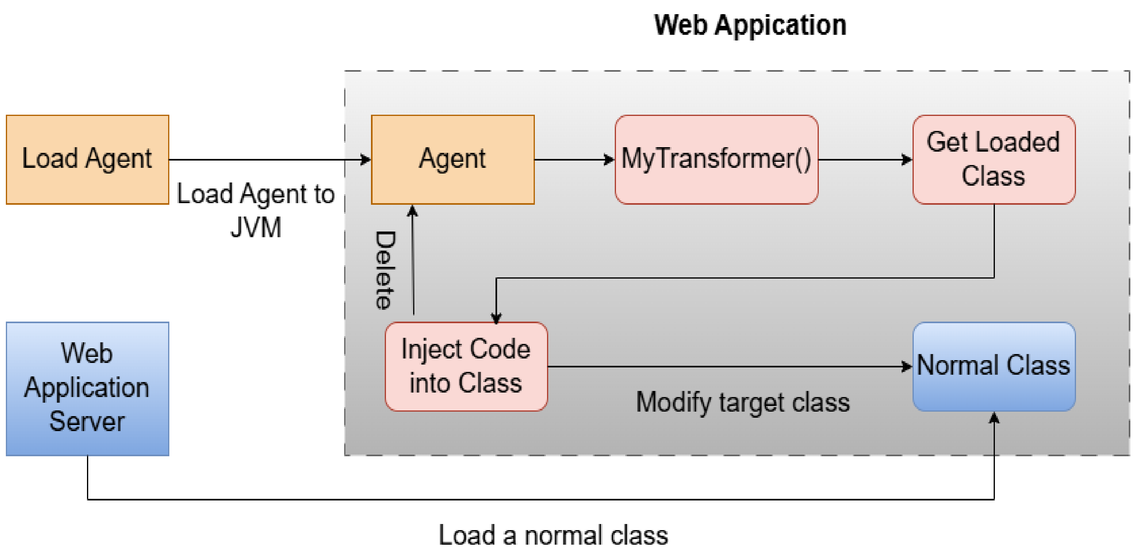
TridentShell: An enhanced covert and scalable backdoor injection attack on web applications

Thành viên nhóm: Đinh Bạch Kiều Phương (21520406), Phạm Trần Hồng Phúc (22521138), Nguyễn Phúc Nhi (22521041)

Mã nhóm: G14, Mã đề tài: S27, GVHD: Phạm Văn Hậu - Phan Thế Duy

Giới thiệu

TridentShell là một loại mã độc web shell fileless khó bị phát hiện. Khác với các phương pháp cũ, TridentShell sử dụng kỹ thuật Java Bytecode Instrumentation để chèn mã vào bộ nhớ các máy chủ Java mà không thay đổi mã nguồn. Ngoài ra, nó dùng mạng blockchain NKN làm kênh liên lạc ẩn danh giữa attacker và máy chủ bị kiểm soát. Mã độc cũng có khả năng tự xóa dấu vết trên Windows. Các thử nghiệm cho thấy TridentShell vượt qua được nhiều biện pháp phòng thủ như static detection và antivirus. Nghiên cứu cũng đề xuất cách phát hiện mới bằng phân tích bytecode trực tiếp trong JVM.



Hình 1: *Mô hình tấn công*

Kết quả triển khai

Tạo ra được mã độc bằng phương pháp được đề cập trong bài báo và khai thác thành công nhưng vẫn còn các hạn chế sau:

- Chỉ mới thực nghiệm trên Tomcat, chưa thực nghiệm được trên nhiều loại máy chủ ứng dụng web khác.
- Chưa thực nghiệm được phiên bản cải tiến với mạng NKN của TridentShellAgent.
- Chưa thực nghiệm được cách phát hiện mã độc dựa trên phương pháp của tác giả..

Hình 3: *Kết quả khi khai thác backdoor*

Phương pháp

Sử dụng kỹ thuật Java instrumentation để hook các class cụ thể bên trong web java qua cơ chế tự động load JAR của server. Khiến class backdoor được load lên và mở ra có thể tấn công bằng phương thức POST lên trang web.

Xây dựng môi trường thực nghiệm là một ứng dụng web sử dụng server Tomcat và tạo file mã độc có khả năng tạo một backdoor:

- File mã độc được build bằng maven, sau đó chèn vào thời điểm khởi động của trang web bằng kỹ thuật Java Instumentation và khởi chạy server.
- Khi run server thì backdoor đã được chèn vào server thành công. => Tấn công bằng phương thức post với serectkey = backdoor&cmd=dir.
- Kiểm tra console log để kiểm tra kết quả.

Workflow của mã độc:

- Bước 1: Tải và kích hoạt Agent
- Bước 2: Gắn Transformer để can thiệp bytecode
- Bước 3: Xóa file JAR ra khỏi đĩa.

Hình 2: *Kết quả khai thác thành công Tomcat server*