CẢNH BÁO

TUẦN 43 (21/10/2019 - 27/10/2019)

Số: /BC-CATTT *Hà Nội, ngày 28 tháng 10 năm 2019*

Tin tức

- Trung Quốc tổ chức Hội nghị Internet thế giới Lần thứ 6.

- Thành lập liên minh an toàn, an ninh mạng công nghệ mới (OTCSA).

- Lỗ hổng trong trình hiển thị Timelion của Kibana cho phép thực thi mã lệnh từ xa

Điểm yếu lỗ hổng

Nguy cơ tấn công từ các điểm yếu lỗ hổng vào hệ thống, phần mềm.

Thống kê

Thống kê nguy cơ tấn công mạng.

Khuyến nghị

Khuyến nghị đối với các cơ quan, đơn vị.

RSG

Báo cáo tài liệu chuyên ngành.

TRUNG TÂM GIÁM SÁT AN TOÀN KHÔNG GIAN MẠNG QUỐC GIA

Trung Quốc tổ chức Hội nghị Internet lần thứ 6

Trong tuần qua, Trung Quốc đã tổ chức Hội nghị Internet thế giới lần thứ 6, còn được gọi là Hội nghị thượng đỉnh Wuzhen, được tổ chức từ năm 2014. Đây là diễn đàn thường niên do chính phủ Trung Quốc tổ chức nhằm thúc đẩy ý tưởng quản trị Internet toàn cầu; thúc đẩy chủ quyền không gian mạng và tiến bộ trong công nghệ AI, 5G.

Hội nghị năm nay, các chuyên gia ATTT mạng của Trung Quốc cũng đã phát hành một bài viết phác thảo các nguyên tắc thực hành chủ quyền không gian mạng, kêu gọi các quốc gia bảo vệ chủ quyền mạng và phát triển các quy tắc được chấp nhận rộng rãi cho không gian mạng.

Bài viết phản ánh ý kiến của các chuyên gia trong hội nghị, những người đã thúc đẩy các tiêu chuẩn an ninh mạng cao hơn cũng như sự hợp tác lớn hơn giữa các quốc gia và các công ty Internet để chống lại các mối đe dọa trong không gian mạng.

Source:

https://www.scmp.com/economy/china-economy/article/3033783/google-and-facebook-stay-away-smaller-us-firms-scout-business

Thành lập liên minh an toàn, an ninh mạng công nghệ mới (OTCSA)

Ngày 22/10, 12 nhà cung cấp dịch vụ và phần mềm an toàn, an ninh mạng đã cùng nhau thành lập một liên minh toàn cầu có tên là Liên minh an toàn, an ninh mạng công nghệ mới (OTCSA). Liên minh này sẽ tập trung vào việc bảo vệ các công nghệ điều khiển vận hành trong cơ sở hạ tầng quan trọng và công nghiệp khỏi các mối đe dọa trên mạng. Công ty có các hoạt động vận hành hệ thống OT hoặc cơ sở hạ tầng quan trọng đều có thể tham gia với tư cách là thành viên.

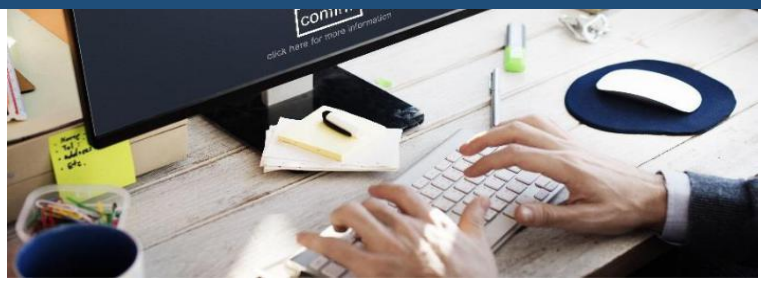
OTCSA sẽ áp dụng cách tiếp cận năm hướng để giảm thiểu nguy cơ tấn công mạng: (1) Tăng cường khả năng, giảm thiểu rủi ro không gian mạng cho các môi trường và giao diện OT cho khả năng kết nối OT/IT; (2) Hướng dẫn các nhà khai thác OT về cách bảo vệ cơ sở hạ tầng OT của họ dựa trên quy trình quản lý rủi ro và các kiến trúc/thiết kế tham chiếu tuân thủ nghiêm ngặt các quy định và tiêu chuẩn quốc tế.

(3) Hướng dẫn các nhà cung cấp OT về kiến trúc hệ thống OT an toàn, giao diện liên quan và chức năng bảo mật; (4) Hỗ trợ mua sắm, phát triển, lắp đặt, vận hành, bảo trì và triển khai cơ sở hạ tầng quan trọng an toàn hơn; (5) Các thành viên của liên minh toàn cầu sẽ tìm cách đẩy nhanh thời gian áp dụng để các cơ sở hạ tầng quan trọng được an toàn hơn.

Source:

https://www.infosecurity-magazine.com/news/otcsa-launched/

Lỗ hổng trong trình hiển thị Timelion của Kibana cho phép thực thi mã lệnh từ xa



Kibana là một nguồn mở được xây dựng chạy như là một web UI. Kibana kết hợp với Elasticsearch để phục vụ cho các tác vụ tìm kiếm, phân tích big data và log stream phức tạp.

Vào ngày 21/10/2019, các chuyên gia nghiên cứu về an toàn thông tin mạng đã công bố cách thức khai thác lỗ hổng (CVE-2019-7609) trong trình hiện thị Timelion của Kibana. Đây là lỗ hổng đã được công bố vào ngày 25/3/2019 cho phép đối tượng tấn công truy cập ứng dụng Timelion để gửi yêu cầu thực thi mã javascript có thể dẫn đến thực thi các lệnh tùy ý quyền của Kibana trên hệ thống máy chủ.

Đây là lỗ hổng nghiêm trọng (có điểm CVSS:10.0), ảnh hưởng đến các phiên bản Kibana trước 5.6.15 và 6.6.1.

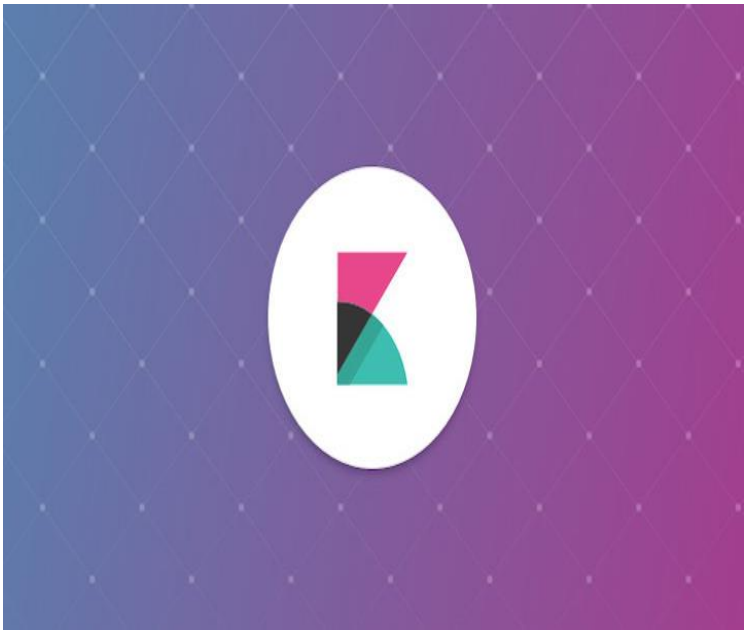
Qua đánh giá sơ bộ của Trung tâm Giám sát an toàn không gian mạng quốc gia, có khoảng 26.256 máy chủ đang công khai dịch vụ Kibana trên Internet, trong đó có nhiều máy chủ của Việt Nam.

Source:

https://www.tenable.com/blog/cve-2019-7609-exploit-script-available-for-kibana-remote-code-execution-vulnerability

Hiện tại lỗ hổng trong Kibana đã có bản vá, các cơ quan tổ chức đang sử dụng Kibana có thể nâng cấp để vá lỗ hổng bảo mật.

Trong trường hợp không thể nâng cấp, có thể vô hiệu hóa tính năng Timelion.



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 265 lỗ hổng, trong đó có 14 lỗ hổng mức cao, 100 lỗ hổng mức trung bình, 08 lỗ hổng mức thấp và 143 lỗ hổng chưa đánh giá. Trong đó có 21 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: 01 lỗ hổng trên hệ điều hành Linux, Nhóm 15 lỗ hổng trên Adobe, Nhóm 45 lỗ hổng trên WordPress, nhóm 02 lỗ hổng trên một số sản phẩm của Apache, Nhóm 03 lỗ hổng trên thiết bị D-Link, Nhóm 06 lỗ hổng trên thiết bị TP-Link, 01 lỗ hổng trên Google, Nhóm 08 lỗ hổng trên Foxit-software… Thông tin chi tiết về một số lỗ hổng trên các sản phẩm/dịch vụ phổ biến tại Việt Nam cụ thể như sau:

Một số lỗ hổng trên các sản phẩm/dịch vụ phổ biến tại Việt Nam:

- *Adobe: CVE-2019-8238, CVE-2019-8088. v.v..*
- *Linux: CVE-2019-18198.*
- *D-Link: CVE-2013-4856, CVE-2013-4855,vv…*
- *TP-Link: CVE-2019-13653, CVE-2019-13650 v.v..*
- *Wordpress: CVE-2015-9497,CVE-2015-9496 v.v..*
- *Apache: CVE-2019-10079, CVE-2019-12415 v.v..*

Thông tin điểm yếu lỗ hổng

STT	Sản phẩm/dịch vụ	Mã lỗi quốc tế	Mô tả ngắn	Ghi chú
1	Linux	CVE-2019-18198	01 lỗ hổng trên hệ điều hành Linux (Linux kernel) cho phép đối tượng tấn công khai thác bộ nhớ FIB-LOOKUP-NOREF, chèn và thực thi mã lệnh tùy ý, tấn công từ chối dịch vụ	Đã có thông tin xác nhận và bản vá
2	Adobe	CVE-2019-8238 CVE-2019-8088 CVE-2019-8087	Nhóm 15 lỗ hổng trên một số thành phần, sản phẩm của Adobe (Experience Manager Forms, Acrobat and Reader) cho phép đối tượng tấn công thu thập thông tin, chèn và thực thi mã lệnh tùy ý. Ảnh hưởng đến nhiều phiên bản Adobe.	Đã có thông tin xác nhận và bản vá.
3	WordPress	CVE-2015-9497 CVE-2015-9496 CVE-2015-9531 …	Nhóm 45 lỗ hổng trên nhiều thành phần của WordPress (The Easy Digital Downloads PDF Stamper extension..) cho phép đối tượng tấn công khai thác lỗi XSS	Đã có thông tin xác nhận và bản vá
4	Apache	CVE-2019-10079 CVE-2019-12415	Nhóm 02 lỗ hổng trên Apache (Traffic Server, POI) cho phép đối tượng tấn công thu thập thông tin	Đã có thông tin xác nhận và bản vá
5	D-Link	CVE-2013-4856 CVE-2013-4855 CVE-2013-4857	Nhóm 03 lỗ hổng trên thiết bị D-Link (DIR-865L)cho phép đối tượng tấn công chèn và thực thi mã lệnh qua nhiều thành phần khác nhau	Chưa có thông tin xác nhận và bản vá
6	Google	CVE-2016-5202	Lỗ hổng trên Goole (Google Chrome)cho phép đối tượng tấn công truy cập trái phép thu thập thông tin	Chưa có thông tin xác nhận và bản vá
7	TP-Link	CVE-2019-13653 CVE-2019-13650 CVE-2013-4848	Nhóm 06 lỗ hổng trên thiết bị TP-Link (M7350) cho phép đối tượng tấn công chèn và thực thi mã lệnh từ xa	Chưa có thông tin xác nhận và bản vá
8	Foxit-software	CVE-2019-17141 CVE-2019-17139 CVE-2019-17145	Nhóm 08 lỗ hổng trên phần mềm Foxit-software (PhantomPDF 9.6.0.25114, PhantomPDF 9.5.0.20732…) cho phép đối tượng tấn công thực thi mã lệnh tùy ý , hướng mục tiêu truy cập trang web độc hại.	Chưa có thông tin xác nhận và bản vá

Thông tin chi tiết lỗ hổng, điểm yếu lưu ý

CVE-2019-11043

Ngày 22/10, chuyên gia bảo mật Omar Ganiev đã thông báo qua Twitter về một lỗ hổng thực thi mã từ xa mới trong PHP-FPM. Lỗ hổng có mã là CVE-2019-11043 với thang điểm nghiêm trọng CVSS v3.1 là 9.8.

Theo các nhà nghiên cứu, lỗ hổng cho phép kẻ tấn công chạy các lệnh trên máy chủ chỉ bằng cách truy cập một URL được thiết kế đặc biệt.

Hiện tại không phải tất cả các máy chủ web PHP đều bị ảnh hưởng. Chỉ các máy chủ NGINX có bật PHP-FPM là dễ bị tấn công.

Lỗ hổng ảnh hưởng đến các phiên bản PHP 7.1.x – 7.1.33, 7.2.x – 7.2.24, 7.3.x – 7.3.11

Source:

https://nvd.nist.gov/vuln/detail/CVE-2019-11043
https://www.zdnet.com/article/nasty-php7-remote-code-execution-bug-exploited-in-the-wild/

CVE-2019-17666

Nhà nghiên cứu bảo mật Nicolas Waisman đã công bố mã bằng chứng khai thác một lỗ hổng Wi-Fi trên hệ điều hành Linux được tiết lộ gần đây.

Lỗ hổng nằm trong trình điều khiển **rtlwife** của các mô-đun Wi-Fi Realtek được xác định với mã lỗi CVE-2019-17666 với thang điểm cao CVSS v3.0 là 8.8. Khi khai thác, chúng cho phép kẻ tấn công có thể xâm nhập hệ thống bằng các thiết bị Wi-Fi gần đó.

Linux đã thông báo lỗ hổng sẽ ảnh hưởng đến phiên bản 5.3.6.

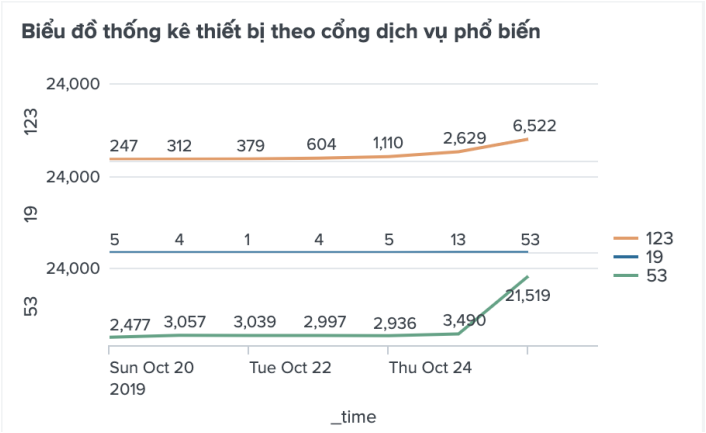
Source:

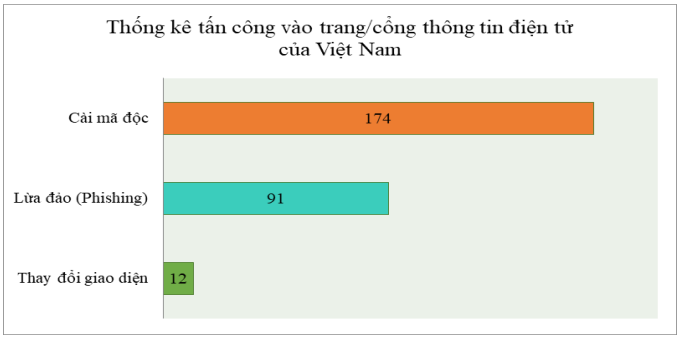
https://nvd.nist.gov/vuln/detail/CVE-2019-17666
https://www.secpod.com/blog/linux-kernel-vulnerability/

Thống kê nguy cơ, các cuộc tấn công tại Việt Nam

Tấn công DRDoS

Tuần vừa qua tại Việt Nam, có rất nhiều máy chủ, thiết bị có thể trở thành nguồn phát tán tấn công DRDoS. Trong tuần có **51.403** (tăng so với tuần trước là **44.673**) 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.



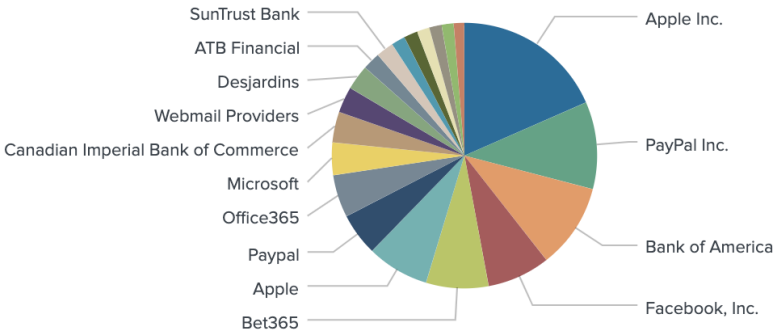


Tấn công Web

Trong tuần, có 316 trường hợp tấn công vào trang/cổng thông tin điện tử của Việt Nam: 2 trường hợp tấn công thay đổi giao diện, 84 trường hợp tấn công lừa đảo (Phishing), 230 trường hợp tấn công cài cắm mã độc.

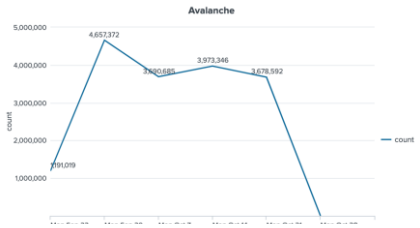
Tấn công Phishing

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.



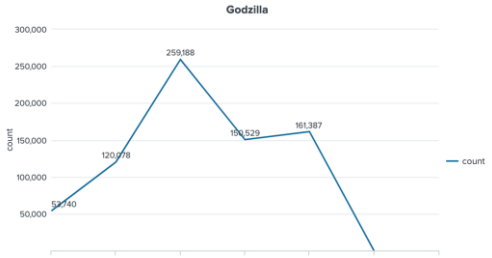
Thống kê nguy cơ, các cuộc tấn công tại Việt Nam

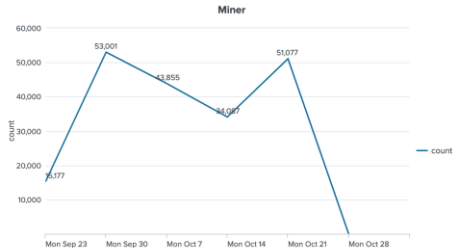
Trong tuần mạng botnet **Avalanche** có 3.678.592 lượt địa chỉ IP kết nối với máy chủ điều khiển giảm so với tuần 42 là 3.973.346.



Trong tuần mạng botnet **Conficker** có 138.534 lượt địa chỉ IP kết nối với máy chủ điều khiển giảm so với tuần 42 là 157.894.

Trong tuần mạng botnet **Godzilla** có 161.387 lượt địa chỉ IP kết nối với máy chủ điều khiển tăng so với tuần 42 là 150.528.





Trong tuần mạng botnet **Miner** có 51.077 lượt địa chỉ IP kết nối với máy chủ điều khiển tăng so với tuần 42 là 34.087.

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

disorderstatus.ru	www.cityofangelsmagazine.com
differentia.ru	morphed.ru
atomictrivia.ru	somicrososoft.ru
soplifan.ru	hw1l3gvj.ru
l677e13te.ru	evbvhzmb.info
xjpakmdcfuqe.com	cs.chromlum.net
xdqzpbcgrvkj.ru	www.corpnox-technologie.fr

Khuyến nghị đối với các cơ quan, đơn vị

HẠN CHẾ TẤN CÔNG TỪ CHỐI DỊCH VỤ

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.

PHÒNG TRÁNH TẤN CÔNG WEB

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.

CẬP NHẬT BẢN VÁ LỖ HỔNG

Theo dõi và cập nhật bản vá cho các lỗ hổng, đặc biệt là lỗ hổng nêu tại mục 2 báo cáo này.

LƯU Ý KIỂM TRA VÀ XỬ LÝ CÁC TÊN MIỀN ĐỘC HẠI

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.

CHỦ ĐỘNG KIỂM TRA, RÀ SOÁT, BÓC GỠ MÃ ĐỘC

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:
Trung tâm Giám sát an toàn không gian mạng quốc gia
024.3209.1616 - ais@mic.gov.vn
Tầng 16, số 115 Trần Duy Hưng, quận Cầu Giấy, Tp. Hà Nội

RSG – Báo cáo, tài liệu chuyên nghành

(1) Số liệu cứ 15 phút lại có 2000 cuộc tấn công

https://s3-eu-central-1.amazonaws.com/evermade-fsecure-assets/wp-content/uploads/2019/09/12093807/2019_attack_landscape_report.pdf

(2) Báo cáo thường niên của Úc về Casestudy tình hình an toàn an ninh mạng của 25 cơ quan nước này

https://www.asd.gov.au/sites/default/files/2019-10/annual_report_2018-19.pdf

(3) Báo cáo của Blackberry chiến dịch tấn công của các tổ chức APT sử dụng mã đọc thiết bị di động

https://threatvector.cylance.com/en_us/home/mobile-malware-and-apt-espionage-prolific-pervasive-and-cross-platform.html

(4) Giải pháp đối phó với mã độc Ransomeware khi cơ quan chính quyền Hoa Kỳ đang là mục tiêu chính

https://www.forbes.com/sites/forbestechcouncil/2019/10/24/ransomware-target-u-s-city-government/#72db97d135c2

(5) Số lượng các cuộc tấn công và quy mô của các yêu cầu tiền chuộc đã tăng vọt

https://uk.investing.com/news/stock-market-news/global-insurers-face-quiet-strain-from-hacker-ransom-demands-1985412