PRO|LOG

담당	팀장	사장

로그 분석 보고서

총괄 보고서

2017-11-30

목차

1. 로그 분석 결과

전체 로그 중 총 334개의 위험이 탐지되었습니다.
(탐지 로그/전체 로그 : 334/11789)
탐지 된 334개의 위험 중 심각한 위험이 44개 발견되었습니다.
전문가의 조치가 즉시 필요합니다.
Pro|Log 홈페이지의 고객센터에서 도움을 받으시는 것을 권고합니다.

2. 로그 분석 세부 사항

A. 로그 현황 분석

로그 현황		
전체 로그	**탐지 로그[1]**	**위험로그[2]**
11789	334	44

- ▶ 로그 수집 기간 : 2012.05.03 ~ 2012.05.04
- ▶ 로그 출처
  - -IP : 201.104.203.1
  - -PORT : 8889
  - -운영체제 : Microsoft Internet Information Services 6.0

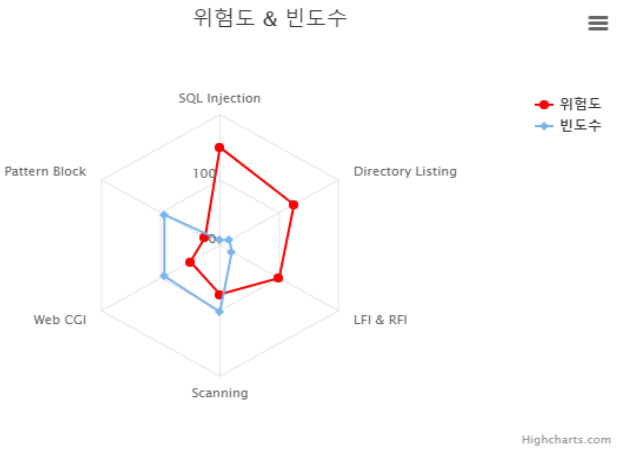
-로그 분석 결과 공격이 많이 들어온 국가는 대한민국(80.54%), 미국(14.07%), 인도네시아(5.39%) 순 입니다.

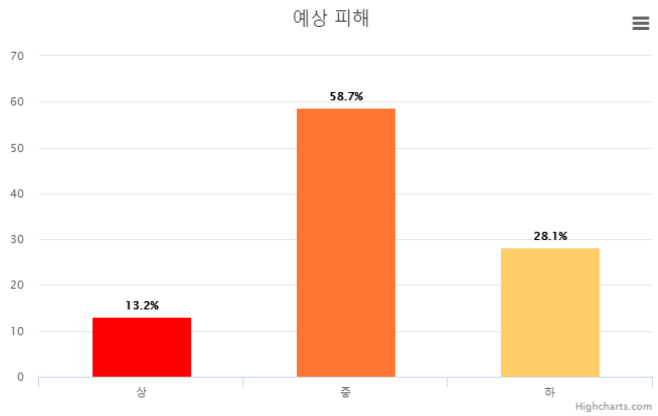
-로그 분석 결과 공격이 많이 들어온 IP는 124.2.44.105(한국), 121.152.227.82(한국), 221.39.150.195(한국), 66.249.71.46(미국) 순 입니다.

공격 빈도가 높은 국가 및 IP	
국가	1. 대한민국 (80.54%)
	2. 미국 (14.07%)
	3. 인도네시아 (5.39%)
IP	1. 124.2.44.105 (26.3%)
	2. 121.152.227.82 (16.5%)
	3. 221.39.150.195 (16.2%)
	4. 66.249.71.46 (9.3%)

[1] 탐지 로그 : 전체 로그 중 위험 요소가 탐지 된 로그.
[2] 위험 로그 : 탐지 로그 중 위험도가 높은 로그 (위험 2단계)

B. 차트 세부 분석





예상피해 레벨	공격 유형	위험도	예상 피해	위험 단계	빈도수
상	SQL Injection	6	개인(DB) 정보 노출, 2차 공격 발생 가능성	[1]위험 2 단계	8
	Directory Listing	5	개인 정보 탈취, 웹 서버 공격	위험2단계	16
	LFI&RFI	4	공격 컴퓨터에 악성 코드 발생	위험2단계	20
중	Scanning	3	개인 정보 수집, 추가 공격 가능성	[2]위험1단계	102
	Web CGI	2	웹 쿠키 정보 노출, 거짓 페이지 생성 후 개인 정보 탈취	위험1단계	94
하	Pattern Block	1	시스템 과부하 및 서비스 성능 저하	위험1단계	94

- ✓ 전체 로그 11789개 중 위험 2단계 44개, 위험 1단계 300개가 발견되었습니다.
- ✓ 예상 피해 정도는 상 13.2%, 중 58.7% 그리고 하 28.1% 입니다.

[1] 위험 2단계 : 위험 로그 중 위험도가 4 이상인 로그.
[2] 위험 1단계 : 위험 로그 중 위험도가 4 미만인 로그.