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 40 (từ 30/09 - 06/10/2019)

Số: /BC-CATTT *Hà Nội, ngày 08 tháng 10 năm 2019*

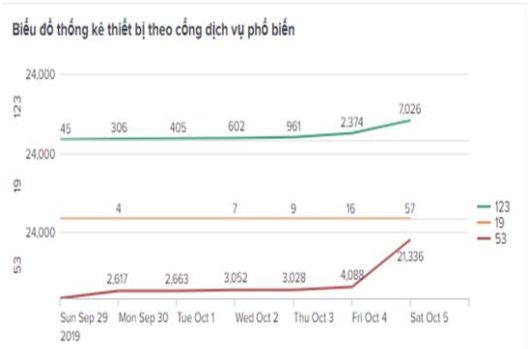
MỘT SỐ BÁO CÁO VỀ VI PHẠM DỮ LIỆU

Theo báo cáo Hacked Off! report của Bitdefender công bố vào ngày 01/10, 57% doanh nghiệp bị vi phạm dữ liệu trong 3 năm qua và 24% đã bị vi phạm dữ liệu trong nửa năm 2019.

CẢNH BÁO TẤN CÔNG TỪ MAGECART – NHÓM HACKER CHUYÊN TẤN CÔNG WEBSITE THƯƠNG MẠI ĐIỆN TỬ

Đầu tháng 10 Mallwarebylab đã cập nhật thông tin về hoạt động của nhóm Magecart - nhóm tội phạm mạng chuyên đánh cắp thông tin thẻ tín dụng trên các trang thương mại điện tử ở nhiều quốc gia trên thế giới.

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 351 lỗ hổng, trong đó có 53 lỗ hổng mức cao, 294 lỗ hổng mức trung bình, 52 lỗ hổng mức thấp và 181 lỗ hổng chưa đánh giá. Trong đó có ít nhất 62 lỗ hổng cho phép chèn và thực thi mã lệnh.

MẠNG XÃ HỘI ĐANG ẢNH HƯỞNG ĐẾN NHIỀU QUỐC GIA TRÊN THẾ GIỚI

Tuần qua, một số báo cáo về mạng xã hội đã cho thấy động thái của các quốc gia liên quan đến việc sử dụng mạng xã hội như một "công cụ" định hướng thông tin từ tất cả các quốc gia lớn nhỏ, phương thức hoạt động khác nhau.

1. Điểm tin đáng chú ý

1.1. Theo báo cáo Hacked Off! report của Bitdefender công bố vào ngày 01/10, 57% doanh nghiệp bị vi phạm dữ liệu trong 3 năm qua và 24% đã bị vi phạm dữ liệu trong nửa năm 2019. Các cuộc tấn công mạng gây ra mối đe dọa lớn nhất đối với các tổ chức trong năm 2019 bao gồm lừa đảo-phishing (36%), trojan (29%), ransomware (28%), rủi ro do tuân thủ (28%), phần mềm chưa được vá (24%), tấn công DDoS (24%) và các mối đe dọa truyền thông xã hội (22%).

Cũng liên quan tới vấn đề vi phạm dữ liệu, một báo cáo mới của Kaspersky cho biết chi phí trung bình của các vi phạm dữ liệu doanh nghiệp đã tăng lên 1,41 triệu đô la trong năm 2018, năm 2017 là 1,23 triệu đô la. Báo cáo chỉ ra rằng các tổ chức có hỗ trợ của Trung tâm giám sát, bảo vệ nội bộ (như SOC) có thể góp phần giảm một nửa thiệt hại tài chính của các vi phạm dữ liệu doanh nghiệp từ 1,4 triệu đô la xuống chỉ còn 675.000 đô la. Theo Kaspersky, các tổ chức doanh nghiệp đã đầu tư nhiều hơn vào an toàn thông tin mạng trong năm 2019, với ngân sách bảo mật CNTT trung bình là 18,9 triệu đô la so với 8,9 triệu đô la trong năm 2018.

1.2. Tuần qua, một số báo cáo về mạng xã hội đã cho thấy động thái của các quốc gia liên quan đến việc sử dụng mạng xã hội như một "công cụ" định hướng thông tin từ tất cả các quốc gia lớn nhỏ với nhiều phương thức hoạt động khác nhau. Theo báo cáo truyền thông qua mạng xã hội năm 2019 của Viện Internet thuộc đại học Oxford, nhiều quốc gia đã sử dụng các mạng xã hội để định hướng các thông tin trong nước. Một số quốc gia còn sử dụng các công cụ này để ảnh hưởng tới truyền thông của các quốc gia khác.

Cũng liên quan tới vấn đề mạng xã hội, các nền tảng mạng xã hội có trụ sở tại Hoa Kỳ bao gồm Facebook và WhatsApp có thể sẽ bị buộc phải chia sẻ tin nhắn được mã hóa của người dùng với cảnh sát Anh theo một hiệp ước mới giữa hai nước. Tuy nhiên Facebook đã bác bỏ việc này và cho biết các báo cáo về việc WhatsApp, Messenger sẽ chia sẻ tin nhắn được mã hóa cho cảnh sát Anh là không chính xác.

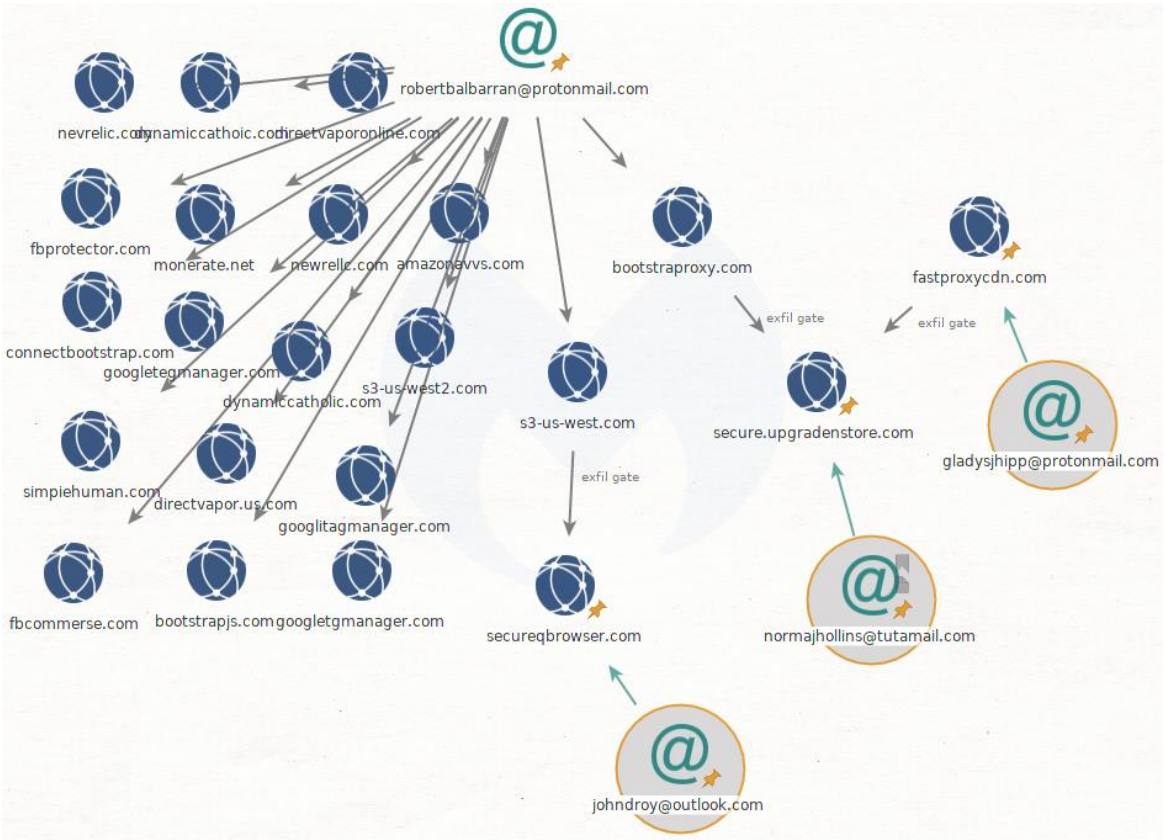
1.3. Đầu tháng 10 Mallwarebylab đã cập nhật thông tin về hoạt động của nhóm Magecart - nhóm tội phạm mạng chuyên đánh cắp thông tin thẻ tín dụng trên các trang thương mại điện tử ở nhiều quốc gia trên thế giới. Kịch bản tấn công nhóm này thường sử dụng như sau:

- Xâm nhập/tấn công các trang web thương mại điện tử;

- Chèn các đoạn mã Javascript trên các trang web này;

- Khi người dùng nhập thông tin trên những trang này thì đoạn mã đã chèn vào trang web sẽ tự động đánh cắp thông tin để truyền về máy chủ điều khiển.

Mangercart cũng đã được nhiều công ty bảo mật lớn thực hiện theo dõi và phân tích từ năm 2018. Kể từ đó đã có nhiều chiến dịch tấn công tương tự được thực hiện. Một cuộc tấn công tự động, có thể khai thác và xâm nhập hơn 960 trang web.



Magecart thường nhằm mục tiêu vào các nhà cung cấp bên thứ 3 sử dụng những tên miền giống với tên miền hợp pháp của nhà cung cấp dịch vụ, phân tích dữ liệu

(như facebook77-cdn[.]com, msdn-cdn[.]com, google-services-s5[.]com) để phục vụ cho các chiến dịch tấn công.

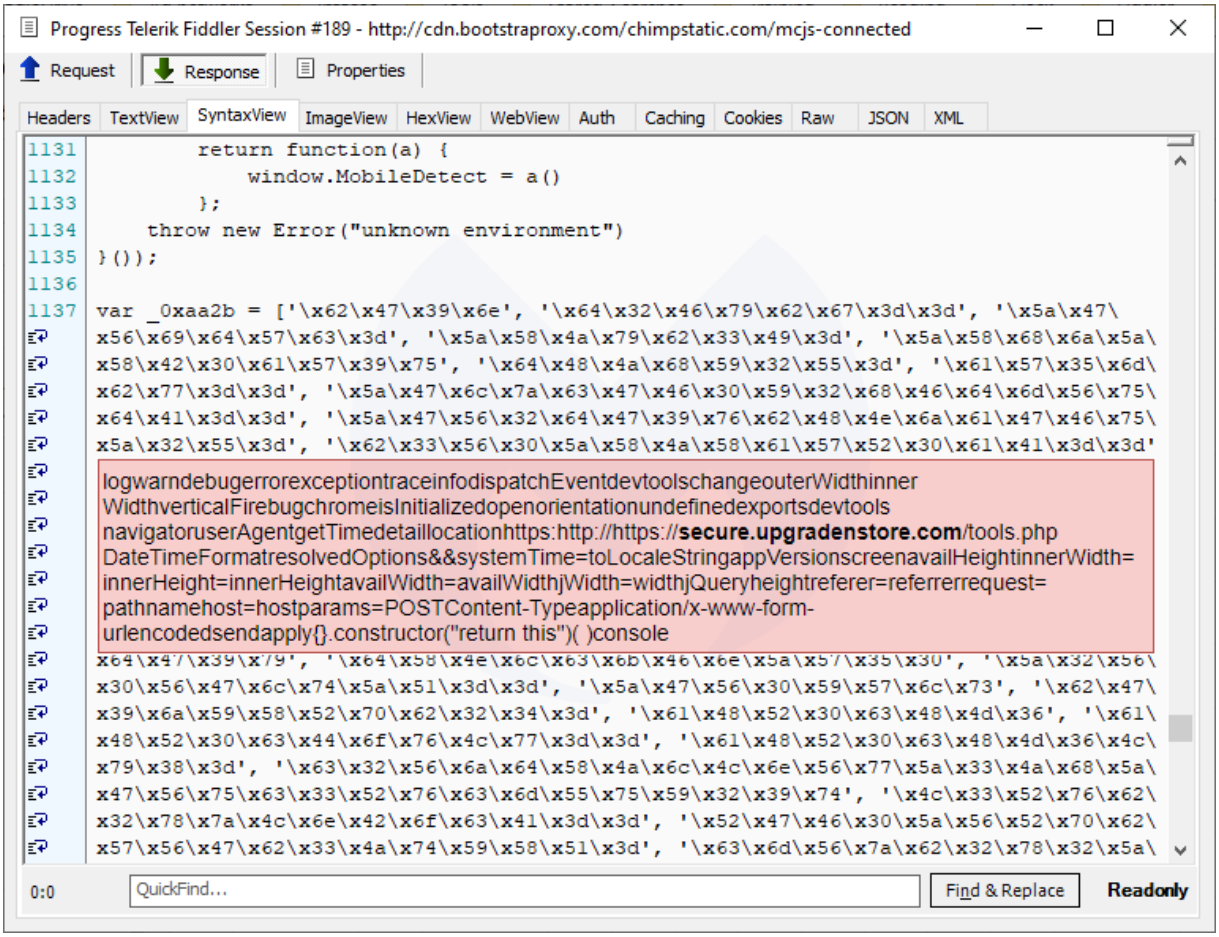
Nhiều nhóm Magecart được theo dõi vẫn đang tập trung vào nền tảng mua sắm Magento (là mục tiêu chính khi các cuộc tấn công này bắt đầu nhân lên). OpenCart cũng được những kẻ tấn công đặc biệt quan tâm.

Ngoài ra, Magacart còn sử dụng nhiều kỹ thuật tinh vi, làm rối mã gây khó khăn trong phát hiện và phân tích.

Magecart tấn công các máy người dùng và máy chủ qua skimmer (là một loại thiết bị siêu nhỏ cho phép đối tượng tấn công chụp hình và thu lại những thao tác khi người dùng thẻ thực hiện mà không cần phải hiểu biết quá nhiều về thủ thuật công nghệ cao hay máy tính).

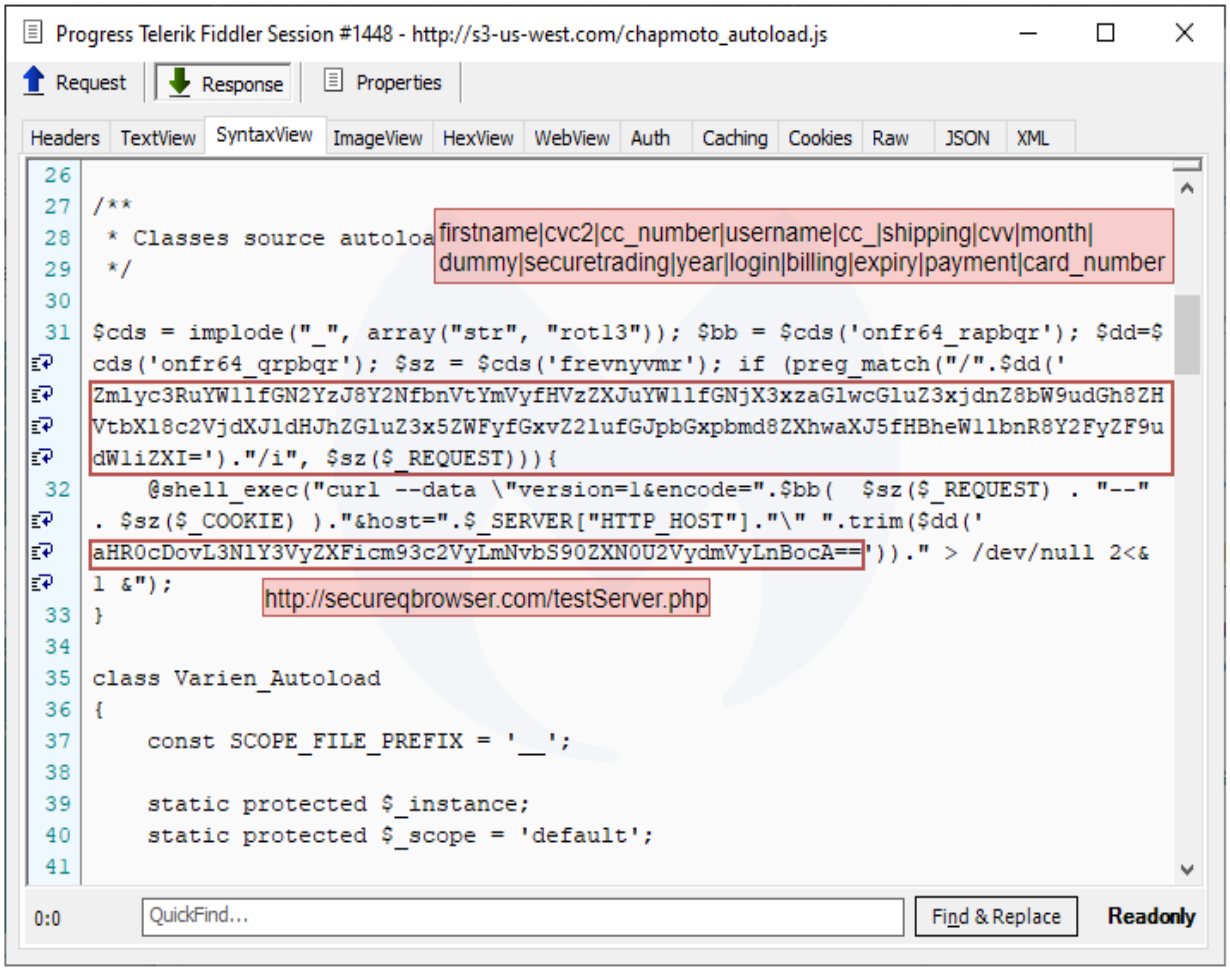
Client-side skimmer

Một trong những skimmers nhóm này đã sử dụng có liên kết với tên miền jquery.mask.js. Mã độc này được thêm vào phần cuối của scirpt, và sử dụng kỹ thuật làm rối mã gây khó khăn cho việc phát hiện.



Server-side skimmer

Khi kiểm tra hạ tầng của Magecart, các chuyên gia đã phát hiện một đoạn mã PHP nhìn giống nhau một đoạn Javascript nếu không phân tích kỹ. Đoạn mã này thực hiện tìm kiếm các từ khóa có liên quan đến giao dịch tài chính, lấy trộm thông tin Cookie và gửi về máy chủ điều khiển. Ví dụ hình dưới sẽ thực hiện đánh cắp thông tin và gửi về máy chủ secureqbrowser[.]com



Cả tên miền client-side và server-side skimmer được sử dụng trên (bootstraproxy [.] Com và s3-us-west [.] Com) được đăng kí vào robertbalbarran@protonmail.com, để kết nối giữa người đăng kí email và cổng exfiltration, bằng cách đẩy tội phạm mạng có thể thu thập các tên miền khác của người dùng.

Thông tin chi tiết có thể tham khảo tại:

https://ti.khonggianmang.vn/dashboard/news/p/canh-bao-tan-cong-tu-magecart/

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 351 lỗ hổng, trong đó có 53 lỗ hổng mức cao, 294 lỗ hổng mức trung bình, 52 lỗ hổng mức thấp và 181 lỗ hổng chưa đánh giá. Trong đó có ít nhất 62 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 06 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 04 lỗ hổng trên Adobe, nhóm 09 lỗ hổng trên hệ điều hành Linux, nhóm 01 lỗ hổng trên thiết bị Dlink, Nhóm 257 lỗ hổng trên Android, Nhóm 43 lỗ hổng trong Cisco, Nhóm 01 lỗ hổng trong hệ thống Wordpress, Nhóm 20 lỗ hổng trên Firefox… Thông tin chi tiết về một số lỗ hổng trên các sản phẩm/dịch vụ phổ biến tại Việt Nam cụ thể như sau:

TT	Sản phẩm/dịch vụ	Mã lỗi quốc tế	Mô tả ngắn	Ghi chú
1	Adobe	CVE-2019-8073 CVE-2019-8074 CVE-2019-8072 CVE-2019-8075	Nhóm 04 lỗ hổng trên một số sản phẩm, thành phần của Adobe (Coldfusion, Flash Player ...) cho phép đối tượng tấn công thu thập thông tin trái phép, thực thi mã lệnh từ xa. 02 lỗ hổng có điểm đặc biệt nghiêm trọng là 10.0	Đã có thông tin xác nhận và bản vá
2	Linux	CVE-2019-16994 CVE-2019-16995 CVE-2019-17054 …	Nhóm 09 lỗ hổng trên hệ điều hành Linux (linux_kernel) cho phép đối tượng tấn công thực thi mã lệnh tùy ý, thu thập thông tin, tấn công từ chối dịch vụ.	Chưa có thông tin xác nhận và bản vá
3	Dlink	CVE-2019-16920	Nhóm 01 lỗ hổng trên một số sản phẩm của thiết bị Dlink (DIR-655C, DIR-652, DIR-886L…) cho phép đối tượng tấn công thực thi mã lệnh từ xa, có được quyền truy cập hệ thống. Lỗ hổng có điểm đặc biệt nghiêm trọng là 10.0	Đã có thông tin xác nhận và bản vá

4	Android	CVE-2019-9259 CVE-2019-9266 CVE-2019-9301 …	Nhóm 257 lỗ hổng trên một số sản phẩm của Android (Android -10Android ID:A-112610994...) cho phép đối tượng tấn công thu thập thông tin trái phép, thực thi mã lệnh từ xa, làm tràn bộ đệm, tấn công từ chối dịch vụ	Đã có thông tin xác nhận và bản vá
5	Cisco	CVE-2019-12713 CVE-2019-12678 CVE-2019-12698 …	Nhóm có 43 lỗ hổng trên một số sản phẩm của Cisco (Cisco Adaptive Security Appliance Softwere, Firepower Threat Defense Software) cho phép đối tượng thực hiện tấn công XSS, tấn công tấn công từ chối dịch vụ, thực thi mã lệnh từ xa, thu thập thông tin trái phép	Chưa có thông tin xác nhận và bản vá
6	Wordpress	CVE-2019-16931	Nhóm có 01 lỗ hổng trên một số sản phẩm, thành phần của Wordpress cho phép đối tượng tấn công thực thi mã lệnh tùy ý , tấn công qua XSS	Chưa có thông tin xác nhận và bản vá
7	Firefox	CVE-2019-11736 CVE-2019-11737 CVE-2019-11741	Nhóm có 20 lỗ hổng trên một số sản phẩm, thành phần của Firefox (Firefox<69, Firefox ESR<68.1…) cho phép đối tượng tấn công thực thi mã lệnh tùy ý, đánh cắp mật khẩu và xóa dữ liệu đã sử dụng của người dùng, tấn công UXSS. Có một số lỗ hổng mức nghiêm trọng cao (9.3 và 7.5)	Đã có thông tin xác nhận và bản vá

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

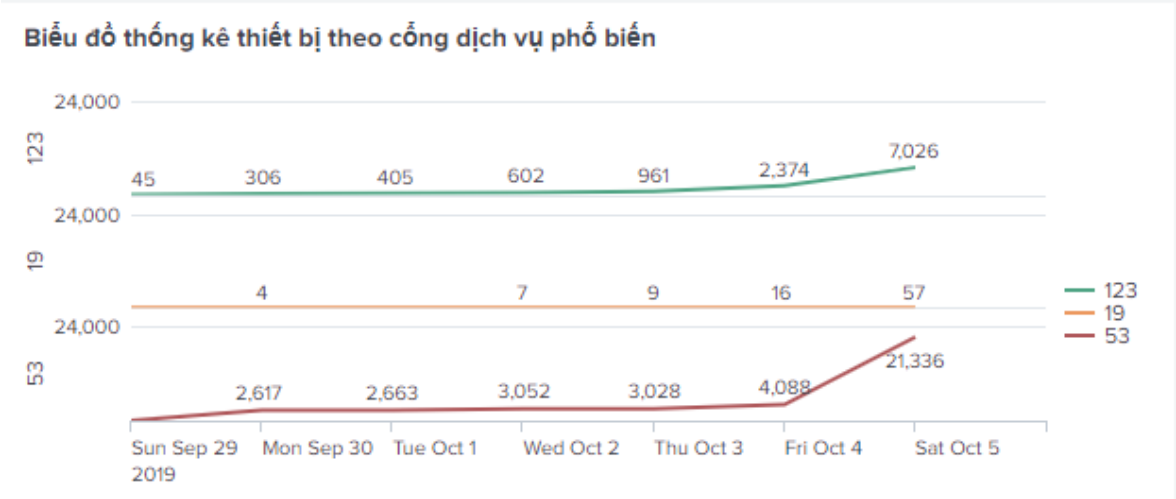
Tấn công từ chối dịch vụ là hình thức tấn công đã có từ lâu, và hiện tại vẫn được đối tượng tấn công ưa thích sử dụng để thực hiện các ý đồ xấu. Tấn công từ chối dịch vụ về cơ bản không nguy hiểm nhưng lại gây ảnh hưởng đến hoạt động của hệ thống, gây thiệt hại về kinh tế cho tổ chức bị tấn công.

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
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

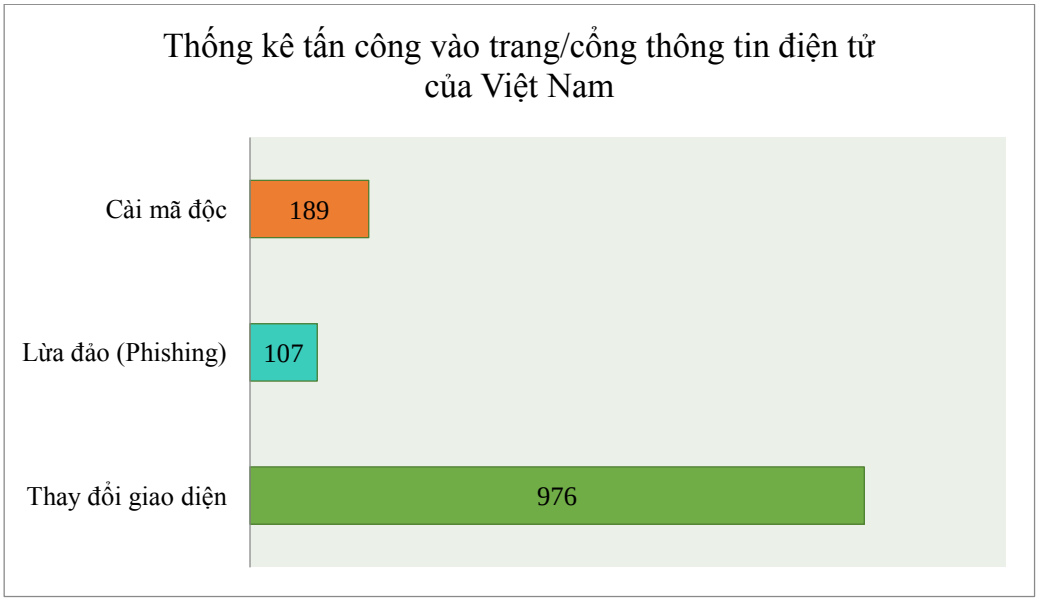
Tại Việt Nam, có rất nhiều máy chủ, thiết bị có thể trở thành nguồn phát tán tấn công DRDoS. Trong tuần có **48.596 (tăng so với tuần trước là 44,638)** thiết bị có khả năng bị huy động và trở thành nguồn tấn công DRDoS. Các thiết bị này đang mở sử dụng các dịch vụ NTP (123), DNS (53), Chargen (19). Dưới đây là biểu đồ thống kê thiết bị theo cổng dịch vụ phổ biến trong tuần.



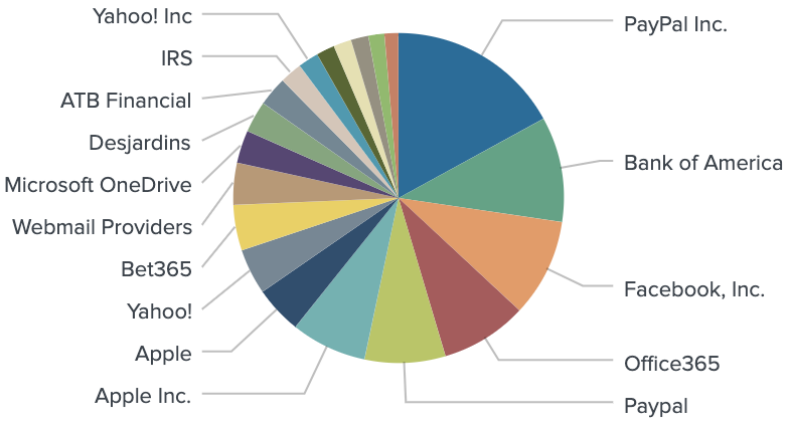
4. Tấn công vào Cổng TTĐT/ứng dụng web của Việt Nam

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 1332 trường hợp tấn công vào trang/cổng thông tin điện tử của Việt Nam: 976 trường hợp tấn công thay đổi giao diện, 107 trường hợp tấn công lừa đảo (Phishing), 249 trường hợp tấn công cài cắm mã độc.



Bonus: *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.*

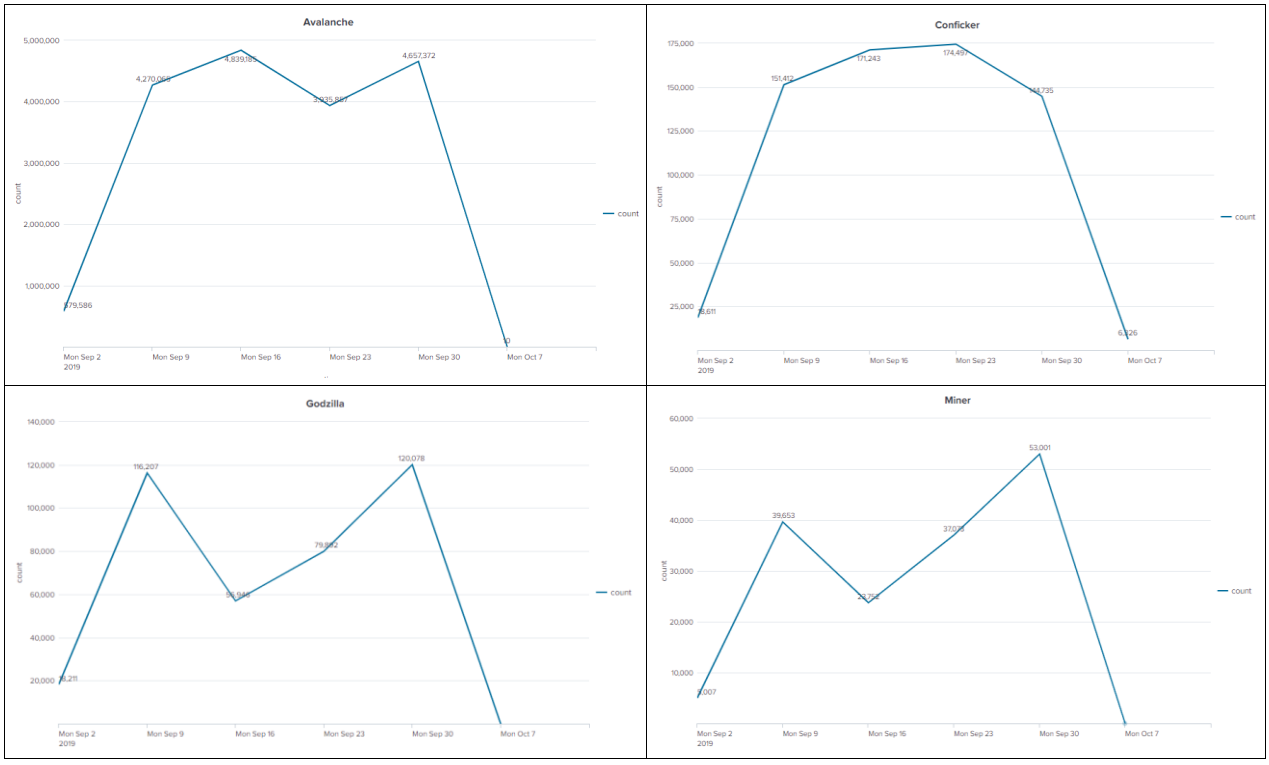


TOP tổ chức bị nhiều trang web giả mạo

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 nhiều nhất và tăng so với tuần trước, có 4.657.372 lượt địa chỉ IP kết nối (từ 771.745 địa chỉ IP) với máy chủ điều khiển (Tuần 39 là 3.935.857).

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

TT	Tên miền/IP
1	disorderstatus.ru
2	differentia.ru
3	atomictrivia.ru
4	soplifan.ru
5	ld3t8xao8.ru
6	xjpakmdcfuqe.com

7	xdqzpbcgrvkj.ru
8	www.iuqerfsodp9ifjaposdfjhgosurijfaewrwergwea.com
9	cp.x1yuqjh9.ru
10	yrwyzgopwjug.info
11	www.cityofangelsmagazine.com
12	morphed.ru
13	kvamuvsju.ru
14	somicrososoft.ru

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./.

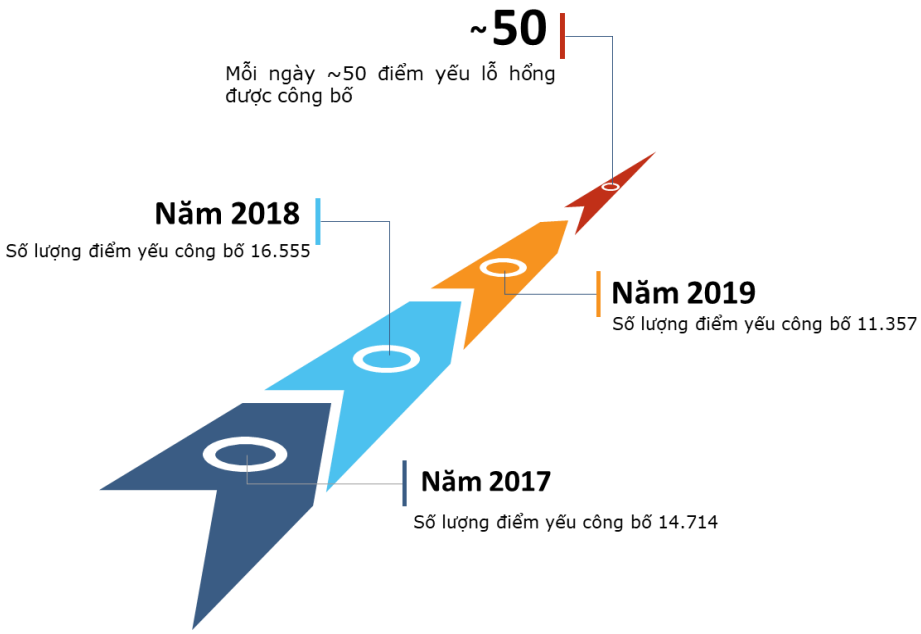
CỤC AN TOÀN THÔNG TIN

HỆ THỐNG

CẢNH BÁO ĐIỂM YẾU VÀ RÀ SOÁT LỖ HỔNG BẢO MẬT TỰ ĐỘNG

https://service.khonggianmang.vn/

Hiện nay, nguy cơ tấn công mạng thông qua điểm yếu, lỗ hổng đối với tổ chức, doanh nghiệp ngày càng gia tăng mạnh.

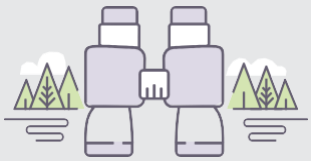


"**Hệ thống Cảnh báo điểm yếu và Rà soát lỗ hổng bảo mật tự động**" tự động rà soát lỗ hổng bảo mật và cảnh báo điểm yếu sớm nhất, cập nhật nhất cho tổ chức, doanh nghiệp.

Kho dữ liệu cập nhật mới nhất

Threat Intelligence Basic

Modul cảnh báo, theo dõi và tra cứu các mối nguy hại, phát hiện các kết nối độc hại và nguy cơ bị tấn công mạng.



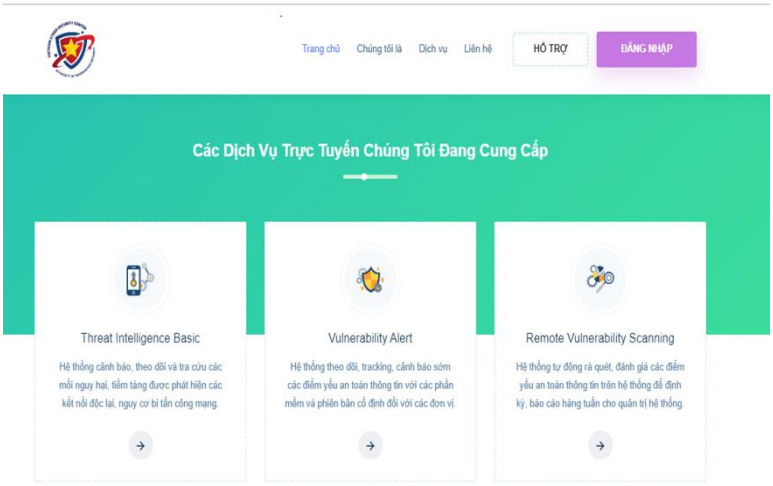
Vulnerability Alert

Modul theo dõi, tracking, cảnh báo sớm các điểm yếu an toàn thông tin với các phần mềm và phiên bản cố định đối với các tổ chức.

Remote Vulnerability Scanning

Modul tự động rà quét, đánh giá các điểm yếu an toàn thông tin trên hệ thống để định kỳ, báo cáo hàng tuần cho quản trị hệ thống.

CHỨC NĂNG HỆ THỐNG DỊCH VỤ TRỰC TUYẾN



Vulnerability Alert

» Cảnh báo điểm yếu bảo mật đến từng phiên bản sản phẩm mà tổ chức đang sử dụng.

» Cung cấp thông tin giải pháp, khuyến nghị với từng lỗ hổng, điểm yếu.

Threat Intelligence Basic

» Giám sát các kết nối độc hại, nguy cơ với các địa chỉ IP tổ chức đang sử dụng.

Remote Vulnerability Scanning

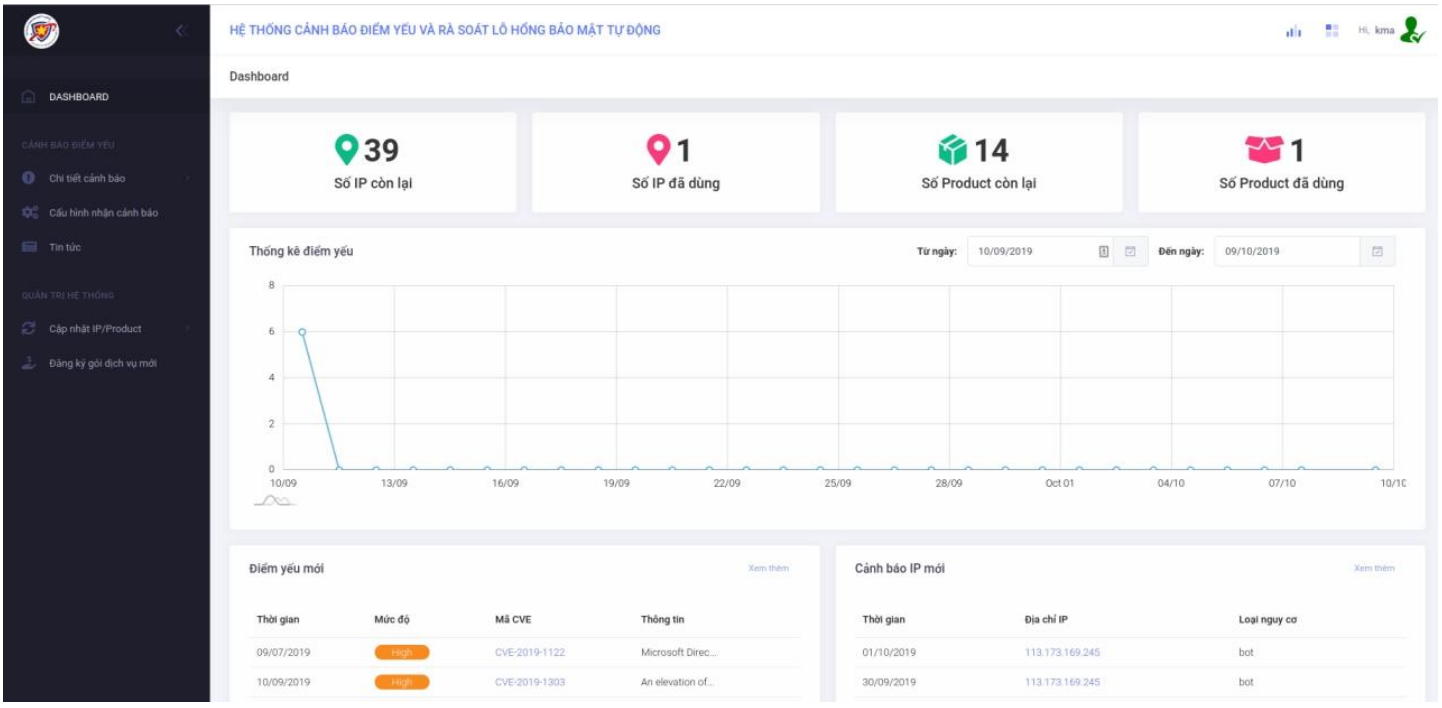
» Tự động rà quét, đánh giá các điểm yếu an toàn thông tin.

» Thiết lập Product/IP cần theo dõi, giám sát.

» Theo dõi thông tin cảnh báo và khắc phục lỗ hổng ngay khi nhận được thông tin cảnh báo

Dashboard hệ thống

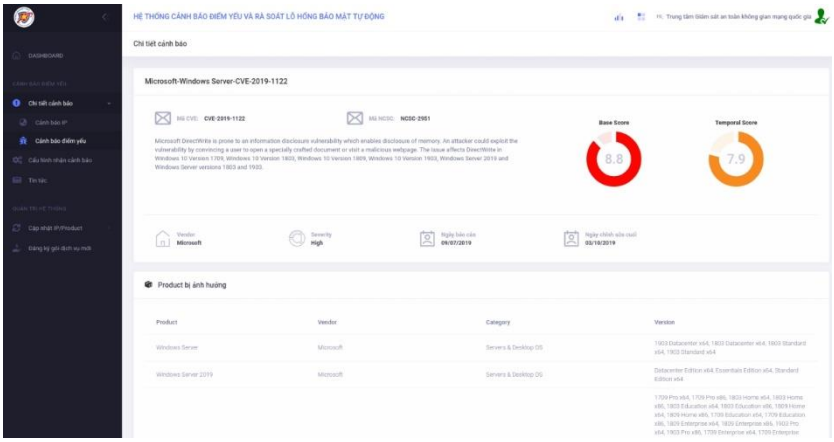
» Hệ thống hiển thị số lượng sản phẩm, IP, gói đăng ký và người dùng.



CHỨC NĂNG HỆ THỐNG DỊCH VỤ TRỰC TUYẾN

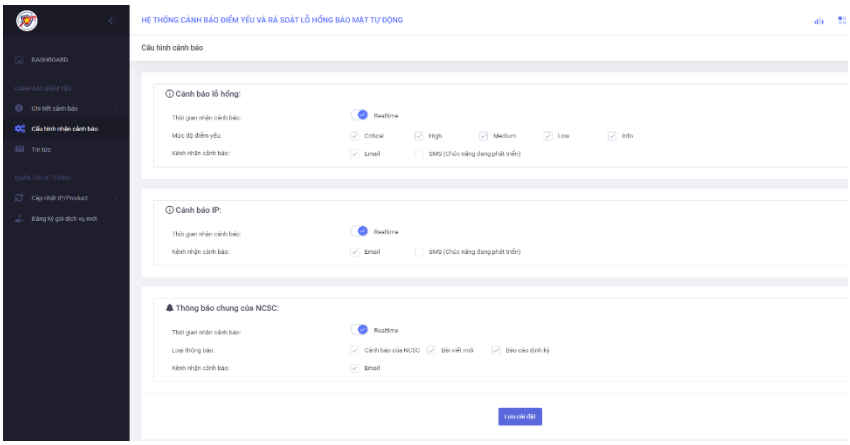
Chi Tiết Cảnh Báo

» Hệ thống hiển thị thông tin chi tiết cảnh báo IP, điểm yếu. Danh sách sản phẩm và thống kê điểm yếu theo mức độ.



Cảnh báo tức thì theo từng sản phẩm

» Thiết lập tùy chỉnh cấu hình nhận cảnh báo lỗ hổng và IP theo mức độ, thời gian và kênh nhận cảnh báo.



Tin tức và báo cáo định kỳ

» Cập nhật những tin tức mới nhất về lỗ hổng bảo mật, phân tích kỹ thuật chuyên sâu và báo cáo định kỳ.

Đặt lịch rà soát và đánh giá

» Đặt lịch định kỳ để rà soát và đánh giá IP của tổ chức.

ĐIỂM ĐẶC BIỆT

- Dễ dàng triển khai và sử dụng
- Tiết kiệm chi phí của Doanh nghiệp
- Cảnh báo sớm rủi, nguy cơ
- Tự động rà quét, đánh giá các điểm yếu
- Thông tin kỹ thuật nóng cập nhật
- Nguồn dữ liệu phong phú
- Hỗ trợ 24/7/365
- Cung cấp nhiều loại báo cáo

Trung tâm Giám sát an toàn không gian mạng Quốc gia (NCSC)
Cục An toàn thông tin
Điện thoại: 024 32091616
Email: ncsc@ais.gov.vn