạ tầng CNTT. *(Nguồn: Cisco)*

- Chỉ 38% các tổ chức toàn cầu cho rằng họ được trang bị và có thể xử lý một cuộc tấn công mạng phức tạp. *(Nguồn: IBM)*

- Hơn 24.000 ứng dụng di động độc hại bị chặn bởi các cửa hàng ứng dụng khác nhau mỗi ngày. *(Nguồn: Symantec)*

- 2,4 triệu USD là chi phí trung bình của một cuộc tấn công bằng phần mềm độc hại trong năm 2017. *(Nguồn: Accergy)*

- Gia tăng 80% các cuộc tấn công bằng phần mềm độc hại trên máy tính Mac trong năm 2017. *(Nguồn: Cisco)*

- Khoảng 60% tên miền độc hại có liên quan đến các chiến dịch thư rác. *(Nguồn: Cisco)*

- Chi phí cho an toàn thông tin dự kiến sẽ đạt 1 nghìn tỷ USD vào năm 2024. *(Nguồn: Cyber Defense Magazine)*

- Chi phí hàng năm do các thiệt hại của tấn công mạng gây ra dự kiến sẽ lên tới 5 nghìn tỷ USD vào năm 2020. *(Nguồn: Cyber Defense Magazine)*

- 65% công ty có hơn 500 nhân viên chưa bao giờ thay đổi mật khẩu. *(Nguồn: Varonis)*

- Các cuộc tấn công mã độc tống tiền (Ransomware) đang tăng hơn 350% mỗi năm. *(Nguồn: Cisco)*

- Chi phí thiệt hại do Ransomware sẽ tăng lên 10 tỷ USD vào năm 2019. *(Nguồn: Cyber Defense Magazine)*

- cứ sau 13.275 giây có một doanh nghiệp trở thành nạn nhân của một cuộc tấn công Ransomware. *(Nguồn: Cyber Defense Magazine)*

- 21% các tập tin hoàn toàn không được bảo vệ. *(Nguồn: Varonis)*

- Báo cáo lỗ hổng hệ thống đã tăng 16% trong năm 2017. *(Nguồn: Varonis)*

- 95% các vi phạm dữ liệu đã được quy cho lỗi của con người. *(Nguồn: Giải pháp Cybint)*

- 30% người dùng Hoa Kỳ mở email lừa đảo. *(Nguồn: Verizon)*

- 12% những người đã mở email lừa đảo sau đó đã mở các liên kết hoặc tệp đính kèm bị nhiễm. *(Nguồn: Verizon)*

- Năm 2018, 76% doanh nghiệp báo cáo rằng họ là nạn nhân của một cuộc tấn công lừa đảo. *(Nguồn: Wombat)*

1.3. Biến thể mới của mạng Botnet Mirai

Vừa qua, hãng bảo mật Palo Alto đã phát hiện ra một biến thể mới của botnet nổi tiếng trong lĩnh vực IoT là Mirai. Mirai được biết đến với việc được sử dụng trong các cuộc tấn công DDoS lớn ở mức độ chưa từng có trong năm 2016. Một số mục tiêu đáng chú ý nhất bao gồm: Nhà cung cấp dịch vụ lưu trữ web, nhà cung cấp dịch vụ DNS.

Biến thể mới này mà Đơn vị số 42 của hãng phát hiện sử dụng nhiều lỗ hổng bảo mật khác nhau, có mục tiêu là các thiết bị nhúng khác nhau như bộ định tuyến, thiết bị lưu trữ qua mạng, camera IP.

Cụ thể, Đơn vị 42 đã tìm thấy biến thể mới của botnet này nhắm mục tiêu vào các hệ thống WePresent WiPG-1000 Wireless Presentation và TV LG Supersign. Cả hai thiết bị này đều được sử dụng phổ biến bởi các doanh nghiệp. Điều này cho chúng ta thấy một sự thay đổi về chiến lược trong việc sử dụng Mirai nhắm vào các doanh nghiệp. Trong khi đó, trường hợp gần đây nhất phát hiện botnet này là tấn công kết hợp của các lỗ hổng liên quan đến các thiết bị sâu trong hệ thống mạng như: Apache Struts và SonicWall.

Ngoài việc nhắm vào mục tiêu mới hơn, biến thể của Mirai có thêm các kiểu khai thác dữ liệu mới, như việc cố gắng tấn công thiết bị bằng các thuật toán phá mật khẩu (brute force). Những tính năng mới này cho botnet mirai khả năng tấn công đa dạng hơn. Ngoài ra, việc nhắm mục tiêu vào các doanh nghiệp, chúng cũng cố gắng xâm nhập các khu vực có lượng băng thông lớn hơn, dẫn đến khả năng các cuộc tấn công DDOS tương lai sẽ có cường độ băng thông lớn, phức tạp hơn.

Những phát hiện này nhấn mạnh tầm quan trọng của các doanh nghiệp về việc bảo mật cho các thiết bị IoT trên mạng của họ, như việc thay đổi mật khẩu mặc định và đảm bảo cập nhật đầy đủ các bản vá trên thiết bị.

Các tính năng khác

- Biến thể mới sử dụng cùng một sơ đồ mã hóa đặc trưng của Mirai với khóa bảng là 0xbeafdead.

- Khi giải mã các chuỗi bằng khóa này, các chuyên gia đã tìm thấy các dữ liệu liên quan đến việc phá mật khẩu hệ thống, thông tin gồm: admin:huigu309; root:huigu309; CRAFTSPERSON:ALC#FGU; root:videoflow

- Sử dụng tên miền epicrustserver[.]cf với cổng 3933 dành cho giao tiếp C&C.

- Ngoài việc quét các thiết bị dễ bị tấn công khác, phiên bản mới có thể được lệnh để gửi các cuộc tấn công HTTP Flood DDoS.

Kết luận

Các botnet liên quan đến IoT tiếp tục mở rộng tấn công, bằng cách kết hợp nhiều phương thức khai thác nhắm vào rất nhiều thiết bị hoặc bằng cách thêm vào danh sách thông tin đăng nhập mặc định hay tìm cách phá mã (brute force) hoặc cả hai. Ngoài ra, mục tiêu là các doanh nghiệp cho phép mã độc có

thể truy cập và có kết nối băng thông lớn hơn so với các mục tiêu cũ, vì vậy năng của mạng botnet này cũng lớn hơn trong các cuộc tấn công DDoS.

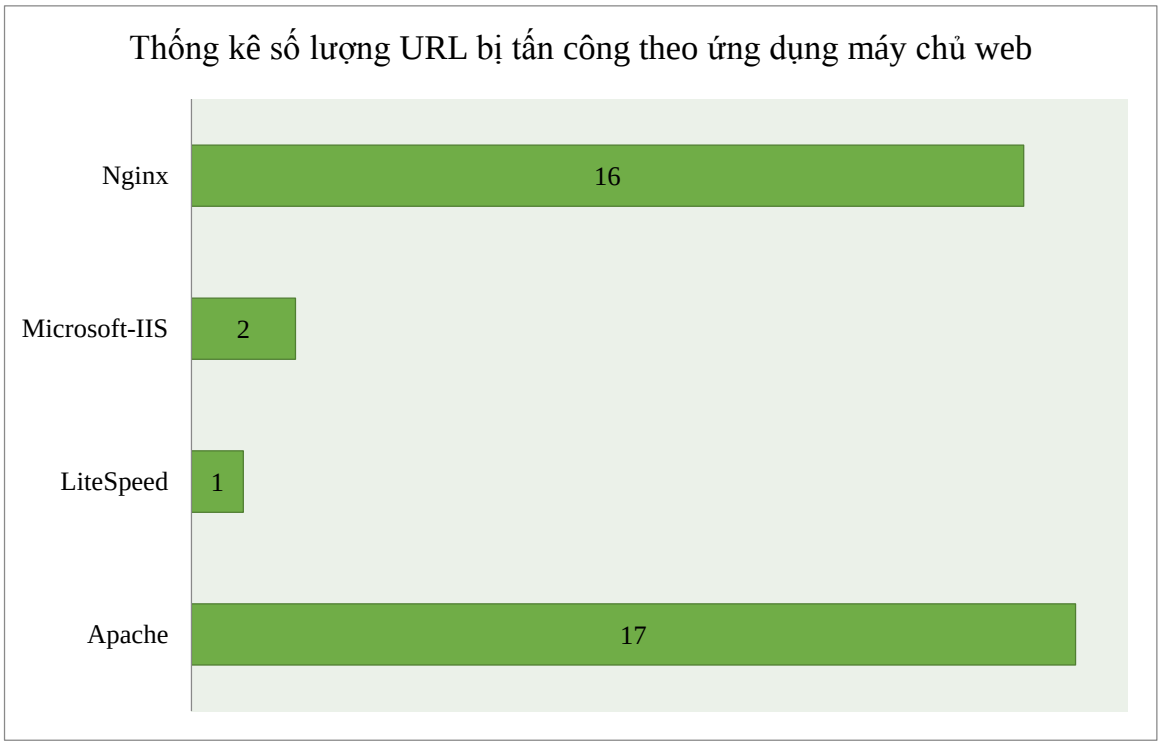
Các lỗ hổng, điểm yếu có thể bị khai thác bởi biến thể này tham khảo tại:

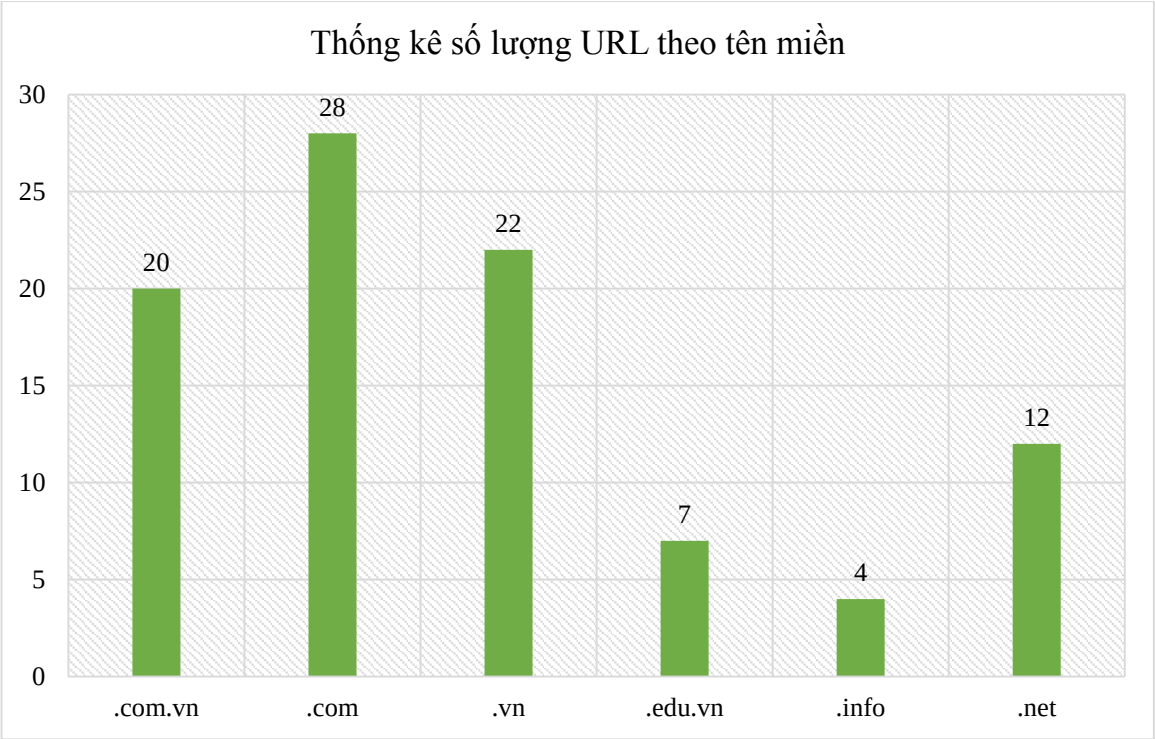
https://ti.khonggianmang.vn/dashboard/news/p/bien-the-moi-mang-botnet-mirai/

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…).

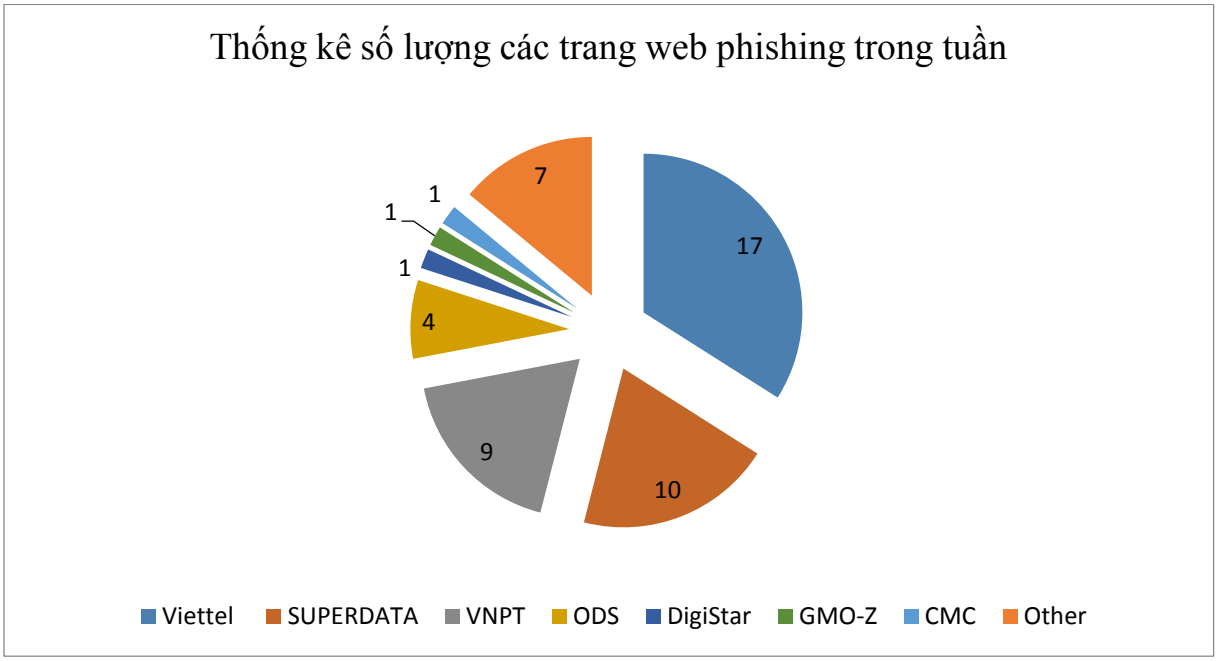
Trong tuần, Cục ATTT ghi nhận có ít nhất **93** đường dẫn (URL) trên các trang web tại Việt Nam bị tấn công, lợi dụng để thực hiện các hành vi gây mất an toàn thông tin. Trong đó, thống kê, phân loại các đường dẫn này theo loại ứng dụng máy chủ web (IIS, Apache …) và nhà cung cấp cụ thể như sau:



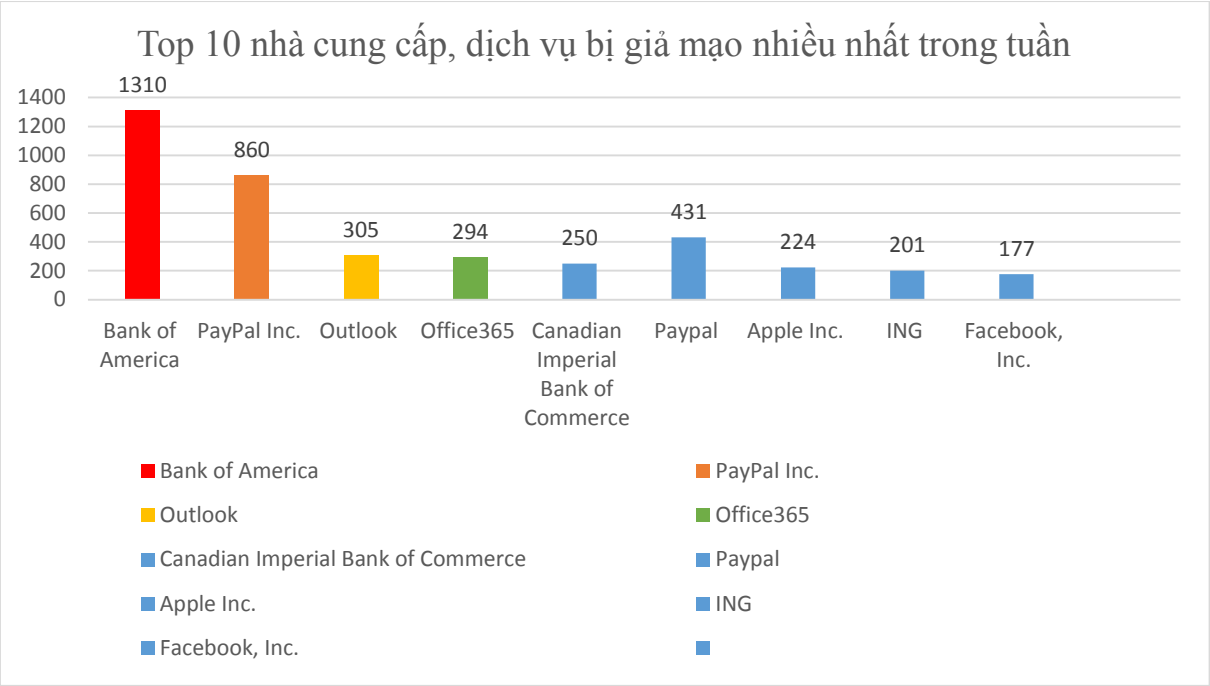


3. Tình hình tấn công lừa đảo (Phishing) trong tuần

3.1. Qua thu thập, theo dõi, trích xuất từ hệ thống kỹ thuật, Cục ATTT còn ghi nhận có ít nhất **50** 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, Paypment, Apple, 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 340 lỗ hổng, trong đó có 27 lỗ hổng mức cao, 109 lỗ hổng mức trung bình, 14 lỗ hổng mức thấp và 190 lỗ hổng chưa đánh giá; 4 lỗ hổng đã có mã khai thác.

4.2. Hệ thống kỹ thuật của Cục ATTT chủ động rà quét trên không gian mạng Việt Nam, đánh giá, thống kê cho thấy có 04 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 25 lỗ hổng trong một số sản phẩm của Cisco; Nhóm 09 lỗ hổng trên phần mềm Jenkins; Nhóm 08 lỗ hổng trên phần mềm Apache ...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	IBM	CVE-2019-4052 CVE-2019-4035	Nhóm 03 lỗ hổng trên một số sản phẩm, ứng dụng của	Đã có thông tin

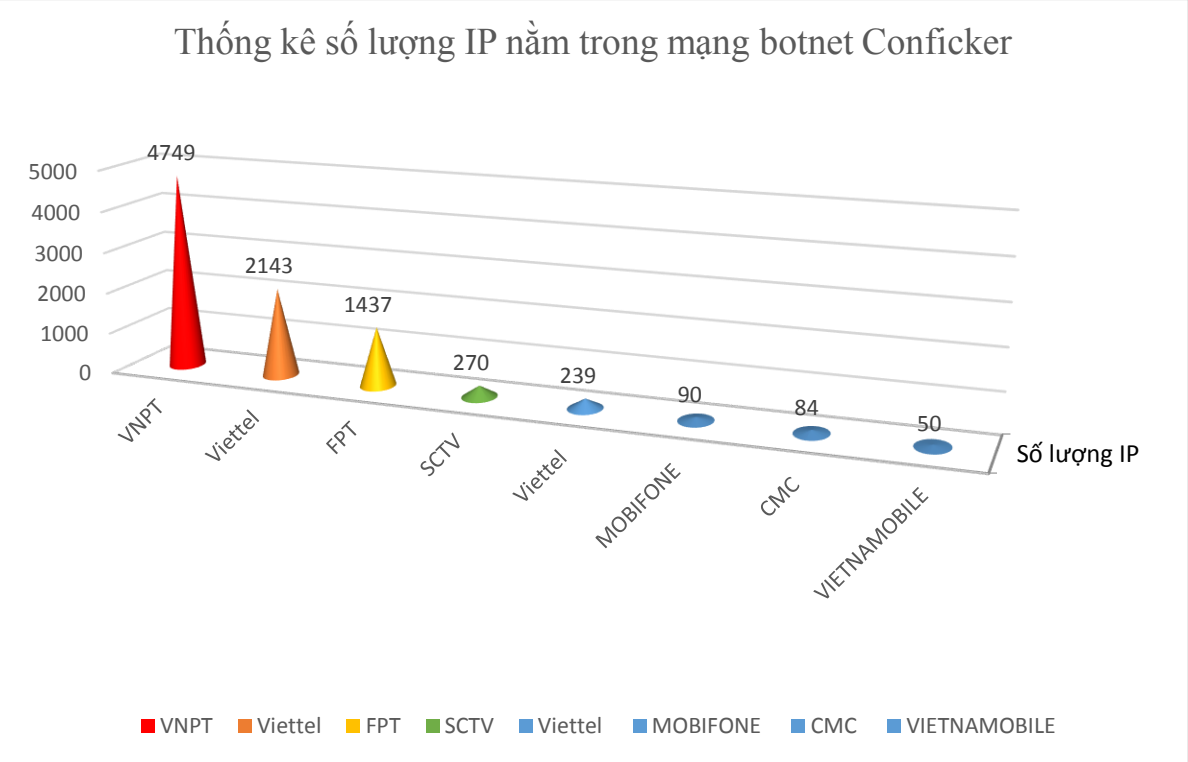
		CVE-2019-4046 ...	IBM (API Connect, DB2 Linux/ Windows, Rational Engineering Lifecycle Manage, IBM SDK, WebSphere Application Server...) cho phép đối tượng tấn công thực hiện thu thập thông tin, khai thác các lỗi tràn bộ đệm để chèn và thực thi mã lệnh, tấn công leo thang.	xác nhận và bản vá
2	Apache	CVE-2019-0204 CVE-2019-0222 CVE-2019-0212 CVE-2019-0225 CVE-2019-0224 CVE-2019-7608 CVE-2019-7609 CVE-2019-7610 ...	Nhóm 08 lỗ hổng trong một số sản phẩm của Apache (JMeter, Solr, Qpid Broker-J, Apache Traffic Server) cho phép đối tượng tấn công thực hiện thu thập thông tin, chèn và thực thi mã lệnh trong phạm vi của ứng dụng.	Đã có thông tin xác nhận và bản vá
3	Jenkins	CVE-2019-1003048 CVE-2019-1003047 CVE-2019-1003046 CVE-2019-1003045 CVE-2019-1003044 …..	Nhóm 9 lỗ hổng trên phần mềm Jenkins (phần mềm sử dụng trong phát triển phần mềm) cho phép đối tượng tấn công thu thập thông tin xác thực lưu trữ trong cấu hình của Plugin, một số lỗ hổng cho phép chèn và thực thi mã lệnh.	
4	Cisco	CVE-2019-1749 CVE-2019-1750 CVE-2019-1758 CVE-2019-1757 CVE-2019-1746 ……	Nhóm 25 lỗ hổng trên một số sản phẩm của Cisco (các dòng switch Nexus, NX-OS, FXOS Software,) cho phép truy cập và thông tin nhạy cảm lưu trữ trên hệ thống, chèn và thực thi mã lệnh để chiếm quyền kiểm soát.	Đã có thông tin xác nhận 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	149.93.145.16
2	38.229.1.71
3	38.229.128.132
4	38.229.128.136
5	38.229.128.146

6	38.229.128.158
7	38.229.128.241
8	38.229.128.246
9	38.229.128.57
10	38.229.128.88

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

TT	Tên miền/IP	Số lượng
1	localhost.localdomain	708
2	n.hmiblgoja.ru	183
3	ajkeahkcueafuiaeuf.ru	82
4	mokoaehaeihgiaheih.ru	63
5	43trfdsds.com	42
6	iuefgauiaiduihgs.com	34
7	bszotsjovih.com	19
8	strikotunrev.top	17
9	mel.cloudcontentsmak.com	17
10	d3s1.me	16
11	analilaofr.com	15
12	dnshkjashsdk3d11144d.ru	13
13	plpanaifheaighai.com	11

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:

- 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 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.

- 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* 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

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.govvn | 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