OPSWAT.

VNISA
VIETNAM INFORMATION SECURITY ASSOCIATION

BÁO CÁO

Bảo mật ứng dụng web tại Việt Nam: Hiện trạng, thách thức và giải pháp

Hiện trạng

Bảo mật ứng dụng web tại Việt Nam

Hiện nay, việc bảo mật ứng dụng web (web app) được mọi tổ chức, doanh nghiệp và cá nhân người dùng ngày càng quan tâm bởi tình trạng tấn công mạng thông qua ứng dụng web xảy ra càng nhiều, đặc biệt là đối với các cơ sở trọng yếu, khối ngân hàng, tài chính và doanh nghiệp lớn.

Tổn thất từ các cuộc tấn công này là rò rỉ thông tin cá nhân, mất mát dữ liệu quan trọng, giả mạo giao dịch, và gián đoạn hoạt động kinh doanh. Điều này gây ra nhiều thiệt hại về tài chính cũng như uy tín của tổ chức và doanh nghiệp.

Chính vì vậy, việc thực hiện các phương pháp bảo mật ứng dụng web là vô cùng cấp thiết. Các nhà quản trị hệ thống thông tin của tổ chức, doanh nghiệp cần xây dựng hệ thống bảo mật cũng như kiểm tra tình trạng bảo mật của web app định kỳ.

Thế nhưng, hiện trạng bảo mật không gian mạng nói chung tại Việt Nam vẫn tồn tại nhiều số liệu đáng quan ngại:

2.063 website

vi phạm an toàn thông tin trong 10 tháng đầu năm 2022 [1]

21.200 tỷ đồng

thiệt hại do mã độc gây ra cho người dùng Việt Nam năm 2022

14.500 máy chủ

nhiễm ransomware tại Việt Nam năm 2022 [2]

30 vụ

rò rỉ, lộ lọt bí mật Nhà nước với 202 đầu tài liệu năm 2021 [3]

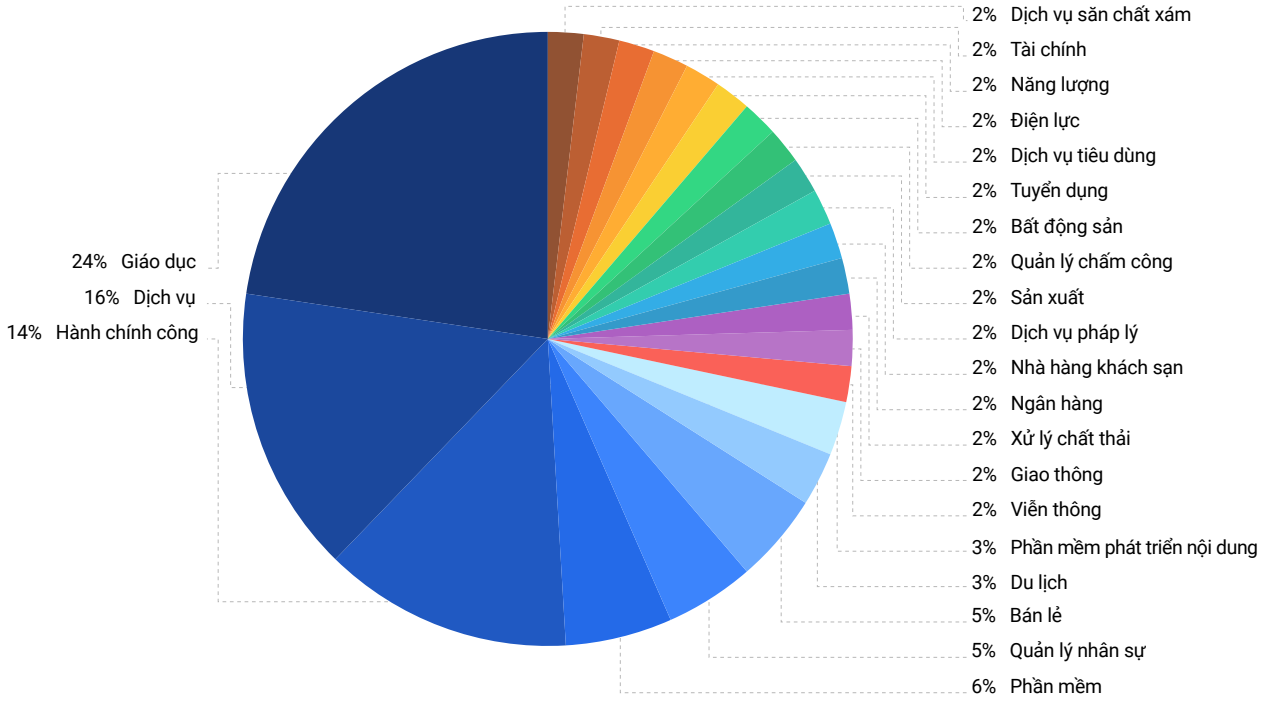
8 triệu

cảnh báo tấn công mạng, trong đó có trên 2.700 đợt tấn công nhằm vào các trang thông tin hay cổng thông tin điện tử trong nước. [3]

Một trong các cách thức tấn công yêu thích của tin tặc đó là thông qua các tệp tin được đăng tải lên web app (file upload) của tổ chức, doanh nghiệp.

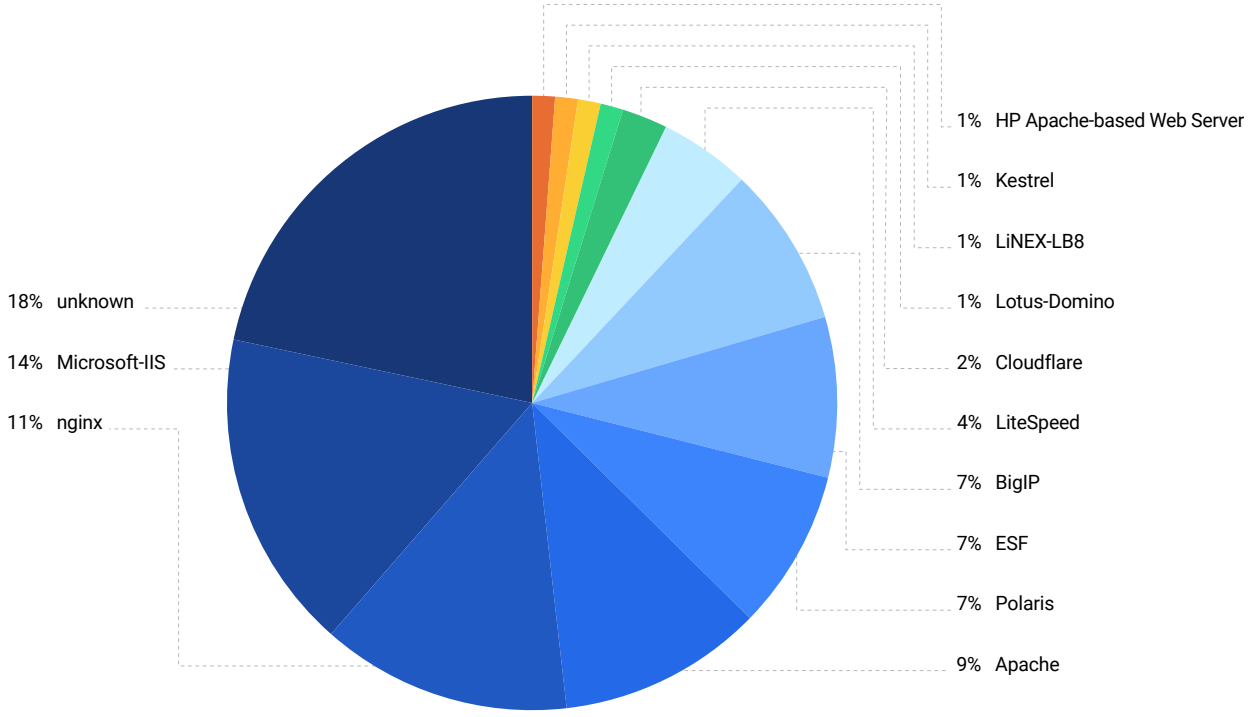
Bằng cách rà soát các web app có chức năng nhận tệp tin đăng tải (file upload), OPSWAT đã tìm ra nhiều web app của các tổ chức, doanh nghiệp tại Việt Nam đang đứng trước nguy cơ bị tấn công qua tệp tin có chứa mã độc. Theo nghiên cứu này, tại Việt Nam hiện có hàng trăm web app có tính năng nhận file upload mà không bao gồm bước xác thực người dùng (User Authentication), một trong 10 bước bảo mật thiết yếu do OWASP (Open Web Application Security Project), tổ chức quốc tế chuyên về bảo mật ứng dụng web, khuyến nghị.

Đáng nói, đa phần các web app này thuộc về các cơ quan, tổ chức trong ngành giáo dục (24%), dịch vụ (16%) và hành chính công (14%).



Tỉ lệ web có tính năng file upload chưa đạt chuẩn bảo mật - theo ngành

Nghiên cứu còn cho thấy các loại máy chủ web (web server) cho các ứng dụng web tại Việt Nam khá đa dạng, bên cạnh các web server nổi tiếng như Cloudflare, Nginx, Apache, Microsoft-IIS, còn có những web server mới như ESF, Kestrel..., và có 1% web app chạy trên web server LiNEX Việt Nam. Có khoảng 18% web server là không xác định, điều này có thể là tích cực trong vấn đề bảo mật khi ẩn dấu thông tin về web server, tuy nhiên cũng có thể là mối lo về an toàn thông tin nếu sử dụng web server mới vốn chưa có độ bảo mật cao.



Tỉ lệ web có tính năng file upload chưa đạt chuẩn bảo mật - theo loại máy chủ

Bên cạnh đó, theo báo cáo Hiện trạng về an toàn thông tin (ATTT) Khu vực phía Nam 2022 của Hiệp hội An toàn Thông tin Việt Nam (VNISA), trên 95% các bộ, ngành, và địa phương chưa thực hiện đầy đủ hoạt động kiểm tra, đánh giá ATTT định kỳ.[4]

Báo cáo của VNISA còn đề cập đến một số hiện trạng khiến gia tăng nguy cơ bị tấn công mạng như ngân phí cho an toàn thông tin vẫn thấp và khó khăn trong việc nâng cao nhận thức an toàn thông tin của người dùng. Đặc biệt, điểm đáng quan ngại nhất chính là tỉ lệ nhận diện các hành vi tấn công của các tổ chức, vốn giảm từ 76% vào năm 2021 đến còn 54% trong 2022. Điều này chứng tỏ các chương trình phát hiện mã độc và phòng thủ các cuộc tấn công mạng của các tổ chức chưa hiệu quả.

Với hiện trạng trên, các tổ chức, doanh nghiệp tại Việt Nam cần tăng cường xây dựng hệ thống bảo mật thông tin cho web app nhằm đối mặt với các mã độc Zero-day, lỗ hổng bảo mật và các cuộc tấn công ngày càng tinh vi và liên tiếp của tin tặc.

Thách thức

Trong việc bảo vệ các tổ chức, doanh nghiệp khỏi mối nguy từ việc đăng tải tệp tin

Theo OWASP (Open Web Application Security Project), tổ chức quốc tế chuyên về bảo mật ứng dụng web, để phòng chống các cuộc tấn công qua quy trình đăng tải tệp tin một cách hiệu quả, các tổ chức, doanh nghiệp cần thực hiện 10 bước sau:

1. Xác thực định dạng tệp tin (Extension Validation)

Kiểm tra và xác thực định dạng tệp tin để tránh trường hợp giả mạo. Trong bước này, tên tệp tin sẽ được giải mã và phần mềm an ninh sẽ dùng các bộ lọc chuyên dụng để loại bỏ trường hợp định dạng kép hoặc định dạng giả.

2. Xác thực định dạng nội dung tệp tin (Content-Type Validation)

Trong bước này, phần mềm an ninh sẽ xác thực định dạng nội dung của tệp tin người tải lên nhằm tránh trường hợp giả mạo hoặc định dạng nhầm nội dung tệp tin.

3. Xác thực chữ ký điện tử (File Signature Validation)

Do tin tặc có thể dễ dàng làm giả chữ ký điện tử, OWASP khuyến nghị thực hiện bước xác thực này song song với xác thực định dạng nội dung tệp tin.

4. Làm sạch tên tệp tin (Filename Sanitization)

Tên tệp tin có thể làm hại đến hệ thống nếu nó chứa ký tự cấm hoặc sử dụng tên bị giới hạn. Để tránh trường hợp trên xảy ra, các tổ chức được khuyến nghị gán chuỗi ký tự hoàn toàn ngẫu nhiên cho tên tệp tin (ví dụ như sử dụng UUID hoặc GUID). Trong trường hợp bắt buộc phải sử dụng tên tệp tin, các doanh nghiệp cần phải có cơ chế xác thực đầu vào tại bên máy khách lẫn máy chủ.

5. Xác thực nội dung tệp tin (File Content Validation)

Nội dung của tệp tin có thể ẩn chứa mã độc hoặc dữ liệu cấm. Để tránh trường hợp này xảy ra, các tổ chức có thể áp dụng cơ chế xác thực riêng cho từng loại tệp tin. Ngoài ra cần có tính năng cho người dùng tố cáo nội dung vi cấm cũng như nội dung vi phạm bản quyền. OWASP còn khuyến nghị các tổ chức xác thực trực tiếp nội dung trong môi trường giả lập trước khi công bố tệp tin.

6. Địa điểm lưu trữ tệp tin (File Storage Validation)

Cần chọn địa điểm lưu trữ các tệp tin theo mức độ an ninh và yêu cầu của tổ chức. OWASP đưa ra khuyến nghị cơ bản như sau:

- Trữ tệp tin tại máy chủ khác, vì tổ chức có thể tách biệt hoàn toàn ứng dụng phục vụ người dùng và máy chủ quản lý việc tải và lưu trữ tệp tin.
- Trữ tệp tin ngoài tên miền gốc, và chỉ trao quyền truy cập cho nhân viên liên quan.
- Trữ tệp tin tại tên miền gốc, và chỉ cho quyền thay đổi.
- Nếu cần phải truy cập tệp tin, các tổ chức cần có cơ chế kiểm soát phù hợp (ví dụ như IP nội bộ, xác thực danh tính, v.v.)

7. Thiết lập quyền truy cập của người dùng (User Permission)

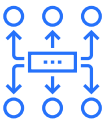
Trước khi người dùng được truy cập vào dịch vụ tải dữ liệu, họ cần phải trải qua hai loại xác thực:

- Xác thực danh tính: Người dùng nên là cá nhân đã đăng ký hoặc có định danh để xác định giới hạn tải dữ liệu của họ.
- Xác thực quyền truy cập: Người dùng cần phải được trao quyền truy cập trước đó để truy cập và thđổi tệp tin.

8. Thiết lập quyền truy cập hệ thống tệp tin (Filesystem Permissions)

OWASP khuyến nghị đặt quyền truy cập cho các tệp tin dựa theo quy tắc quyền truy cập tối thiểu. Cụ thể là:

- Chỉ người dùng được trao quyền mới được truy cập tệp tin.
- Người dung cần phải yêu cầu trước mới được truy cập tệp tin.
- Trong trường hợp cần phải chạy tệp tin, cần phải quét trước để tránh kích hoạt mã độc.



9. Giới hạn dung lượng tệp tin (Upload and Download Limits)

Ứng dụng nên có giới hạn cho tính năng tải lên nhằm tránh quá tải tính năng trữ tệp tin. Nếu hệ thống phải giải nén và xử lý tệp tin, tổ chức nên xác định giới hạn dung lượng tệp tin sau khi đã giải nén và tính toán dung lượng tệp tin nén bằng biện pháp an toàn.

10. Sử dụng các giải pháp bảo mật web (Web Application Security Solution)

Đặc biệt, OWASP khuyến nghị tổ chức, doanh nghiệp ứng dụng nhiều công nghệ bảo mật vào cùng hệ thống bảo mật của mình để có thể bảo vệ ứng dụng web và mạng lưới của tổ chức một cách toàn diện. Một số các công nghệ bảo mật cần có là:

- Chương trình phát hiện mã độc (Anti-virus)
- Công nghệ làm sạch và tái lập nội dung tệp tin nhằm phòng chống mã độc Zero-day và các mã độc có kỹ thuật lẩn tránh anti-virus (Content Disarm & Reconstruction)
- Công nghệ phòng chống rò rỉ thông tin (Data loss prevention)
- Công nghệ phát hiện lỗ hổng bảo mật

Tuy nhiên việc cài đặt và sử dụng nhiều chương trình, công nghệ bảo mật khác nhau vào hệ thống của tổ chức mang tới một thách thức mới đó là sự phức tạp trong quản lý và vận hành, cũng như chi phí cao để chi trả cho đội ngũ vận hành và các đối tác khác nhau.

Giải pháp

Bảo mật ứng dụng web toàn diện cho tổ chức và doanh nghiệp

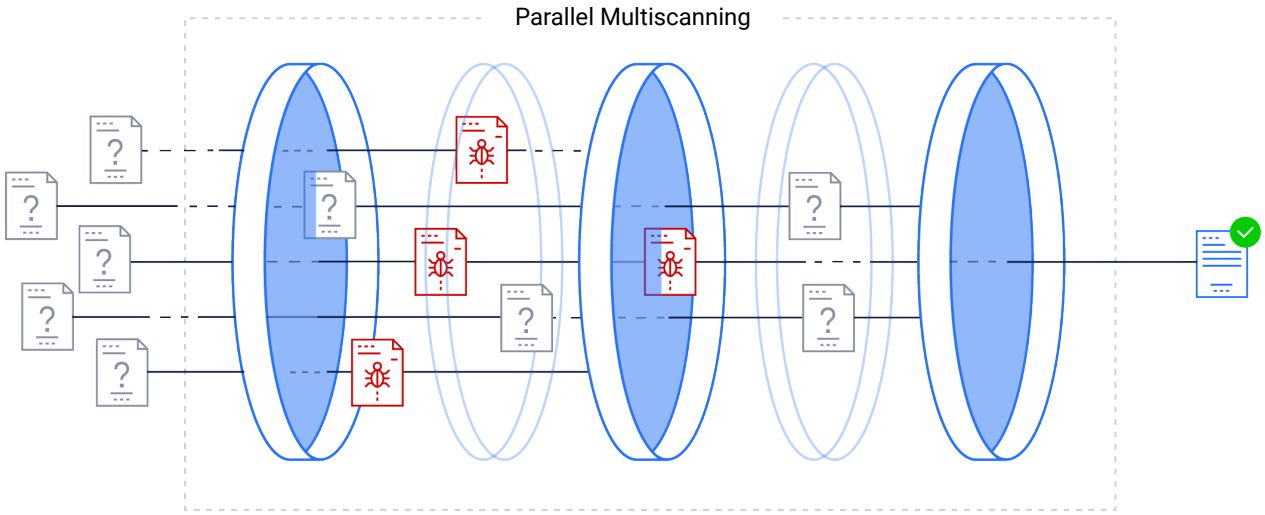
Để giải quyết cả nguy cơ bị tấn công, sự thiếu hụt các công nghệ bảo mật chuyên sâu, cũng như các thách thức về vận hành và chi phí, giải pháp bảo mật ứng dụng web của OPSWAT cung cấp các công nghệ bảo mật tiên tiến bảo vệ ứng dụng web của tổ chức/ doanh nghiệp một cách toàn diện khỏi các cuộc tấn công sử dụng file upload.

Các công nghệ bảo mật ứng dụng web của OPSWAT bao gồm:

- Công nghệ Nhận dạng mã độc đa ứng dụng xử lý
- Công nghệ Đánh giá lỗ hổng bảo mật của tệp tin
- Công nghệ Làm sạch và tái lập nội dung chuyên sâu
- Hỗ trợ tệp tin lưu trữ
- Công nghệ Ngăn ngừa rò rỉ dữ liệu chủ động
- Xác thực định dạng tệp tin

Công nghệ nhận dạng mã độc đa ứng dụng xử lý (Multiscanning)

Công nghệ Nhận dạng mã độc đa ứng dụng xử lý (Multiscanning) là một công nghệ bảo mật nâng cao do OPSWAT phát triển. Giải pháp bảo mật web của OPSWAT có thể cung cấp tới hơn 30 phần mềm phát hiện mã độc (Anti-virus) để kiểm tra tệp tin. Ngoài ra, giải pháp còn sử dụng cơ chế quét suy nghiệm được bổ trợ bởi công nghệ học máy.



Tỉ lệ phát hiện mã độc lên tới hơn 99%

Sử dụng nhiều phần mềm anti-virus giúp tối đa tỉ lệ phát hiện mã độc

Cải thiện thời gian phát hiện mã độc

Rút ngắn thời gian từ khi mã độc bùng phát tới khi phát hiện mã độc

Nâng cao hiệu suất

Bằng việc thực hiện song song các nhiệm vụ: xử lý tệp nén, xác định loại tệp tin và phát hiện mã độc.

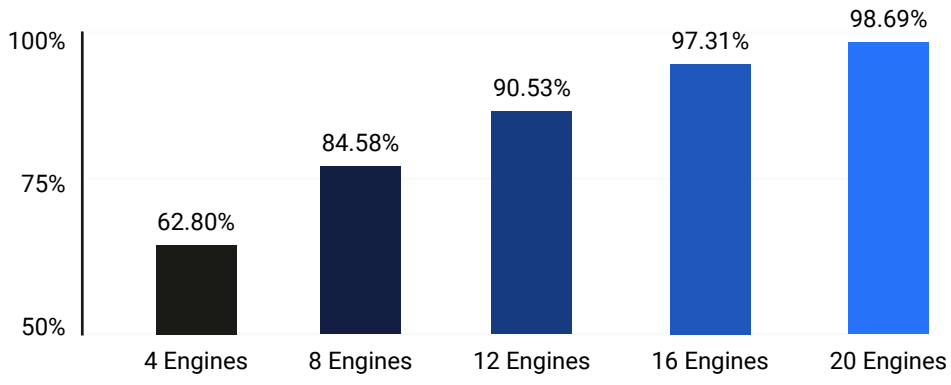
Tiết kiệm chi phí

OPSWAT hợp tác với nhiều nhà cung cấp để mang đến giải pháp tích hợp đã được tối ưu hóa, giúp doanh nghiệp tiết kiệm tối đa về chi phí.

Tỉ lệ False Positives thấp

Sử dụng nhiều phần mềm anti-virus giúp giảm tối đa tỉ lệ False Positives

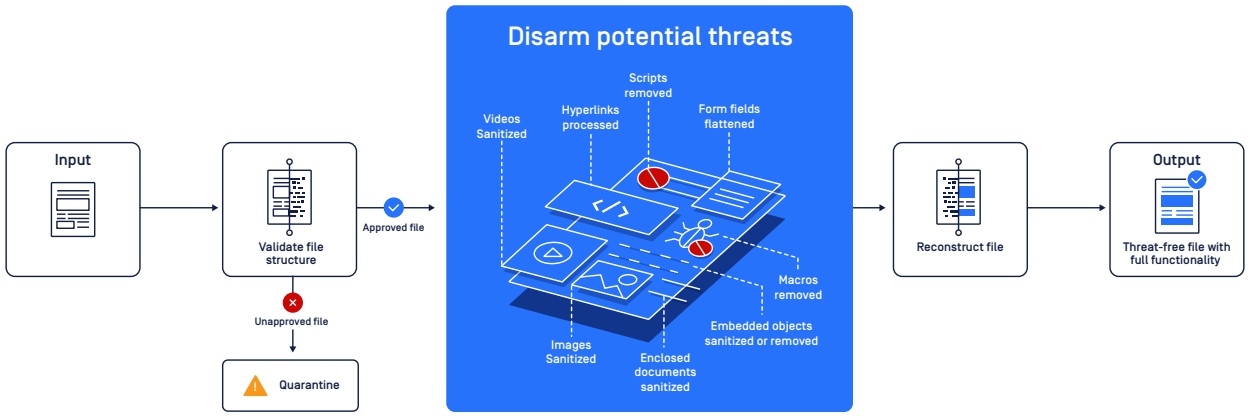
Tỉ lệ phát hiện mã động của công nghệ Multiscanning của OPSWAT được chứng minh qua việc rà soát hơn 10,000 mã độc thực tế:



Công nghệ làm sạch và tái lập nội dung chuyên sâu

(Deep Content Disarm and Reconstruction)

Công nghệ Làm sạch và tái lập nội dung chuyên sâu (Deep CDR) ngăn ngừa mã độc đã xác định lẫn chưa xác định bằng cách phân tích tệp tin và làm sạch mọi thành phần trong đó, sau đó tái tạo lại tệp tin với những thành phần an toàn. Deep CDR mang lại hiệu quả cao trong việc phòng tránh và ngăn chặn các mã độc được trang bị công nghệ lẩn tránh hệ thống anti-virus, mã độc VMware, mã độc được mã hóa cũng như các mã độc tinh vi khác.



Làm sạch hơn 130 loại tệp tin

Xử lý nhiều loại tệp tin thường gặp như PDF, Microsoft Office, HTML, cũng như các tệp tin hình ảnh. Ngoài ra còn quét các tệp tin định dạng dành riêng cho từng khu vực như JTD hoặc HWP

Xử lý tệp nén (Archive)

Tính năng làm sạch mạnh mẽ hỗ trợ các tệp nén phức tạp, tài liệu, dữ liệu đính kèm email, hay siêu liên kết (hyperlink)

Vô hiệu hóa mã độc giấu trong hình ảnh

Vô hiệu hóa các mã độc trong tệp hình ảnh và nén tệp tin mà không ảnh hưởng chất lượng hiển thị

Hiệu năng cao

Làm sạch tệp tin chỉ trong vài mili giây, giúp công việc của bạn thuận lợi hơn.

Công nghệ ngăn ngừa rò rỉ dữ liệu chủ động

(Proactive Data Loss Prevention)

Với công nghệ Ngăn ngừa rò rỉ dữ liệu chủ động (Proactive DLP), giải pháp của OPSWAT sẽ rà soát và ngăn chặn rò rỉ thông tin mật hoặc dữ liệu nhạy cảm có trong tệp tin. Các loại dữ liệu nhạy cảm bao gồm mã số thẻ tín dụng hoặc số căn cước công dân. Công nghệ Ngăn ngừa rò rỉ dữ liệu chủ độnghiện hỗ trợ hơn 70 loại tệp tin khác nhau, bao gồm các loại tệp tin phổ biến như PDF và Microsoft Office.

Phát hiện dữ liệu mật trong mã nguồn

Phát hiện và báo động nếu có dữ liệu mật trong các tệp tin chữ (AWS, Microsoft Azure, và Google Cloud Platform)

Nhận dạng ký tự quang học (OCR)

Nhận diện và xóa thông tin nhạy cảm trong các tệp tin PDF dạng hình hoặc có nhúng hình.

Khả năng xử lý nhiều loại dữ liệu nhạy cảm

- Số căn cước công dân
- Mã số thẻ tín dụng
- Địa chỉ IPv4, CIDR
- Custom Regular Expressions (RegEx)

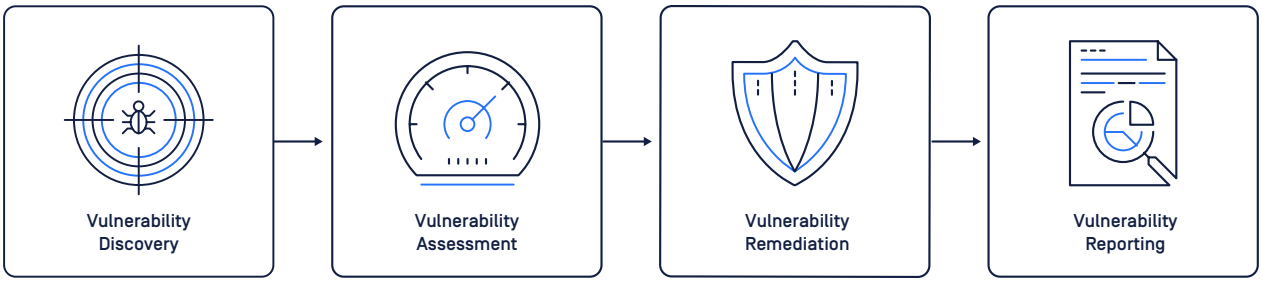
Dấu chìm (Watermark)

Tăng cường bảo mật và khả năng truy thu dữ liệu bị mất.

Công nghệ đánh giá lỗ hổng bảo mật của tệp tin

(File-Based Vulnerability Assessment)

Công nghệ Đánh giá lỗ hổng bảo mật của tập tin (File-Based Vulnerability Assessment) sẽ truy tìm lỗ hổng bảo mật trong tệp tin trước khi chúng được cài đặt nhằm mục đích tăng cường bảo mật.



Hơn một tỉ điểm dữ liệu

Sử dụng hơn một tỉ điểm dữ liệu về lỗ hổng bảo mật thu thập từ các thiết bị thực

Phát hiện chương trình cài đặt có lỗ hổng bảo mật

Ngăn chặn các chương trình cần cài đặt vào mạng nội bộ.

Phát hiện lỗ hổng trong phần mềm và thiết bị

Phát hiện lỗ hổng bảo mật trước khi phần mềm và thiết bị được cài đặt và sử dụng.

Hỗ trợ tệp tin lưu trữ

(Archive Extraction)

Giải pháp bảo mật web của OPSWAT có khả năng xử lý hơn 50 loại tệp tin lưu trữ (archive) khác nhau. Giải pháp này cũng cho phép người dùng quét tệp tin chưa giải nén hoặc đã giải nén nhằm ngăn ngừa nguy cơ tấn công từ tệp tin lưu trữ.

Tăng cường khả năng phòng chống mã độc

Xử lý cả tệp tin đã giải nén và chưa giải nén

Tối ưu thời gian xử lý

Giảm thời gian phát hiện mã độc và làm sạch tệp nén bằng cách loại bỏ các bước trùng lặp trong khi xử lý

Ngăn chặn các cuộc tấn công archive bombs

Kiểm tra, rà soát mã độc và làm sạch từng tệp tin trong tệp nén một cách riêng lẻ.

Xác thực định dạng tệp tin

(File Type Verification)

Với tính năng xác thực định dạng tệp tin của OPSWAT, người dùng có thể xác định định dạng thực tế dựa trên nội dung của tệp tin nhằm chống lại các cuộc tấn công bằng định dạng giả mạo. Người dùng cũng có thể cấu hình các quy trình bảo mật dựa trên loại tệp thực tế. Ví dụ, người dùng có thể áp dụng các biện pháp phòng ngừa nhiều hơn đối với các loại tệp nguy hiểm như các tệp EXE và DLL - thiết lập các chính sách khác nhau hoặc các quy tắc làm việc dựa trên loại tệp.

Một tệp tin giả mạo thường là biểu hiện điển hình của tấn công mạng, vì vậy để giảm thiểu rủi ro này, giải pháp bảo mật của OPSWAT sẽ chặn các tệp có định dạng sai. Tính năng này của OPSWAT hỗ trợ đến hơn 4.500 loại tệp tin khác nhau.

Về OPSWAT

OPSWAT là công ty hàng đầu thế giới về các giải pháp an ninh mạng dành cho các hệ thống công nghệ thông tin (IT), công nghệ vận hành (OT) và điều khiển công nghiệp (ICS) của các cơ sở hạ tầng thiết yếu. OPSWAT cũng là nhà cung cấp đầu ngành về công nghệ làm sạch và tái lập nội dung chuyên sâu (Deep CDR), bảo vệ các cơ sở trọng yếu trên thế giới khỏi các phần mềm độc hại và các cuộc tấn công Zero-day. Những giải pháp bảo vệ cơ sở hạ tầng trọng yếu của OPSWAT đảm bảo an ninh mạng cho cả khối tư nhân lẫn các tổ chức nhà nước với công nghệ và quy trình tiên tiến nhất, đảm bảo tính bảo mật trong việc truyền dữ liệu, tệp tin và sự truy cập của các thiết bị vào hệ thống mạng trọng yếu. Hơn 1.500 tổ chức trên toàn thế giới bao gồm các định chế tài chính, cơ quan Quốc phòng, cơ sở sản xuất, nhà máy năng lượng, cơ quan hàng không vũ trụ và hệ thống giao thông, đã và đang tin tưởng sử dụng các giải pháp của OPSWAT để bảo vệ tệp tin và thiết bị của họ; từ đó, đảm bảo việc tuân thủ các chính sách và quy định đặc thù của mỗi ngành và chính phủ, đồng thời bảo vệ danh tiếng, tài chính, cũng như nhân viên và khách hàng của họ khỏi sự gián đoạn do các cuộc tấn công mạng.

Để biết thêm thông tin về OPSWAT, vui lòng truy cập www.opswat.com

Về VNISA

Hiệp hội An toàn Thông tin Việt Nam (VNISA) – Chi hội phía Nam là một tổ chức xã hội nghề nghiệp phi lợi nhuận hoạt động trong lĩnh vực bảo mật và an toàn thông tin được nhà nước Việt Nam công nhận. VNISA tập hợp các cá nhân, tổ chức đang hoạt động trong lĩnh vực ATTT nhằm tuyên truyền nhận thức, phát triển công nghệ và đẩy mạnh ứng dụng đảm bảo ATTT trong mọi lĩnh vực kinh tế, xã hội.

VNISA hoạt động trong các lĩnh vực:

1. Tổ chức sự kiện, hội thảo, tọa đàm, báo cáo chuyên đề về ATTT.
2. Khảo sát, điều tra về ATTT trên phạm vi vùng miền và toàn quốc.
3. Tư vấn và đào tạo chuyên sâu cho các tổ chức, cá nhân về giải pháp và ứng dụng trong lĩnh vực ATTT.
4. Dịch vụ tư vấn và phản biện về ATTT.
5. Dịch vụ đánh giá về an ninh và bảo mật thông tin.
6. Tổ chức các cuộc thi, diễn tập về ATTT.
7. Chủ trì hợp tác với các hội, các doanh nghiệp trong và ngoài nước có liên quan để trao đổi, chia sẻ kinh nghiệm, cùng giúp đỡ nhau nhằm phát triển và đẩy mạnh ứng dụng ATTT.

Để biết thêm thông tin về Chi hội VNISA phía Nam,vui lòng truy cập www.vnisahcm.org.vn

Thông tin tham khảo:

[1] https://phutho.gov.vn/vi/ngay-toan-thong-tin-2022-chung-tay-bao-ve-nguoi-dan-va-doanh-nghiep-chuyen-doi-so-toan
[2] https://cand.com.vn/Cong-nghe/nam-2022-viet-nam-thiet-hai-833-trieu-usd-do-virus-may-tinh-i677696/
[3] https://antoanthongtin.vn/an-toan-thong-tin/bo-cong-an-phat-hien-30-vu-ro-ri-lo-lot-bi-mat-nha-nuoc-107746
[4] Hiện Trạng Về An Toàn Thông Tin Khu Vực Phía Nam 2022, VNISA
[5] https://cheatsheetseries.owasp.org/cheatsheets/File_Upload_Cheat_Sheet.html

OPSWAT.
Protecting the World's Critical Infrastructure