Datasheet

Viettel Advanced Malware Analysis
(VCS - AMA)

viettel security

Sự cần thiết của giải pháp

Trong thời đại ngày nay, thừa hưởng sự phát triển của công nghệ thông tin (CNTT), kỹ thuật tấn công của hacker cũng được nâng cao đáng kể. Các hệ thống phân tích mã độc thông thường như Firewall hay Anti Virus chỉ phát hiện mã độc dựa trên chữ ký và thông tin đặc trưng của những mã độc đã biết.

Trong khi đó, các cuộc tấn công có chủ đích đến các cơ quan doanh nghiệp, các tổ chức, chính phủ phần lớn đều sử dụng những loại mã độc, mã khai thác hết sức tinh vi với các lớp ngụy trang bảo vệ và khai thác các lỗ hổng chưa từng được biết tới.

Do đó, việc trang bị một giải pháp phân tích mã độc đa lớp đang là một nhiệm vụ hết sức cấp thiết đối với các tổ chức, doanh nghiệp trong thời đại hiện nay.

Giải pháp Viettel Advanced Malware Analysis

Viettel Advanced Malware Analysis (VCS - AMA) là hệ thống phân tích mã độc tự động, đa lớp dựa trên các tri thức tích lũy, hỗ trợ phân tích hầu hết các loại file nhằm phát hiện mã độc, mã khai thác đặc biệt là các loại mã độc trong các cuộc tấn công có chủ đích APT, các loại mã độc chưa từng được biết đến.

Hệ thống nhận yêu cầu quét file từ các hệ thống khác và phân tích, đưa ra kết quả file có bị nhiễm mã độc hay không.

Hệ thống VCS - AMA sử dụng nhiều phương pháp phân tích với các tính năng và công nghệ vượt trội như Sandbox, Static Analysis, Dynamic Analysis, Machine Learning... cho phép phát hiện cả những dòng mã độc thông thường và những dòng chưa từng được biết đến.

Những tính năng chính

Phân tích đa lớp thông minh

Giải pháp VCS - AMA áp dụng các công nghệ phân tích khác nhau giúp phân tích theo nhiều lớp như:

- Quét file, URL dựa trên tập cơ sở dữ liệu đã được phát hiện.
- Phân tích tĩnh dựa trên nội dung file để đánh giá điểm bất thường.
- Quét động file office, file pdf, URL bằng cách thực thi trong môi trường cô lập để đánh giá tác động.

Chống mã độc cao cấp

Một số loại mã độc cao cấp có khả năng nhận diện môi trường ảo, từ đó, có các hành vi ẩn mình hoặc vượt qua môi trường đó (bypass). Giải pháp VCS - AMA sử dụng các module làm giảm thiểu tối đa sự khác biệt giữa máy ảo phân tích và máy thật của người dùng, đồng thời giả lập các thao tác từ đó chống được các hành vi bypass của mã độc.

Phân tích mã độc động trên sandbox

VCS - AMA chạy các file office, pdf và các URL nghi ngờ trong trong các môi trường ảo để theo dõi các hành vi như: kết nối C&C, tạo tiến trình, ghi key khởi động cùng hệ thống, ghi file, hay các hành vi độc hại.

Áp dụng các cơ chế quét, phân tích thông minh, phân tích hành vi kết hợp với các tri thức khác để phát hiện mã độc hay các kết nối độc hại.

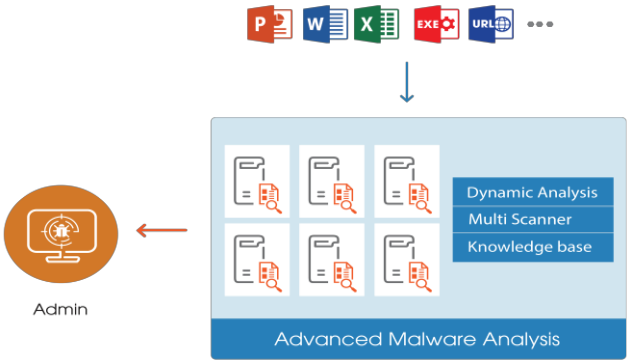
Tích hợp với các hệ thống khác

Giải pháp cung cấp một tập đầy đủ các API, cho phép các hệ thống khác dễ dàng tích hợp để phân tích và lấy các kết quả phân tích đó:

- API upload file tới VCS - AMA để phân tích
- API upload URL tới VCS - AMA để phân tích
- API lấy kết quả quét file
- API lấy kết quả quét URL

Ngoài ra, hệ thống cho phép người dùng cấu hình giới hạn thời gian quét trong môi trường VCS - AMA. Cấu hình mặc định là 2 phút.

Mô hình triển khai giải pháp



Giải pháp VCS - AMA bao gồm:

- **Thành phần Sandbox:** Nền tảng ảo hóa cho phép cài đặt các máy ảo phân tích với tài nguyên tiết kiệm và môi trường tối ưu cho quá trình phân tích mã độc trên môi trường sandbox. Hỗ trợ khả năng tùy biến môi trường phân tích.
- **Thành phần quét mã độc tĩnh:** Là tập hợp cơ sở dữ liệu và các thành phần phân tích file tĩnh, dựa trên cấu trúc và nội dung của file để đánh giá các điểm bất thường.
- **Thành phần quét mã độc động:** Là các thành phần phân tích động trên môi trường Sandbox, dựa trên hành vi của file khi chạy trong môi trường thực để đánh giá các dấu hiệu bất thường. Hỗ trợ phân tích các loại file thực thi, file office, pdf, java, script, ...

ƯU ĐIỂM

1. Phát hiện những dòng mã độc mới, mã khai thác 0-day, 1-day trong các chiến dịch tấn công APT.
2. Chống hành vi bypass của các mã độc cao cấp.
3. Dễ dàng triển khai, tích hợp.