CẢNH BÁO

TUẦN 42 (14/10/2019 - 20/10/2019)

Số: /BC-CATTT *Hà Nội, ngày 22 tháng 10 năm 2019*

Tin tức

- Báo cáo thường niên IOCTA của Europol.

- Hiệu quả trong việc vá lỗi cho hệ điều hành và ứng dụng.

- Nhóm APT41 tấn công vào hệ thống cài đặt phần mềm TeamViewer

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

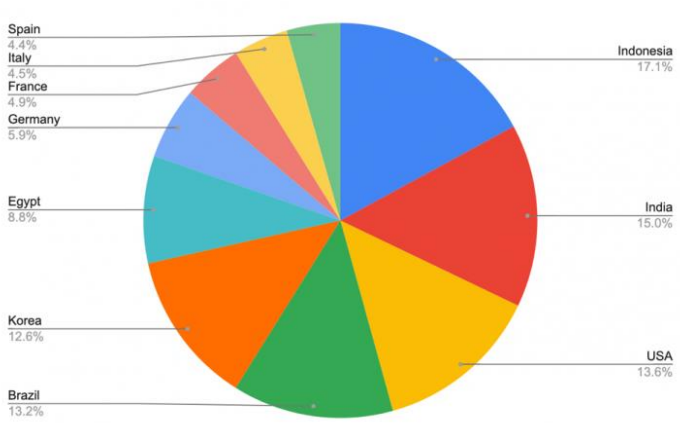
Báo cáo tài liệu chuyên ngành..

TRUNG TÂM GIÁM SÁT AN TOÀN KHÔNG GIAN MẠNG QUỐC GIA

Báo cáo thường niên IOCTA năm 2019 của Europol

Theo báo cáo IOCTA thường niên năm 2019 của Europol, mã độc mã hóa dữ liệu tống tiền (Ransomware) vẫn là mối đe dọa hàng đầu. Theo báo cáo, chiến thuật của Ransomware đã thay đổi, từ cách tiếp cận phổ rộng chuyển sang nhắm mục tiêu tập trung hơn vào các đối tượng có khả năng trả tiền chuộc cao hơn so với người dùng bình thường.

Theo một thống kê dựa trên dữ liệu từ hơn 230.000 lần thông tin người dùng cung cấp, trong khoảng thời gian từ ngày 01/04/2019 đến ngày 30/9/2019 cho thấy TOP 10 dòng mã độc Ransomware phổ biến nhất hiện nay và danh sách 10 quốc gia bị lây nhiễm nhiều nhất như sau.



Source:

https://blog.malwarebytes.com/awareness/2019/10/europol-ransomware-remains-top-threat-in-iocta-report/

- STOP (djvu): 56.00%
- Dharma (.cezar family): 12.00%
- Phobos: 8.90%
- GlobeImposter 2.0: 6.50%
- REvil / Sodinokibi: 4.50%
- GandCrab v4.0 / v5.0: 3.60%
- Magniber: 3.30%
- Scarab: 2.00%
- Rapid: 1.80%
- Troldesh / Shade: 1.40%

Hiệu quả trong việc vá lỗi cho hệ điều hành và ứng dụng

Mặc dù có sự thừa nhận rộng rãi rằng việc vá lỗi cho các hệ điều hành, các ứng dụng là rất hiệu quả trong việc giảm thiểu rủi ro, tuy nhiên việc vá lỗi thường tốn nhiều tài nguyên và hành động vá lỗi có thể làm giảm tính khả dụng của hệ thống, dịch vụ. Nỗ lực đẩy nhanh việc phân phối bản vá, chẳng hạn như không kiểm tra bản vá trước khi triển khai, có thể vô tình phá vỡ chức năng hệ thống và làm gián đoạn hoạt động. Mặt khác, sự chậm trễ trong việc triển khai bản vá tạo ra một cửa sổ cơ hội lớn hơn cho đối tượng tấn công.

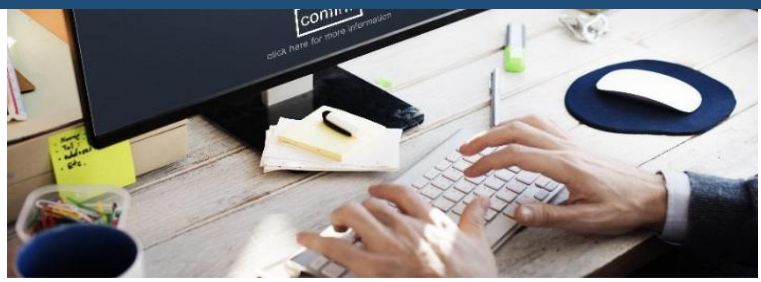
Microsoft và Viện Tiêu chuẩn và Công nghệ quốc gia Hoa Kỳ (NIST) đang hợp tác để phát triển một hướng dẫn mới giúp quản lý các bản vá điểm yếu, lỗ hổng. Dự án có tên là "Patching the Enterprise" sẽ tập trung vào việc xây dựng các kiến trúc và quy trình tham khảo quản lý bản vá điểm yếu, lỗ hổng chung cho doanh nghiệp.

Các kết quả dự kiến sẽ được chia sẻ trong hướng dẫn thực hành ấn phẩm đặc biệt 1800 của NIST (NIST Special Publication 1800) sau khi các nhà cung cấp có liên quan xác nhận các hướng dẫn triển khai trong phòng thí nghiệm NCCoE (National Cybersecurity Center of Excellence). Dự án này hiện đang tìm kiếm các nhà cung cấp công nghệ để tham gia cùng phát triển giải pháp.

Source:

https://www.nccoe.nist.gov/projects/building-blocks/patching-enterprise

Nhóm APT41 tấn công vào nhiều hệ thống có cài đặt phần mềm TeamViewer



Phần mềm điều khiển từ xa TeamViewer đã bị hack từ nhiều năm trước và một số máy tính người dùng đã bị tội phạm mạng kiểm soát để đánh cắp dữ liệu. Gần đây, FireEye đã tiết lộ rằng TeamViewer đã bị tấn công, tội phạm mạng có thể điều khiển tất cả các máy tính đang cài đặt phần mềm Teamviewer.

APT41 là một nhóm tấn công APT có nguồn gốc từ Trung Quốc. Nhóm này có mục tiêu tấn công là các tổ chức trong lĩnh vực kinh tế, công nghệ cao, viễn thông. APT41 đã tấn công các tổ chức trên 14 quốc gia trong khoảng 7 năm bao gồm: France, India, Italy, Japan, Myanmar, the Netherlands, Singapore, South Korea, South Africa, Switzerland, Thailand, Turkey, the United Kingdom, the United States.

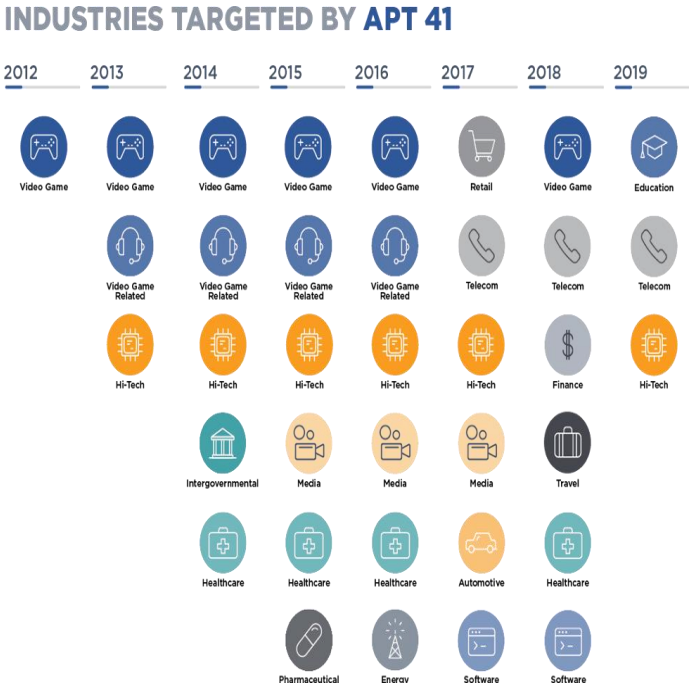
Gần đây, trong hội nghị FireEyeSummit, đã có báo cáo công bố và xác nhận về chiến dịch tấn công của APT41 thông qua TeamViewer, chiến dịch tấn công này đã được phát hiện từ năm 2016 cho phép truy cập và kiểm soát tất cả các máy tính, hệ thống có cài đặt TeamViewer. Ngoài ra APT41 còn lợi dụng các máy tính này để tìm kiếm thêm nhiều nạn nhân.

Source:

https://content.fireeye.com/apt-41/rpt-apt41

Hiện nay, theo số liệu trên trang chủ của TeamViewer có hơn 400 nghìn người cài đặt TeamViewer mỗi ngày và trong cùng 1 thời gian người ta thống kê được gần 45 triệu người đang sử dụng phần mềm.

Ở Việt Nam có rất nhiều người dùng, thậm chí là cán bộ kỹ thuật tại các đơn vị thực hiện cài đặt Teamviewer có các máy tính để thuận tiện cho công việc, điều này đồng nghĩa với việc hoàn toàn có thể đã bị nhóm này tấn công. Do vậy các cơ quan tổ chức cần phải siết chặt các quy chế, chính sách trong việc sử dụng các sản phẩm để hỗ trợ khi làm việc từ xa, đặc biệt là các máy chủ, máy tính có dữ liệu quan trọng.



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 497 lỗ hổng, trong đó có 51 lỗ hổng mức cao, 206 lỗ hổng mức trung bình, 44 lỗ hổng mức thấp và 196 lỗ hổng chưa đánh giá.

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 08 lỗ hổng trên Android, nhóm 10 lỗ hổng trên hệ điều hành Linux, nhóm 08 lỗ hổng trên thiết bị D-Link, Nhóm 136 lỗ hổng trên Oracle… 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:

- *Android: CVE-2019-2186, CVE-2019-2185. v.v..*
- *Linux: CVE-2019-17351, CVE-2019-17133 .v.v...*
- *D-Link: CVE-2019-17508, CVE-2019-17506,vv…*
- *Cisco: CVE-2019-15259, CVE-2019-12707 v.v..*
- *Wordpress: CVE-2019-17386*
- *Oracle: CVE-2019-2937, CVE-2019-2971 v.v..*

Thông tin điểm yếu lỗ hổng

STT	Sản phẩm/ dịch vụ	Mã lỗi quốc tế	Mô tả ngắn	Ghi chú
1	Android	CVE-2019-2186 CVE-2019-2185 CVE-2019-2184 …	Nhóm 08 lỗ hổng trên một số thành phần của hệ điều hành Android cho phép đối tượng tấn công chèn và thực thi mã lệnh từ xa mà không cần quyền thực thi, thu thập thông tin (user và mật khẩu người dùng).	Đã có thông tin xác nhận và bản vá
2	Linux	CVE-2019-17351 CVE-2019-17133 CVE-2019-17075 …	Nhóm 10 lỗ hổng trên hệ điều hành Linux cho phép đối tượng tấn công thực hiện tấn công từ chối dịch vụ	Đã có thông tin xác nhận và bản vá
3	D-Link	CVE-2019-17508 CVE-2019-17506 CVE-2017-14948	Nhóm 08 lỗ hổng trên một số sản phẩm của D-Link (DAP-1320 A2-V1.21, DIR-412 A1-1.14WW, DIR-866L 1.03B04, DIR-816 A1 1.06…) cho phép đối tượng tấn công khai thác lỗi XSS,thu thập thông tin về hệ thống mạng, đánh cắp thông tin xác thực, chèn và thực thi mã lệnh từ đó kiểm soát thiết bị	Một số lỗ hổng đã có thông tin xác nhận và bản vá
4	Cisco	CVE-2019-15259 CVE-2019-15256 CVE-2019-12707 …	Nhóm 41 lỗ hổng trên một số sản phẩm, ứng dụng của Cisco (Aironet Access Points, Catalyst 9100 Access Points, Unified Communications Manager, Firepower Management Center…) cho phép đối tượng tấn công thực hiện nhiều hình thức tấn công khác nhau gồm thu thập thông tin, thực thi mã lệnh từ xa.	Đã có thông tin xác nhận và bản vá
5	WordPress	CVE-2019-17386 CVE-2019-17672 CVE-2015-9490	Nhóm 25 lỗ hổng trên một số thành phần, phiên bản của WordPress cho phép đối tượng tấn công thu thập thông tin người dùng trên hệ thống (user_login, user_pass, user_email values), khai thác lỗi XSS, SSRF,	Một số lỗ hổng Đã có thông tin xác nhận và bản vá
6	Oracle	CVE-2019-2937 CVE-2019-2971 CVE-2019-2901	Nhóm 136 lỗ hổng trên một số sản phẩm của Oracle (Oracle Outside In Technology, Oracle Jdeveloper&ADF, Database Server, E-Business Suite...) cho phép đối tượng tấn công truy cập trái phép vào ứng dụng trên hệ thống, tấn công từ chối dịch vụ, sửa đổi trái phép dữ liệu,	Đã có thông tin xác nhận và bản vá

Thông tin chi tiết lỗ hổng, điểm yếu lưu ý

CVE-2019-15260

Ngày 16/10, các tổ chức đã công bố lỗ hổng trên các thiết bị truy cập từ xa (AP) của Cisco (Aironet), cho phép kẻ tấn công không được xác thực và có quyền truy cập trái phép vào thiết bị với các quyền nâng cao. Lỗ hổng có mã là CVE-2019-15260 với thang điểm nghiêm trọng CVSS v3.1 là 9,8.

Theo nhà nghiên cứu của Fortinet, lỗ hổng ảnh hưởng đến các dòng sản phẩm Aironet như phiên bản: 1540, 1560, 1800, 2800, 3800 và 4800.

Sản phẩm này còn tồn tại 2 lỗ hổng từ chối dịch vụ nghiêm trọng khác nữa là: CVE-2019-15264 và CVE-2019-15261 nên người sử dụng và các nhà quản trị cần hết sức lưu ý với các dòng thiết bị này.

Source:

https://nvd.nist.gov/vuln/detail/CVE-2019-15260
https://www.zdnet.com/article/security-researcher-publishes-proof-of-concept-code-for-recent-android-zero-day/

CVE-2019-2215

Một nhà nghiên cứu bảo mật Hoa Kỳ đã công bố mã bằng chứng khai thác một lỗ hổng zero-day trên hệ điều hành Android được tiết lộ gần đây.

Lỗ hổng được đặt tên là Qu1ckR00t xác định với mã lỗi CVE-2019-2215 với thang điểm cao CVSS v3.0 là 7,8. Khi khai thác, chúng cho phép kẻ tấn công có thể bỏ qua kiểm soát truy cập (DAC - Discretionary Access Control) và có thể vô hiệu hóa các tính năng tăng cường bảo mật như: SELinux (Một dạng tường lửa của Linux), chế độ tính toán khả năng an toàn (Secure Computing Mode) và kiểm soát truy cập bắt buộc (Mandatory Access Control).

Google đã thông báo lỗ hổng sẽ ảnh hưởng đến một dòng sản phẩm như sau: Pixel 2 with Android 9 and Android 10 preview, Huawei P20, Xiaomi Redmi 5A, Xiaomi Redmi Note 5Xiaomi A1, Oppo A3, Moto Z3, Oreo LG phones, Samsung S7, S8, S9.

Source:

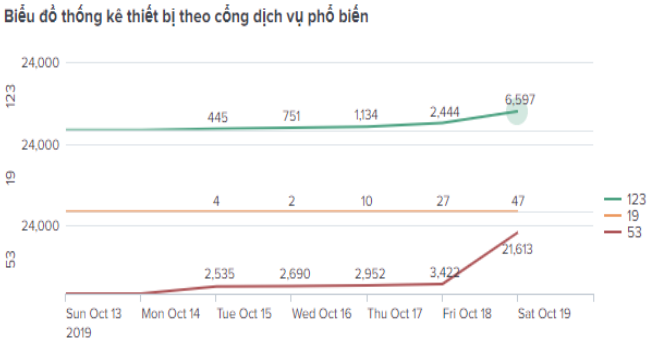
https://nvd.nist.gov/vuln/detail/CVE-2019-2215
https://www.zdnet.com/article/security-researcher-publishes-proof-of-concept-code-for-recent-android-zero-day/

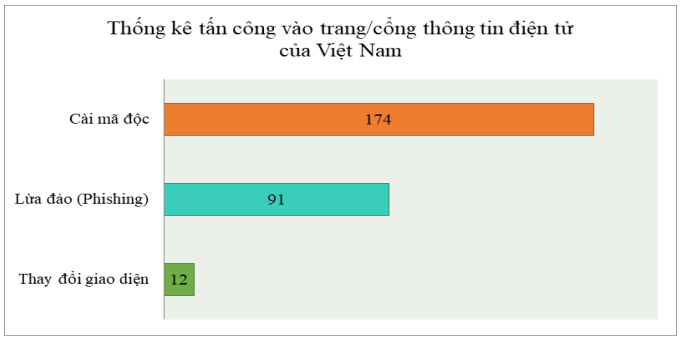
s

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 **44,673** (giảm so với tuần trước là **49,094**) 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.



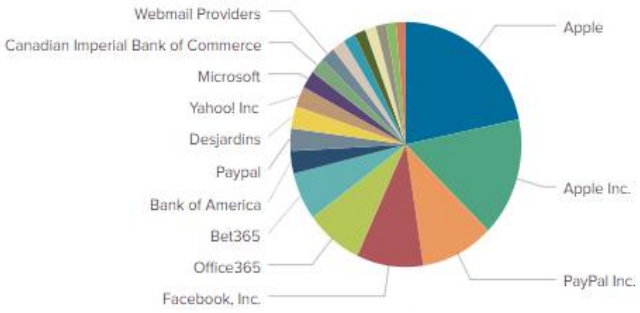


Tấn công Web

Trong tuần, có 277 trường hợp tấn công vào trang/cổng thông tin điện tử của Việt Nam: 12 trường hợp tấn công thay đổi giao diện, 91 trường hợp tấn công lừa đảo (Phishing), 174 trường hợp tấn công cài cắm mã độc.

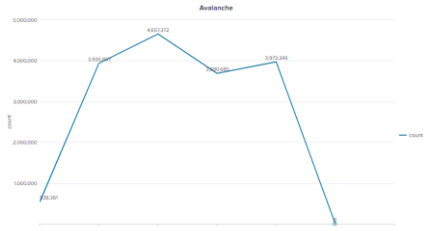
Tấn công Phishing

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.



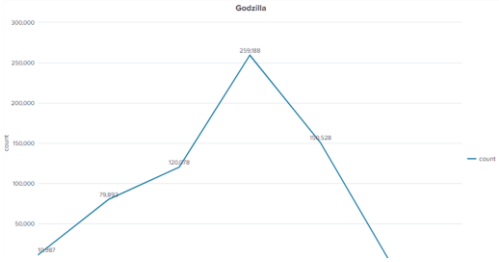
Thống kê nguy cơ, các cuộc tấn công tại Việt Nam

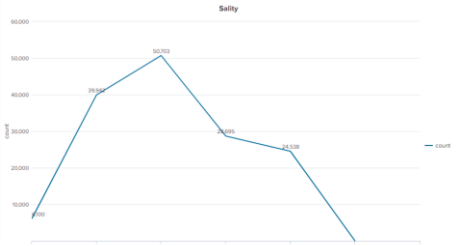
Trong tuần mạng botnet **Avalanche** có 3,973,346 lượt địa chỉ IP kết nối với máy chủ điều khiển giảm mạnh so với tuần 40 là 3.690.685.



Trong tuần mạng botnet **Conficker** có 157,894 lượt địa chỉ IP kết nối với máy chủ điều khiển giảm so với tuần 41 là 155.084.

Trong tuần mạng botnet **Godzilla** có 150,528 lượt địa chỉ IP kết nối với máy chủ điều khiển giảm so với tuần 41 là 259.188.





Trong tuần mạng botnet **Sality** có 24,538 lượt địa chỉ IP kết nối với máy chủ điều khiển giảm so với tuần 41 là 28,659.

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

disorderstatus.ru	hjb343e8.ru
differentia.ru	rkphklelf.ru
atomictrivia.ru	cp.hfuabnqx.ru
rchmm2r9.ru	morphed.ru
soplifan.ru	somicrososoft.ru
xjpakmdcfuqe.com	evbvhzmb.info
xdqzpbcgrvkj.ru	www.cityofangelsmagazine.com

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) Báo cáo hoạt động của các nhóm tin tặc Nga sau tấn công bầu cử Hoa Kỳ năm 2016 của ESET

https://www.welivesecurity.com/wp-content/uploads/2019/10/ESET_Operation_Ghost_Dukes.pdf

(2) Báo cáo của Kaspersky: Việt nam đứng thứ 6 nguồn tấn công IoT trên thế giới

https://securelist.com/iot-a-malware-story/94451/

(3) Báo cáo về tội phạm mạng là một trong những thách thức lớn nhất mà nhân loại sẽ phải đối mặt trong hai thập kỷ tới

https://www.herjavecgroup.com/the-2019-official-annual-cybercrime-report/

(4) Báo cáo Đánh giá Nguy cơ Tội phạm (IOCTA) hàng năm

https://www.thehaguesecuritydelta.com/media/com_hsd/report/261/document/iocta-2019.pdf

https://blog.malwarebytes.com/awareness/2019/10/europol-ransomware-remains-top-threat-in-iocta-report/

(5) Thống kê 10 vụ vi phạm dữ liệu lớn nhất trong thập kỷ qua (2010 - 2019).

https://www.businessinsider.com/biggest-hacks-2010s-facebook-equifax-adobe-marriott-2019-10

https://www.acq.osd.mil/cmmc/docs/cmmc-draft-model-30aug19.pdf

(6) Thống kê 10 thách thức lớn nhất an toàn an ninh mạng cho thiết bị IoT

https://www.peerbits.com/blog/biggest-iot-security-challenges.html

(7) Thống kê 90% tất cả tấn các cuộc tấn công mạng là do lỗi hoặc hành vi của con người

https://chiefexecutive.net/almost-90-cyber-attacks-caused-human-error-behavior/

(8) Thống kê các quốc gia đứng đầu trong bảng xếp hạng "Thất bại" trong việc bảo vệ quyền riêng tư

https://qz.com/india/1728927/indias-among-the-worlds-top-three-surveillance-states/

https://www.comparitech.com/blog/vpn-privacy/surveillance-states/

(9) Số liệu báo cáo Quý 2 - 3 về tấn công mã hoá dữ liệu Ransomware

https://id-ransomware.malwarehunterteam.com/index.php?lang=en_US

https://blog.emsisoft.com/en/34335/ransomware-statistics-for-2019-q2-to-q3-report/