ỨNG DỤNG GIẢI PHÁP GIÁM SÁT WEBSITE TẬP TRUNG TẠI MỘT BỘ Ở VIỆT NAM

Nhận được yêu cầu tư vấn từ một Bộ ở Việt Nam, Công ty Công ty Cổ phần công nghệ an ninh không gian mạng Việt Nam (VNCS) đã tiến hành khảo sát hệ thống của Bộ. Vấn đề triển khai ứng dụng CNTT đã được đẩy mạnh để phục vụ cho các công tác quản lý, điều hành, nâng cao hiệu quả công việc. Song song với hệ thống mạng vận hành, nhằm tăng cường thêm khả năng phòng, chống các nguy cơ tấn công, xâm nhập hệ thống công nghệ thông tin và ngăn chặn, khắc phục kịp thời các sự cố mất an toàn thông tin trên hệ thống mạng cũng như ngăn ngừa việc lộ, lọt tài liệu thông tin bí mật nhà nước. Các lãnh đạo của Bộ đã chủ động đầu tư thêm các trang thiết bị để bảo vệ toàn bộ hệ thống mạng như các thiết bị tường lửa, hệ thống phát hiện xâm nhập, hệ thống chống thất thoát dữ liệu…

Trách nhiệm quản lý không chỉ đối với các hệ thống đặt tại Bộ, mà còn phải quản lý các website tại các đơn vị trực thuộc tại nhiều địa phương khác nhau (không đặt tại datacenter của Bộ). Mặc dù cũng đã được đầu tư rất nhiều, nhưng đội ngũ kỹ thuật vẫn phải làm việc rất vả và rất cần thiết phải có các giải pháp quản lý tập trung, giúp cơ quan quản lý có thể nhanh chóng nắm bắt được tình hình toàn bộ hệ thống, cho phép người quản trị có thể tự động lọc, phân tích các dữ liệu hệ thống. Công việc này cần được thực hiện định kì và hoàn toàn tự động, đưa ra được các cảnh báo sớm nhất khi có các dấu hiệu hệ thống bị tấn công.

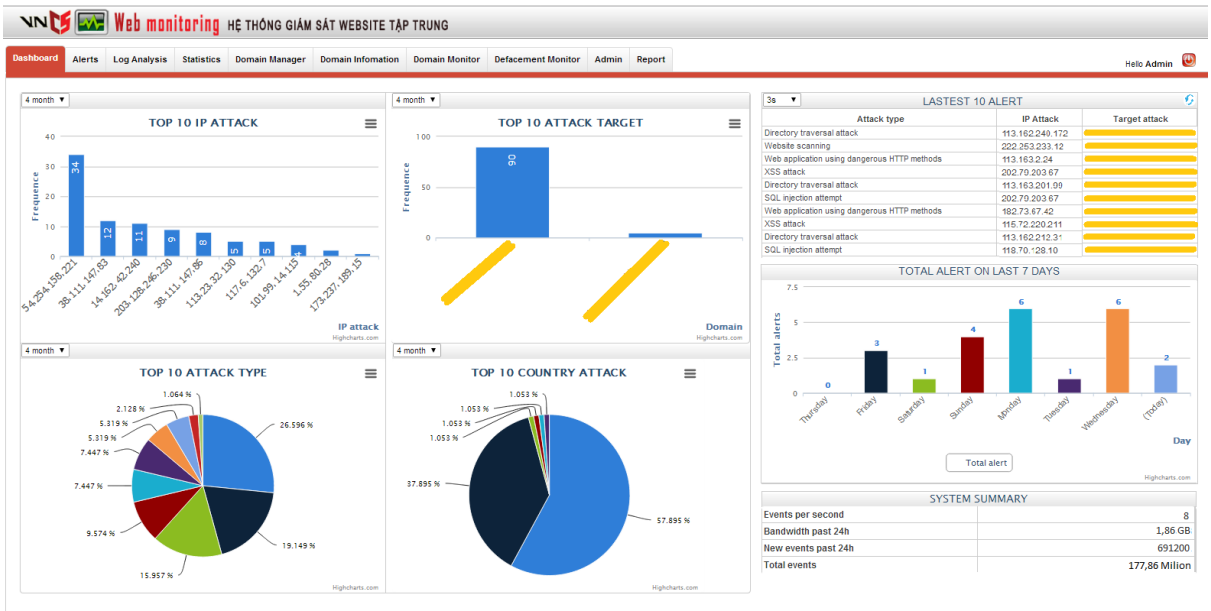
Phòng CNTT tại Bộ này đã từng khảo sát và triển khai thử một số giải pháp, sản phẩm giám sát tập trung của nước ngoài như IBM/Qradar, HP/ArcSight, Symantec …Các sản phẩm này đều được tích hợp đóng gói sẵn rất nhiều tính năng cho người dùng giám sát toán bộ hệ thống mạng. Qua quá trình sử dụng sản phẩm, có những hạn chế nhất định: đó là giao diện quản lý chưa thực sự thân thiện, người dùng khó có thể tập trung vào các tính năng mà họ cần. Các sản phẩm này có những tính năng được tích

hợp sẵn trong sản phẩm nhưng không thật sự cần thiết, từ đó người dùng mặc dù không muốn nhưng vẫn phải bỏ ra khoản đầu tư không hề nhỏ để mua một sản phẩm chỉ để đáp ứng một vài nhu cầu của mình. Các sản phẩm này cũng không tập trung vào việc giám sát các vấn đề liên quan đến website và khả năng tùy biến với các hệ thống mạng chưa cao.

Trước tình huống này, VNCS đã giới thiệu đến Bộ giải pháp giám sát website tập trung (VNCS Web Monitoring). VNCS Web Monitoring là sản phẩm được VNCS phát triển hoàn toàn, không phụ thuộc vào các công nghệ của nước ngoài, do đó có khả năng khắc phục được hầu hết các hạn chế mà các sản phẩm nước ngoài không có được.

VNCS đã triển khai giải pháp này tại Bộ. Để có thể triển khai được VNCS Web Monitoring chỉ cần một thành phần agent thực hiện đổ log về thiết bị của VNCS Web Monitoring (đây là máy chủ hoàn toàn độc lập, được đặt tại datacenter của Bộ, do đó VNCS Web Monitoring sẽ không can thiệp hay ảnh hưởng gì tới hoạt động các máy chủ khác).

Sau khi cài đặt và cấu hình thông tin các tên miền cần quản lý, người quản trị có thể đăng nhập và theo dõi tình trạng các website trên hệ thống của mình trên một màn hình duy nhất. Dưới đây là một số giao diện thực tế khi chạy hệ thống giám sát website tại Bộ:



3s

LASTEST 10 ALERT

Attack type	IP Attack	Target attack
Directory traversal attack	113.162.240.172	
Website scanning	222.253.233.12	
Web application using dangerous HTTP methods	113.163.2.24	
XSS attack	202.79.203.67	
Directory traversal attack	113.163.201.99	
SQL injection attempt	202.79.203.67	
Web application using dangerous HTTP methods	182.73.67.42	
XSS attack	115.72.220.211	
Directory traversal attack	113.162.212.31	
SQL injection attempt	118.70.128.10	

Bảng trên là thông tin tóm tắt của 10 cảnh báo gần nhất mà VNCS Web Monitoring phát hiện được. Mặc dù VNCS Web Monitoring được đặt sau rất nhiều thiết bị bảo vệ của hệ thống tại Bộ này, các dòng thông tin phía trước đã bị các thiết bị tường lửa và hệ thống phát hiện xâm nhập chặn bắt và phân tích khá nhiều, nhưng VNCS Web Monitoring vẫn tỏ ra hoạt động khá tốt, phát hiện ra một số dấu hiệu tấn công nguy hiểm mà các thiết bị bảo vệ phía trước không phát hiện ra được.

Đồng thời, trên giao diện quản lý tập trung, người quản trị có thể nắm bắt được tình hình chung của toàn hệ thống, thống kê các sự kiện và lượng truy cập hằng ngày trên hệ thống.

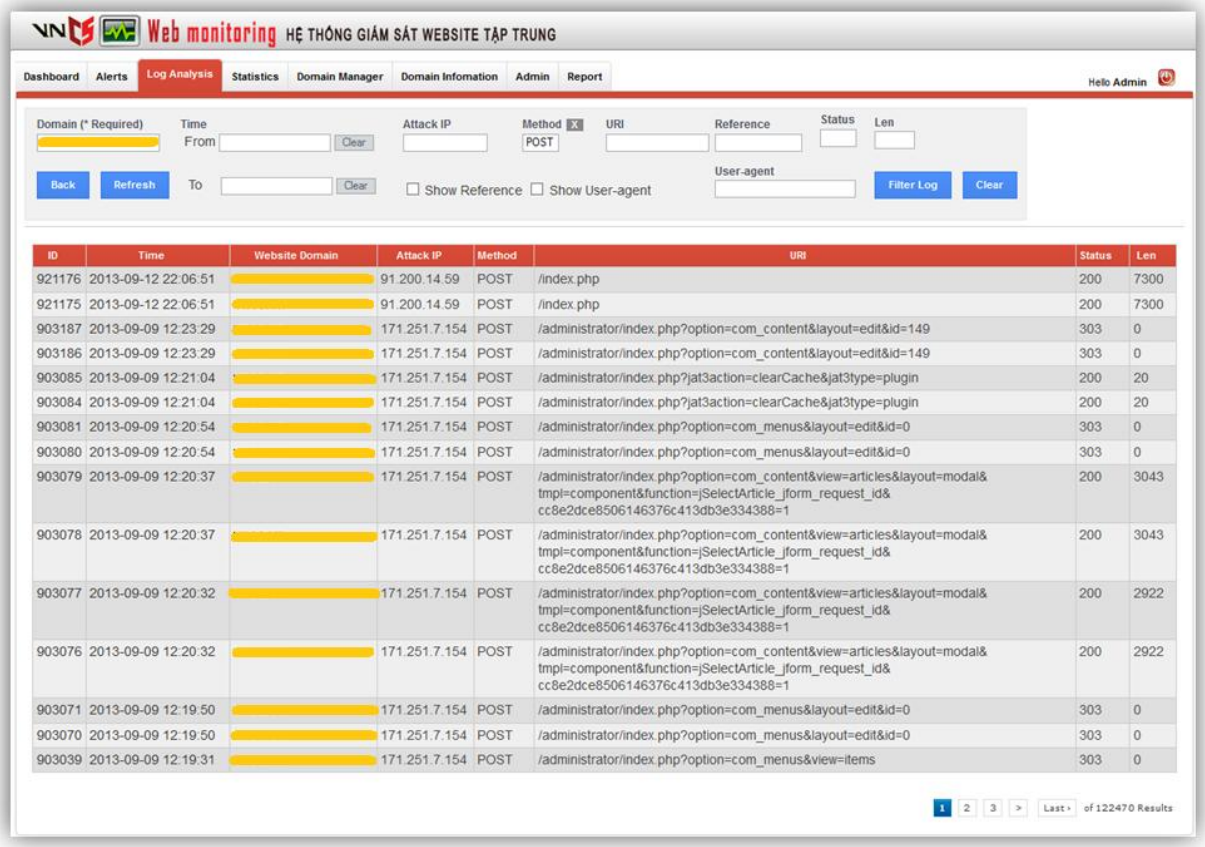
SYSTEM SUMMARY

Events per second	8
Bandwidth past 24h	1,86 GB
New events past 24h	691200
Total events	177,86 Milion

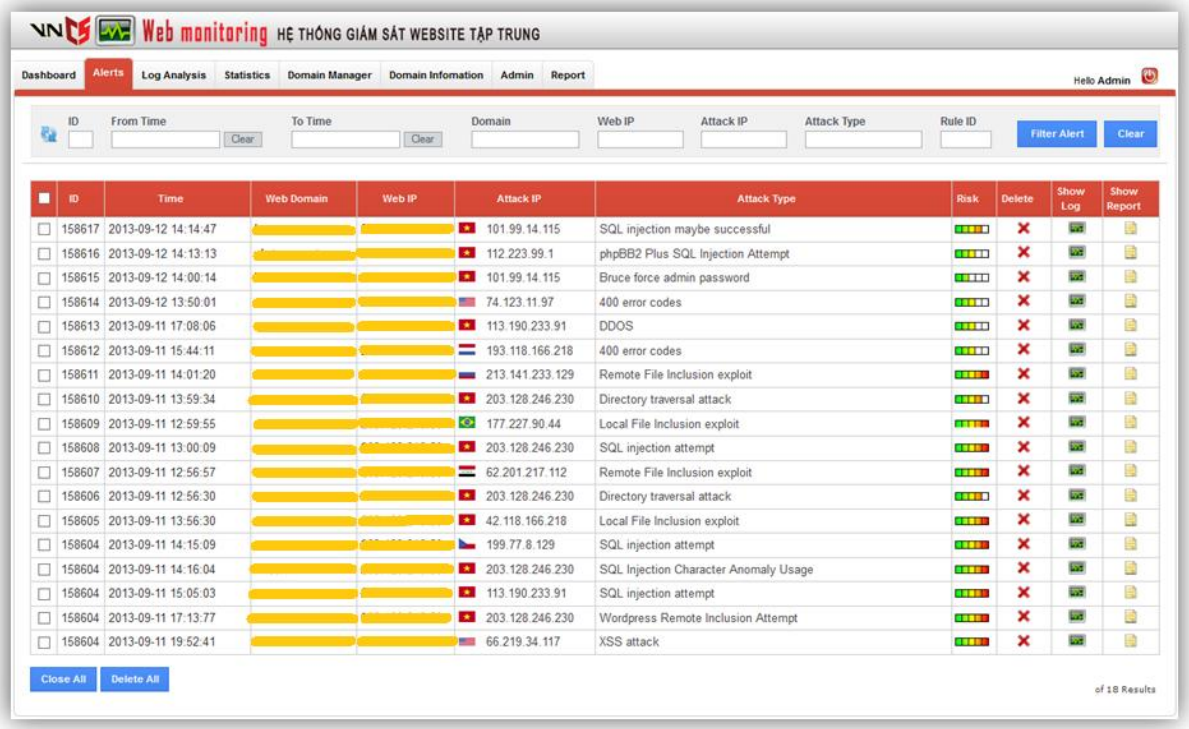
Với thống kê hệ thống hằng ngày như vậy, có thể dễ dàng nhận biết được khi hệ thống có dấu hiệu lạ như số lượng các sự kiện và băng thông tăng nhanh một cách đột biến. Đó có thể là một trong các dấu hiệu của một cuộc tấn công từ chối dịch vụ (DoS, DDoS).v.v.

Điểm đặc biệt của VNCS Web Monitoring, đó là khả năng phân tích, chọn lọc, phân loại các thông tin thu được từ hệ thống, người quản trị hoàn

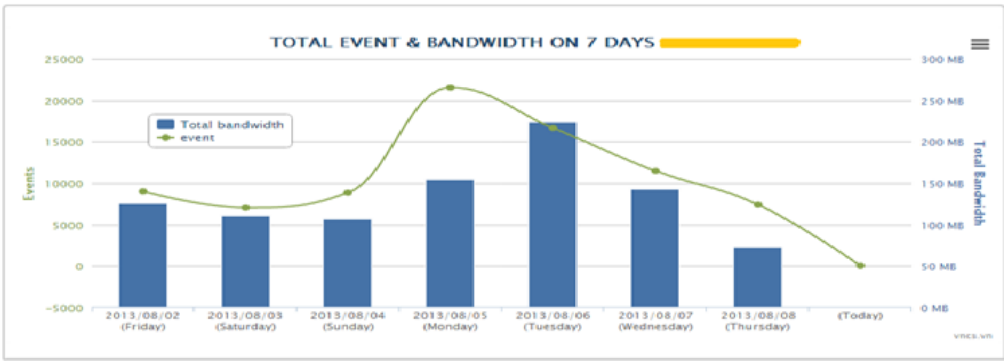
toàn có thể tự mình phân tích các dòng log đổ về bằng Giao diện phân tích bằng tay.



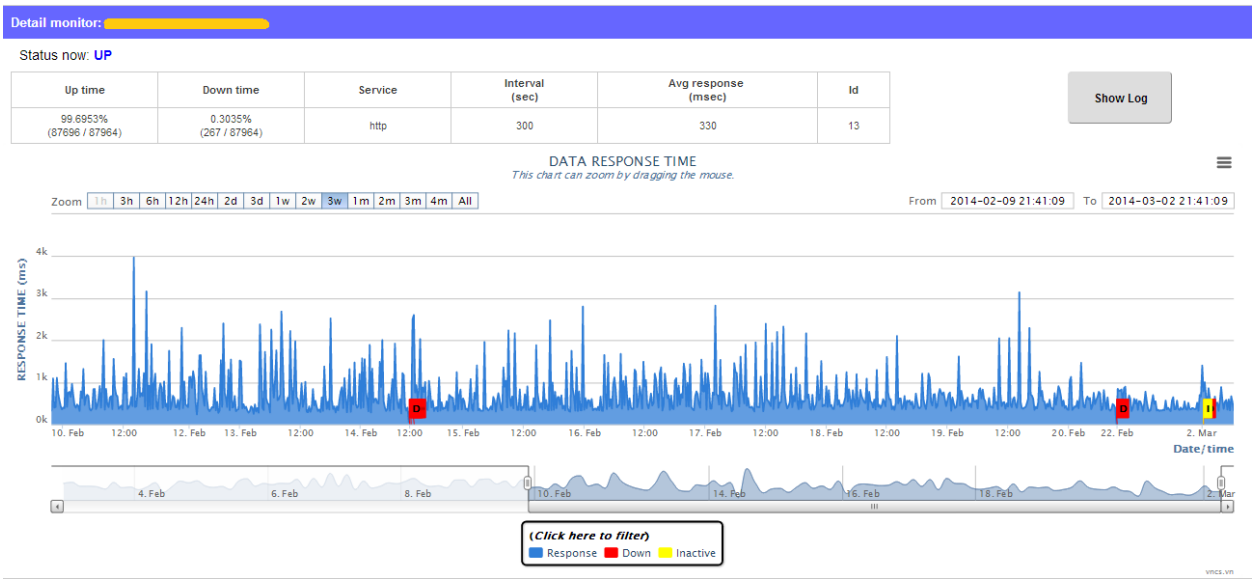
VNCS Web Monitoring có hệ thống cơ sở dữ liệu các mẫu tấn công khá đầy đủ do được cập nhật đặc điểm nhận dạng liên quan đến các cuộc tấn công mới nhất hiện có trên thế giới một cách thường xuyên. Bằng các thuật toán thông minh, hệ thống giám sát website có thể tự động phân tích các tình huống tấn công và sẽ gửi cảnh báo tức thời (qua Email, SMS) đến người quản trị khi phát hiện có tấn công vào website. Giải pháp này giúp người quản trị không cần can thiệp vào hệ thống log mà vẫn nhận được các báo cáo tấn công. Các hình thức tấn công mới luôn được đội R&D nghiên cứu và cập nhật sớm nhất để tích hợp vào hệ thống. Vì thế hệ thống có thể phát hiện chính xác và kịp thời các tấn công mới. Dưới đây là một số hình ảnh khi chạy trực tiếp theo dõi 30 website của Bộ này.



Với một giao diện thân thiện và trực quan. VNCS Web monitoring đưa ra các thống kê về các hình thức tấn công, các địa chỉ tấn công. Bên cạnh đó, VNCS Web Monitoring dựa trên một số kỹ thuật đánh giá đặc biệt (như Evaluation Correlation) để đánh giá, phân loại mức độ nguy hiểm của các kiểu tấn công. Đưa ra cái nhìn tổng quan nhất về hệ thống cũng như các sự kiện mới, số log gửi về trên hệ thống. Thông qua các hình thức tấn công, người quản trị có thể lần ra các dấu vết tấn công, để đưa ra các hình thức xử lý thích hợp. Thông qua các hệ thống này quản trị có thể sơ bộ phát hiện ra các cuộc tấn công vượt qua giới hạn cho phép như DoS, DDoS.



Tình trạng website dead/live được theo dõi thường xuyên, với giao diện biểu đồ trực quan, cho phép người quản trị theo dõi xem trong 1 khoảng thời gian (6h, 12h, 24h, 1 tuần, 2 tuần, 1 tháng, 2 tháng,…) website cần theo dõi bị ngừng bao nhiêu lần, thông tin lỗi xảy ra.



Nhờ được tích hợp sẵn vào sản phẩm VNCS Webmonitoring, Deface Monitor tính năng phát hiện website bị tấn công thay đổi nội dung (deface). Deface không chỉ gây thiệt hại về kinh tế, mà còn ảnh hưởng rất lớn uy tín và hình ảnh của các cơ quan, tổ chức khi hacker đưa các hình ảnh xấu lên website. Đây là một tính năng thực sự rất hữu ích cho người quản trị hệ thống. Trên thị trường hiện nay, rất ít các sản phẩm có tính năng này, hoặc như có cũng chưa được tối ưu hoặc tiện lợi cho người sử dụng. Với tính năng phát hiện tấn công deface website, người quản trị hệ thống hoàn toàn có thể yên tâm khi có bất kì sự thay đổi nào bất thường trên hệ thống, VNCS Webmonitoring sẽ gửi ngay cảnh báo cho quản trị viên (Email, SMS) kèm với ảnh chụp website để xác minh.

Khi theo dõi hệ thống của Bộ này, khi có bất kì tấn công nào xảy ra, hoặc hệ thống website bị ngừng hoạt động đột xuất VNCS Web monitoring ngay lập tức sẽ gửi cảnh báo đến người dùng, giúp quản trị viên hệ thống.

Chào [redacted]
Website [redacted] vừa bị tấn công.
Thông tin tấn công như sau:
- Thời gian tấn công: **2013/09/25 15:52:49**
- Địa chỉ IP tấn công: 101.99.14.115 **(Viet Nam)**
- Kiểu tấn công: **Web application using dangerous HTTP methods**

Chi tiết cuộc tấn công:

Time	2013/09/25 15:52:49
Target attack	[redacted]
Attack IP	101.99.14.115
Attack type	Web application using dangerous HTTP methods
Method	OPTIONS
URI	[redacted]
Status	200
Length	0
Useragent	Mozilla/5.00 (Nikto/2.1.5) (Evasions:None) (Test:httpoptions: OPTIONS *)

Tính năng xuất ra các báo cáo là một phần không thể thiếu của bất cứ hệ thống giám sát nào. VNCS Web Monitoring cho phép người quản trị có thể trích xuất ra các báo cáo bất cứ lúc nào, hoặc có thể cấu hình lập lịch để hệ thống tự động tạo ra các báo cáo và gửi tới các địa chỉ mail đã được chỉ định sẵn.

Trước khi triển khai hệ thống, Bộ không thể nhận biết bất cứ khi nào các website bị tấn công ? không truy cập được (down)… Nhưng sau khi triển khai VNCS Web Monitoring, hệ thống phát hiện 20-30 cuộc tấn công mỗi ngày từ các nước khác nhau, nhờ đó đội ngũ kỹ thuật đã đưa ra các phản ứng kịp thời. Đồng thời lãnh đạo cũng nắm bắt được tình hình nhờ có các bản báo cáo do hệ thống đưa ra từ đó có sự đầu tư hợp lý vào công tác bảo mật.