SK infosec

Threat Intelligence Report

EQST INSIGHT

2018

07

EQST(이큐스트)는 'Experts, Qualified Security Team'이라는 뜻으로 사이버 위협 분석 및 연구 분야에서 검증된 최고 수준의 보안 전문가 그룹입니다.

SK infosec

Contents

EQST insight

2018년 상반기 보안 이슈는? 금전적 이득을 노리는 사이버 공격 증가

2018년 상반기에는 동계 올림픽부터 남북 정상회담까지 전 세계의 이목이 집중되는 큰 사건이 많았던 만큼 정보보안 이슈도 올림픽 해킹 공격을 비롯하여 진화된 랜섬웨어의 등장, 암호화폐 탈취 공격까지 다양했다. SK인포섹의 보안 전문가 이큐스트(EQST)그룹은 상반기 발생한 정보보안 이슈를 분석했다. 주요 이슈별 취약점과 전체 공격 현황 및 유형, 해킹 사고 사례, 사용된 악성코드 등을 상세히 알아보자.

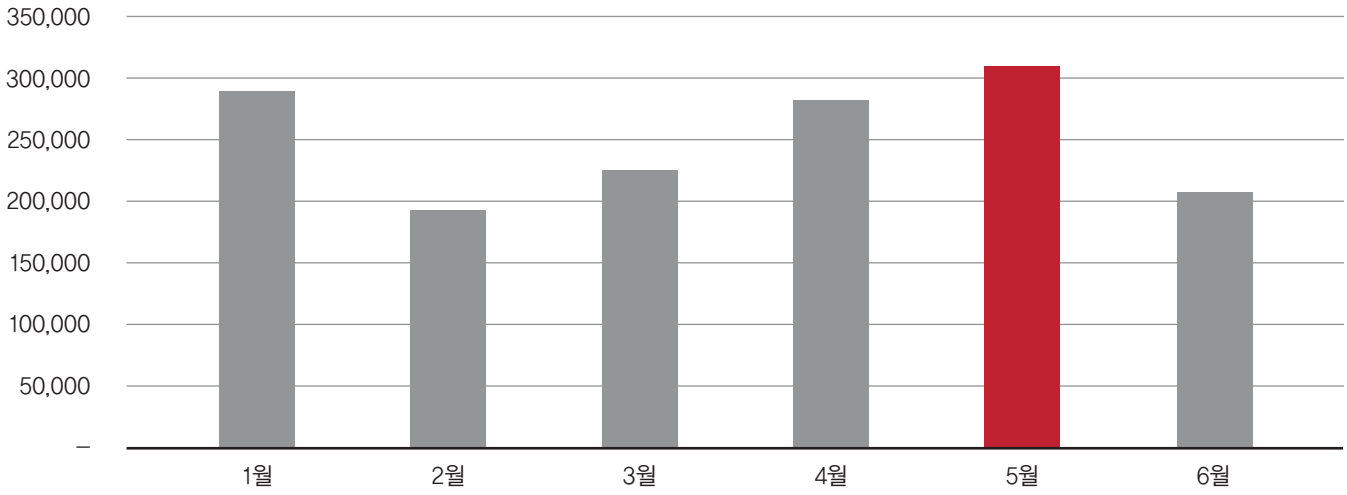
2018년 상반기 정보보안 사고 리뷰

[2018년 상반기 주요 정보보안 사고]

지난 1월, G사에서 발표한 I사의 CPU 취약점인 멜트다운(Melt Down)과 스펙터(Spector)는 CPU 아키텍처 취약점으로, 공격자가 데이터를 가로채기하여 볼 수 있다. 매우 치명적인 취약점인 것에 비해 아직 특별한 공격 징후는 보이지 않고 있으나, 멜트다운과 스펙터 보안 패치 이후에 성능 저하가 발생해 패치를 주저하는 기업들이 있었다. 그럼에도 포털사이트와 게임사 등 대형 사이트에서 패치를 진행하였고, 약 10% 정도의 성능 저하가 발생했다. 2월에는 평창 동계올림픽 해킹 사고가 있었다. 메인 프레스 센터로의 영상 전송과 공식 홈페이지의 입장권 판매 및 출력 등의 서비스가 원활하지 못했으나, 조사보다는 긴급 복구로 방향을 선회하면서 원인을 밝혀내지는 못하였다. 사건의 배후로는 러시아 해킹 그룹이 지목되었다. 3월에는 갠드크랩(GandCrab) 랜섬웨어가 유포되어 많은 PC가 랜섬웨어에 감염되는 사고가 발생했다. 갠드크랩은 파일리스(Fileless) 보안 솔루션 우회 기법과 같은 다양한 보안 취

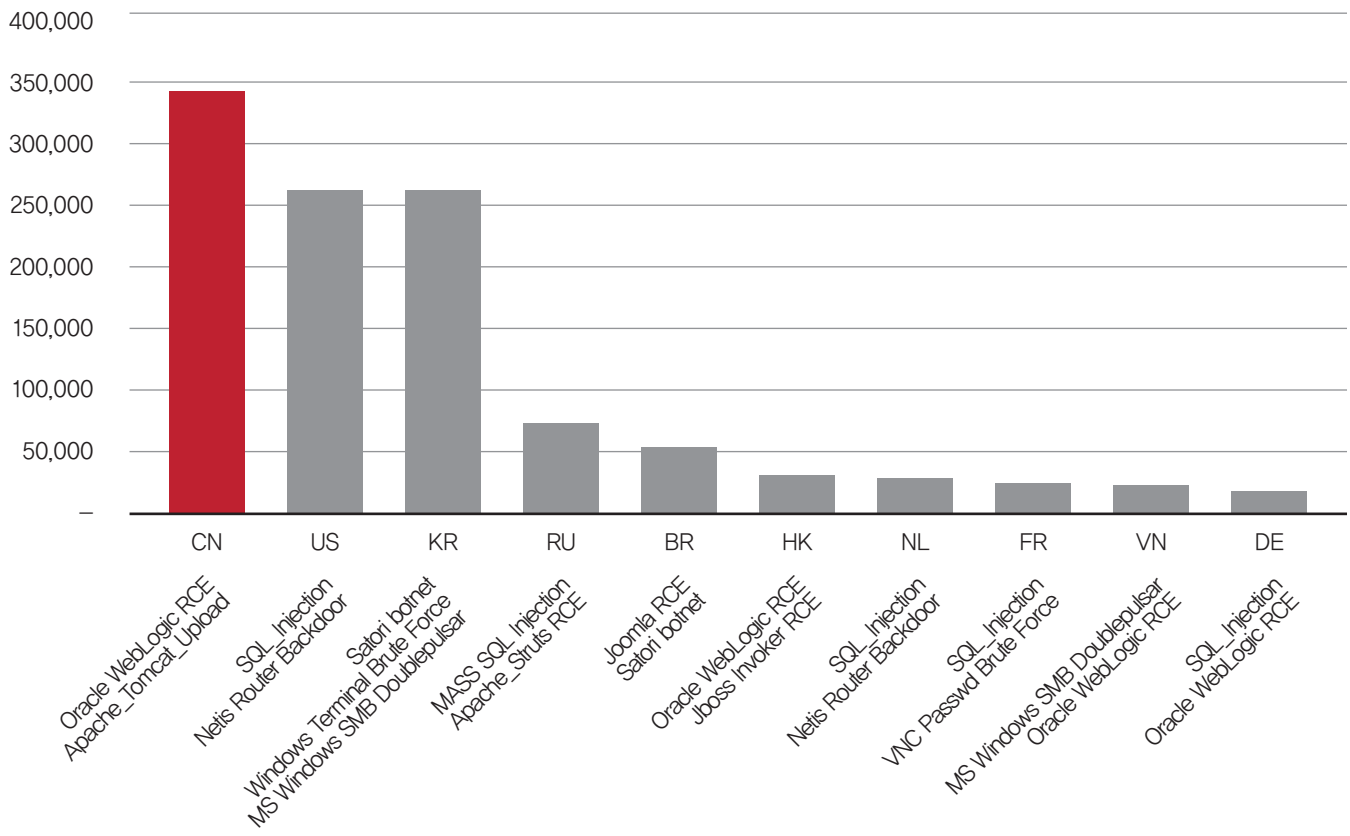
약점과 결합해 전파되었고, 지속적으로 상위 버전이 배포되었다. 이외에도 에르메스(Hermes), 마이랜섬(MyRansom) 등 다양한 랜섬웨어가 유포되었다. 5월에는 액티브X(ActiveX) 취약점을 통해 전파되는 악성코드가 발견되었다. 낮은 버전의 액티브X 사용자가 해당 사이트에 접속하면 악성코드에 감염 되는데, 배후로는 북한으로 추정되는 그룹이 지목되었다. 6월에는 2건의 암호화폐거래소 해킹 사고가 있었다. C사의 400억 암호화폐 탈취 해킹 사고, B사의 189억 암호화폐 탈취 해킹 사고가 발생했으나, 아직 사건이 마무리되지 않아 원인이 밝혀지지는 않았다. 권한을 가진 운영자를 타깃으로 여러 가지 형태로 악성코드 감염을 시도해 감염시킨 후, 접근통제 등 보안 솔루션을 거쳐 코인서버에 접근한 뒤 암호화폐를 탈취했을 것으로 추정된다.

상반기 해킹 공격 통계



[2018년 월별 해킹 공격 건수]

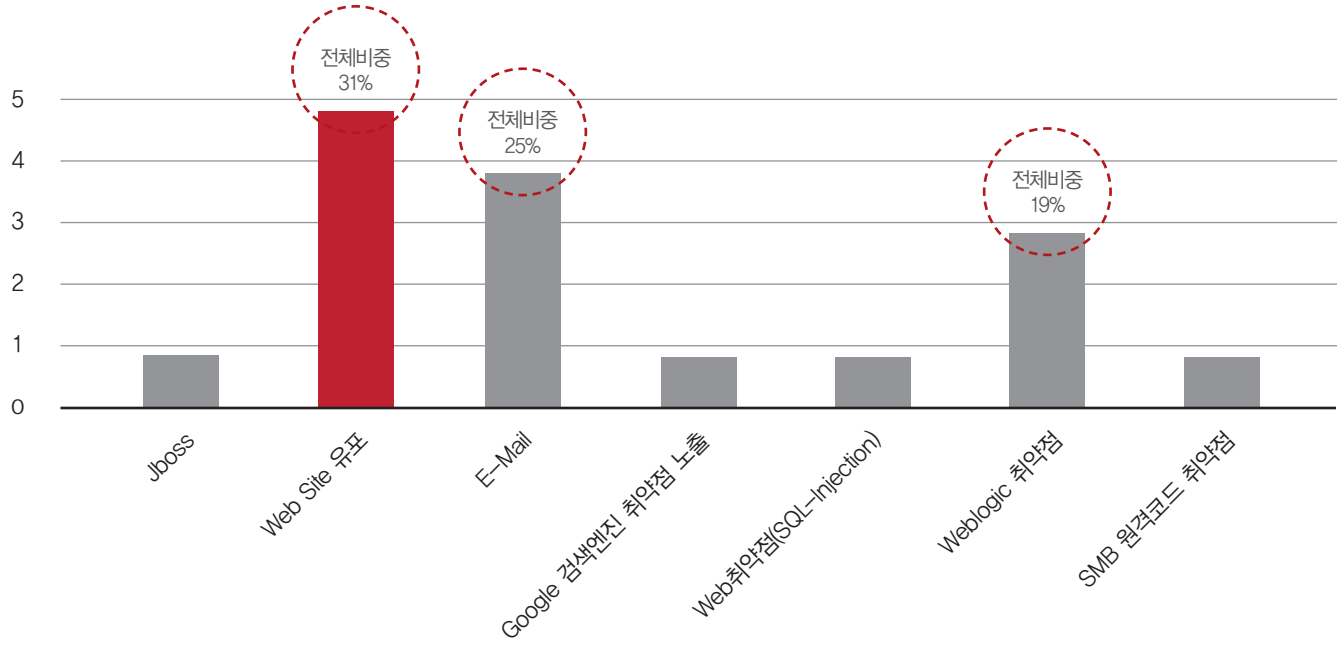
’18년 상반기의 전체 공격 발생 이벤트 건수는 총 157만 건이며, 월평균 26만 건의 해킹 공격 이벤트가 발생한 것으로 확인되었다. 특히, 5월이 가장 높은 수치를 보였는데 한 달 동안 30만 건이 넘는 공격이 발생했다.
월별 가장 두드러진 취약점 공격을 살펴보면, 1월에는 아파치 스트럿츠(Apache Strusts) 취약점 공격이 11,016건, 2월에는 톰캣 디폴트페이지(Tomcat Default Page)에 대한 업로드 공격이 6,987건 발생하였다. 3월에는 SQL 인젝션(Injection) 공격이 9,248건, 4월과 5월에는 웹로직(Weblogic) RCE 공격이 각각 25,187건과 59,617건이 발생했다. 6월에는 사토리 봇넷(Satori Botnet)이 D브랜드와 G브랜드 인터넷 공유기를 공격하는 등 IoT 관련 봇넷 공격이 많이 탐지되었다. 월별 공격을 살펴보면 자동화 공격 툴이나 취약점을 자동으로 스캔해서 공격하는 공격 이벤트가 가장 많이 탐지되었다.



[2018년 상반기 공격 국가 Top 10 및 주요 취약점]

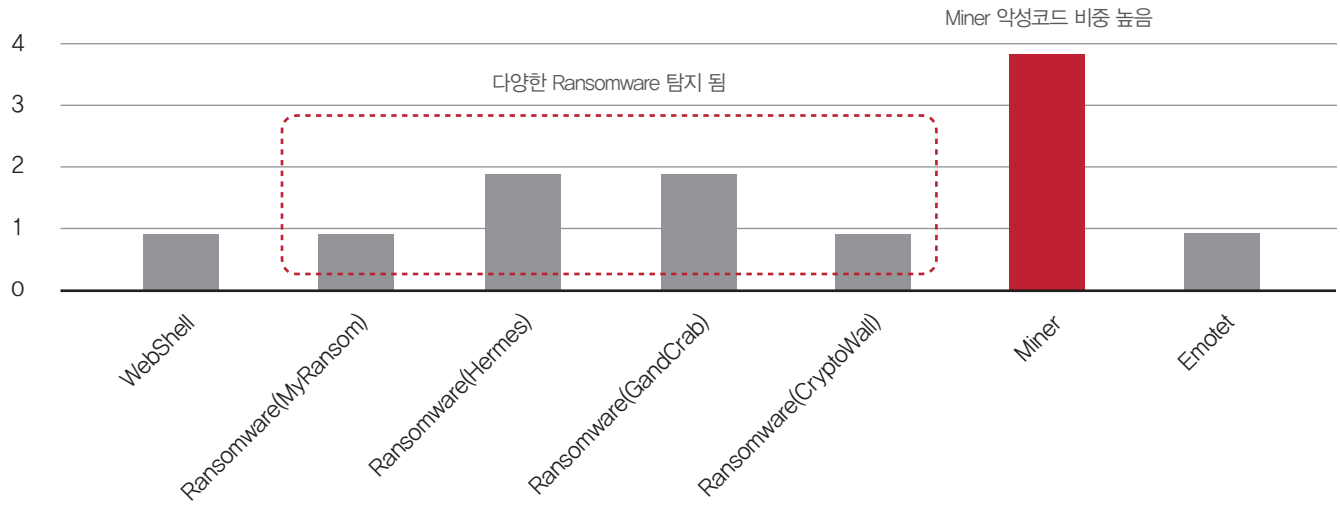
공격 국가 Top 10 통계 확인 결과, 중국에서 35만 건의 해킹 공격이 발생하여 가장 높은 비중을 차지했다. 그 다음으로 미국과 한국은 각각 26만 건의 해킹 공격이 발생해 2, 3위로 집계되었다. 중국에서는 웹로직과 톰캣 공격이 가장 많이 일어났고, 미국에서는 SQL 인젝션과 4년 전 발견된 네티스 인터넷 공유기(Netis Router) 패스워드 취약점을 이용해 악성코드를 설치하는 공격들이 탐지되었다. 한국에서는 사토리 봇넷과 터미널 브루트 포스(Terminal Brute Force) 공격, 이터널블루 취약점을 이용하는 SMB 더블펄사(Doublepulsar) 공격이 탐지되었다. 브라질의 경우, CMS 콘텐츠 오픈 소스인 줌라(Joomla) 오픈 소스에 대한 취약점 공격이 탐지되었다. 이외에도, 다른 국가에서 SQL 인젝션이나 SMB 펄사(Pulsar), VNC 패스워드 브루트 포스(Passwd Brute Force) 공격이 다수 탐지되었다.

주요 해킹 사고의 원인과 악성코드 유형



[2018년 상반기 해킹 사고 원인]

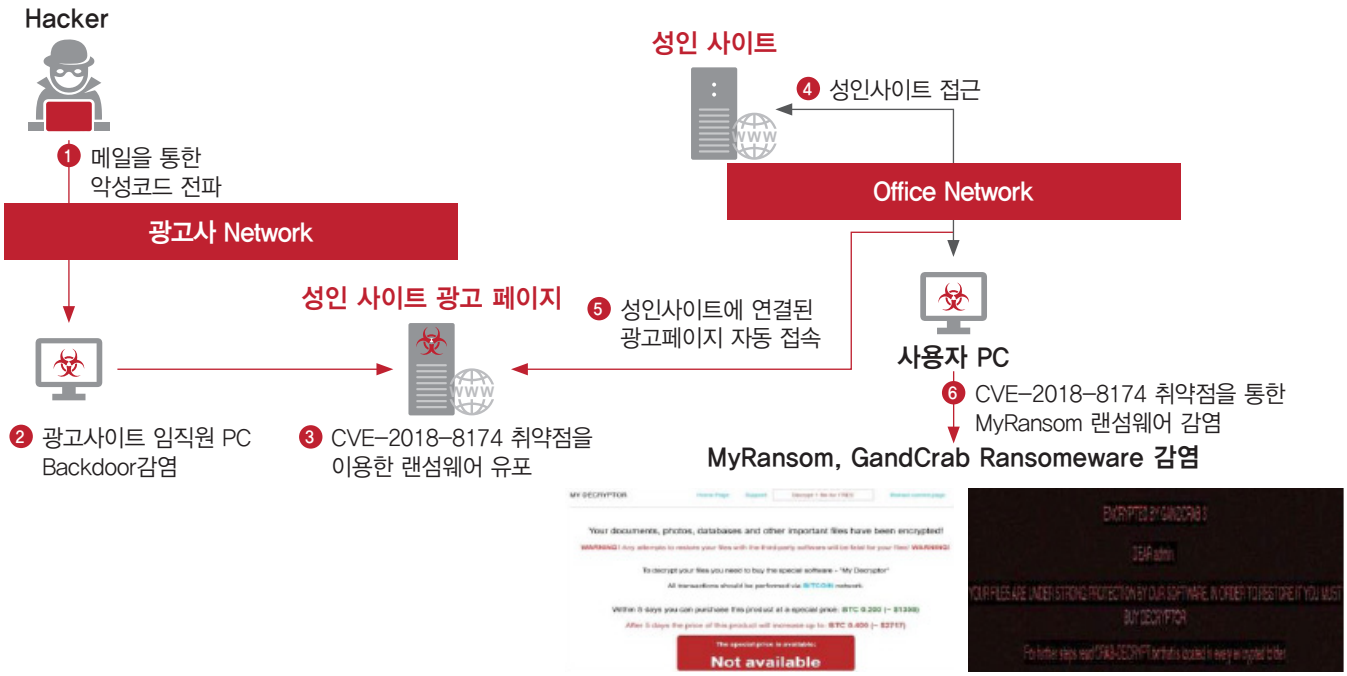
'18년 상반기 해킹 사고 원인을 분석한 결과, 전체 16건 중에서 웹 악성코드 유포가 31%로 가장 많은 비중을 차지했으며, 이메일을 통한 사고 유입이 25%, 웹로직 취약점을 통한 사고 유입이 19%로 확인되었다. 익스플로러와 VB 스크립트 취약점이 결합된 웹 악성코드가 발전하고 있으며 제이보스(Jboss) RCE 취약점과 SQL 인젝션, 웹로직 RCE 취약점, SMB 관련 원격 코드 취약점 등을 활용한 사고도 발생하였다.



[2018년 상반기 악성코드 유형]

공격자는 다양한 취약점을 이용하여 랜섬웨어를 설치하였다. 암호화폐 채굴(Miner) 악성코드를 포함하여 가상화폐를 목표로 한 공격은 전체 악성코드 중 80% 이상으로 확인되었다. 랜섬웨어 종류 또한 마이랜섬, 에르메스, 갠드크랩, 크립토월(Crytowall) 등으로 매우 다양해졌다. SMB 더블펄사 취약점을 이용하여 클라우드 서버의 가상머신 300대 이상에 암호화폐 채굴 악성코드를 감염시킨 사고도 발생했다.

갠드크랩 랜섬웨어 감염 시나리오

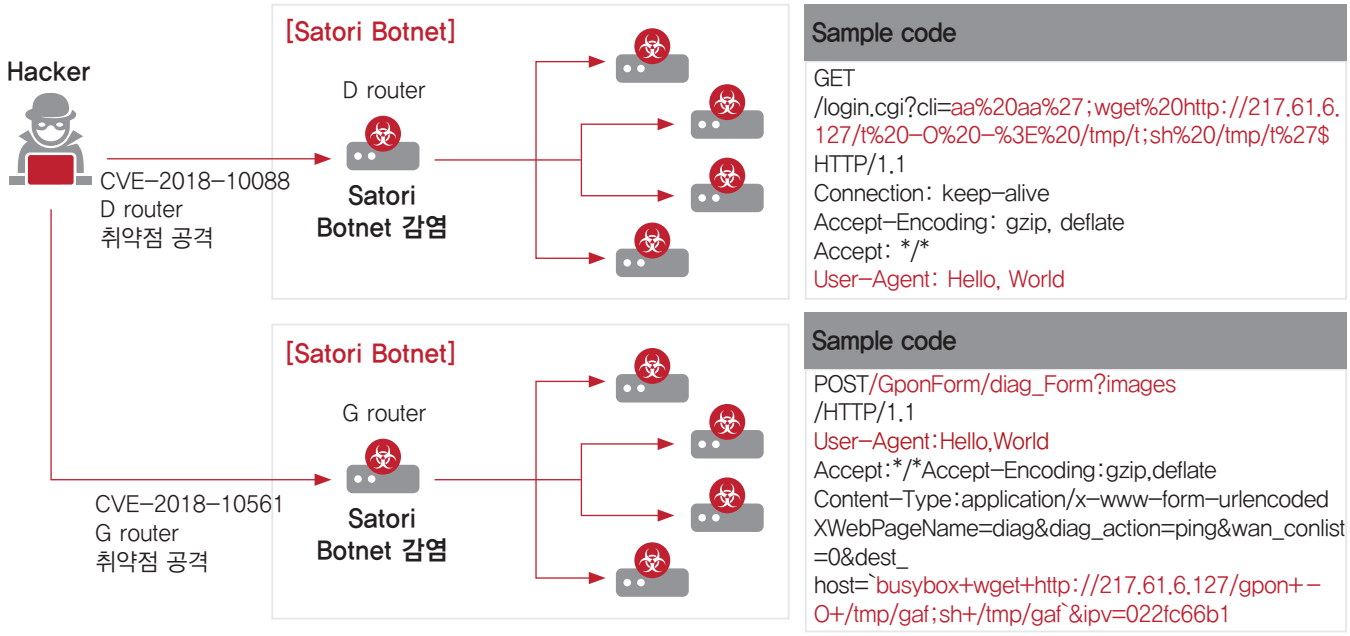


[갠드크랩(GandCrab) 랜섬웨어 감염 시나리오]

'18년 상반기에는 갠드크랩과 마이랜섬웨어 감염 사고가 발생하였다. 이 공격은 신규 취약점과 은닉형 공격 기법이 결합하여 진화한 형태로, 웹 악성코드 유포 형식이다.

1차 해커는 메일을 통해 광고 사이트 임직원 PC를 감염시켜 성인 광고 페이지에 VB스크립트 취약점인 CVE-2018-8174 취약점을 이용한 랜섬웨어를 유포한다. 직원들이 사내 PC로 인터넷 서핑 중 감염된 광고 페이지에 접근하면 해당 취약점을 통해 랜섬웨어가 전파되어 PC가 암호화되고 이를 빌미로 암호화폐를 요구하는 사고가 발생했다.

사토리 봇넷 감염 시나리오



[사토리 봇넷(Satori Botnet) 감염 시나리오]

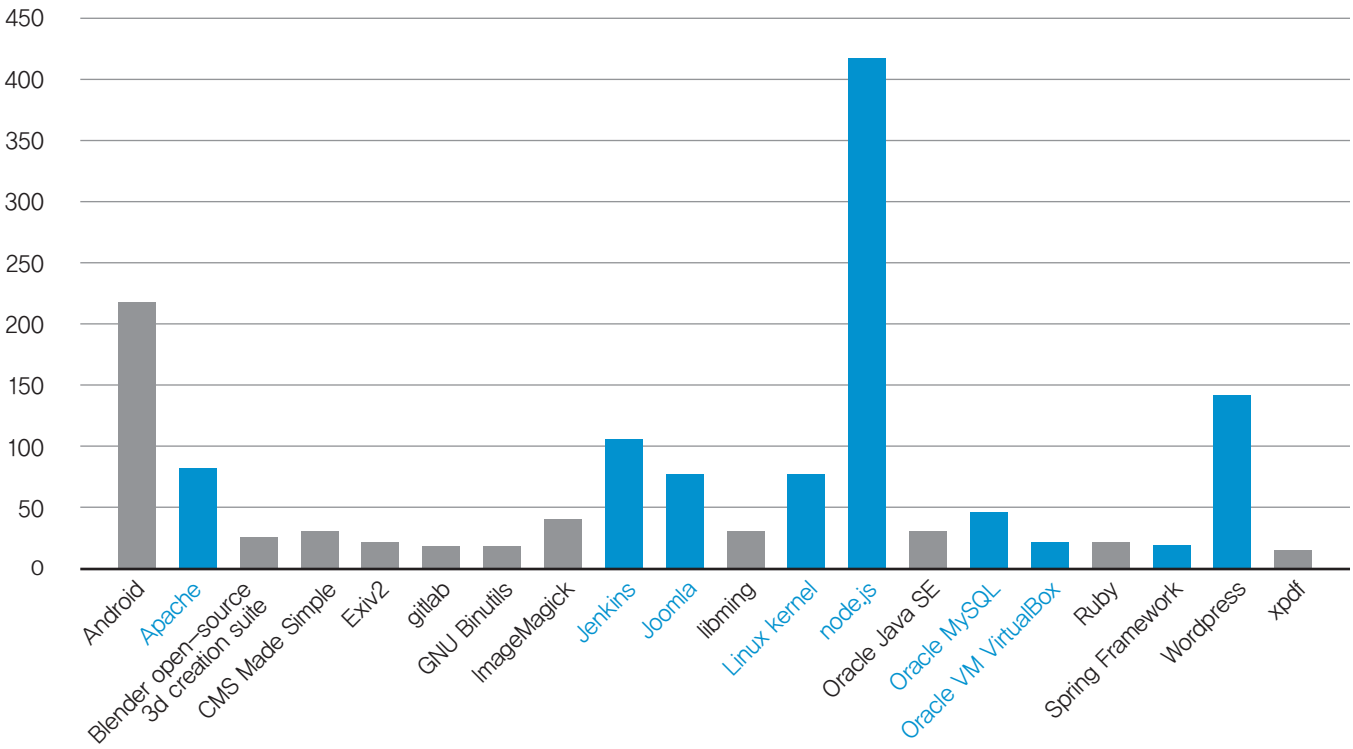
미라이 봇넷(Mirai Botnet)과 유사한 사토리 봇넷이 출현하여 D브랜드 인터넷 공유기 취약점을 통해 악성코드를 감염시키고, 감염된 공유기는 또 다른 기기를 연속적으로 감염시키는 공격이 발생했다. 해커가 제작한 사토리 봇(Satori Bot) 악성코드는 D브랜드 인터넷 공유기(CVE-2018-10088)와 D사 G브랜드 인터넷 공유기(CVE-2018-10561) 취약점을 통해 전파되며, Wget 명령어를 통해 악성 스크립트 프로그램을 다운로드한다. CVE-2018-10088 취약점은 uc-httpd-1.0.0-Buffer Overflow Exploit이며, CVE-2018-10561 취약점은 D사 G브랜드 인터넷 공유기에 대한 인증 우회 취약점이다. 두 취약점 모두 Wget 명령어를 통해 특정 서버에서 악성 스크립트를 다운로드 하여 공유기에 설치하고, 설치된 공유기를 제어하여 암호화폐 채굴 서버 공격 및 디도스(DDoS) 공격 등을 수행한다.

상반기에 발생한 갠드크랩 랜섬웨어나 암호화폐 거래소 공격 등을 보더라도 사이버 공격이 금전적 이득을 노리는 경향이 커지고 있다는 것을 알 수 있다. 또 하나 주목할 점은 남북 정상회담 이후부터 북한으로 추정되는 공격들이 정보 탈취에서 정보 수집 양상으로 변하고 있다는 것이다. 한반도 평화 국면 속에서 서버 정보를 탈취하고 무력화하는 직접적인 공격보다는 기업이나 개인 사용자 PC에서 은밀하게 정보를 수집하는 공격으로 전환되고 있다.

오픈 소스 소프트웨어가 위험하다

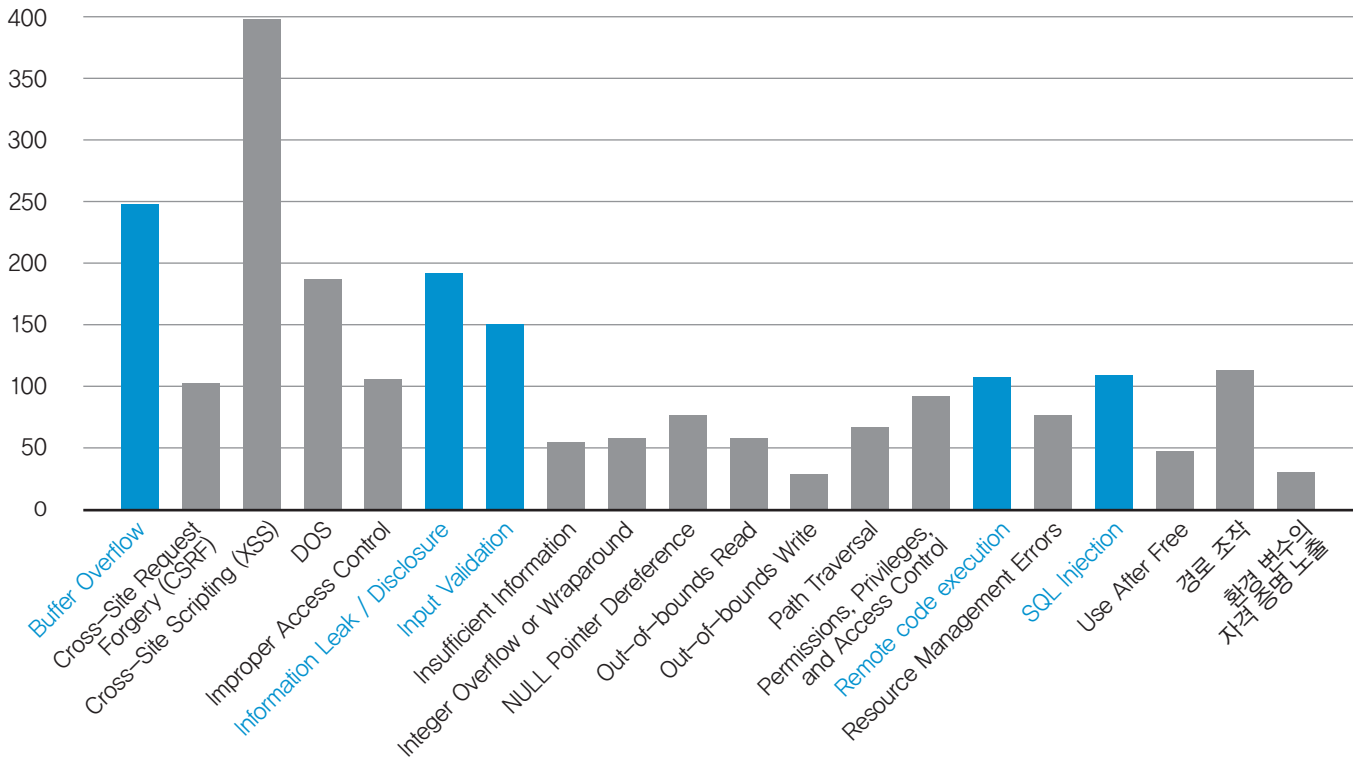
올해 상반기 보안 이슈 중 눈에 띄는 것이 바로 오픈 소스 소프트웨어 취약점이다. 오픈 소스 소프트웨어를 사용하는 기업들이 많아지고 있음에도 불구하고, 기본적인 보안 조치를 하지 않아 생기는 해킹 피해 사례가 늘고 있다. 개발 단계부터 오픈 소스에 대한 보안을 신경 쓰지 않으면 해커에게 공격할 수 있는 문을 열어주는 것과 같다. 상반기 주요 보안 이슈인 오픈 소스 취약점을 가상의 시나리오로 구성한 해킹 시연을 통해 알아보자.

'18년 상반기 오픈 소스 취약점과 유형



[2018년 상반기 오픈 소스 취약점 Top 20]

전체 취약점 중 오픈 소스 관련 취약점이 차지하는 비중이 지속적으로 높아지고 있다. '18년 발표된 취약점은 총 7,341개로, 그 중 3,157개(43%)가 오픈 소스 관련 취약점으로 확인되었다. 취약점이 많이 발표된 오픈 소스는 아파치(Apache) 계열과 CMS(Contents Management System)인 줌라, 웹 서버 백엔드(Back-End)에서 많이 사용되는 노드.js(node.js), 게시판으로 사용되는 워드프레스(Wordpress), 그리고 스프링 프레임워크(Spring Framework)이다.

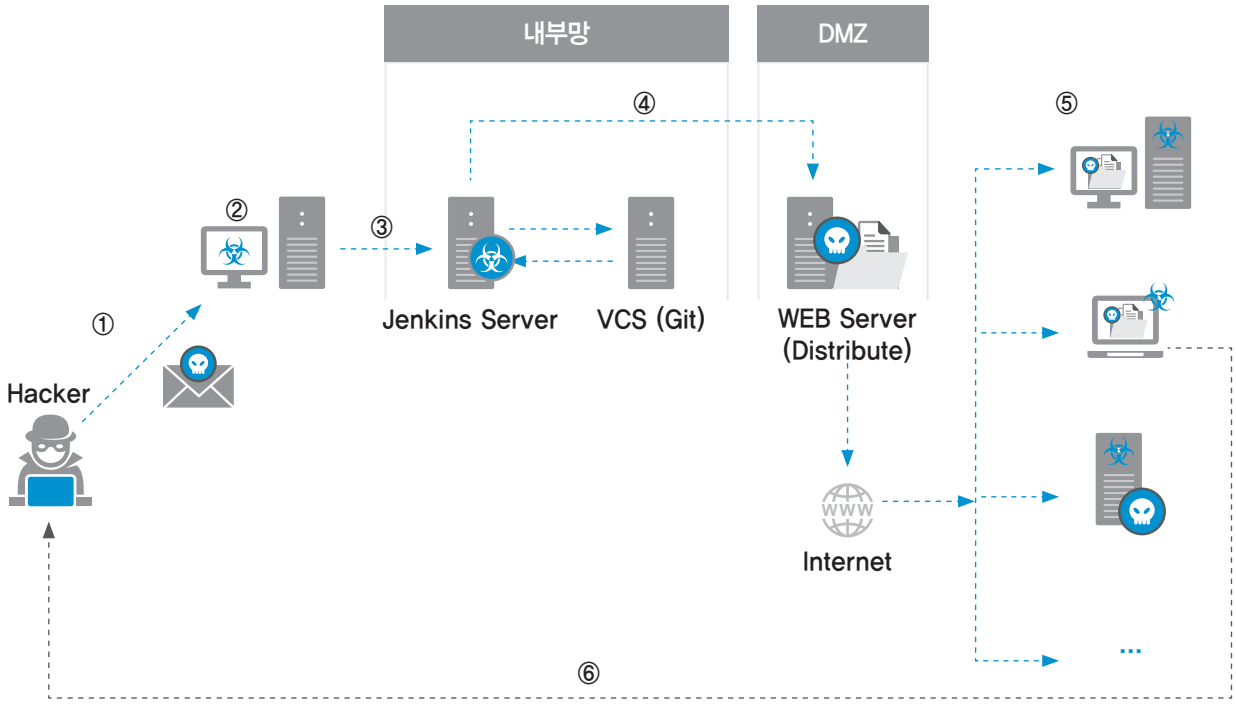


[2018년 상반기 오픈 소스 취약점 유형 Top 20]

'18년 상반기 오픈 소스 취약점 유형 Top 20 중 RCE(Remote Code Execution)와 버퍼 오버플로(Buffer Overflow) 등 위험도가 높은 취약점이 발표되어 오픈 소스에 대한 보안 강화가 필요한 상황이다. 특히 원격에서 공격할 수 있는 RCE와 버퍼 오버플로 취약점을 통한 사고가 지속적으로 발생하고 있으며, 해당 사고로 인해 개인 정보 유출, 디도스 공격 등 치명적인 사고가 발생하는 사례가 있기 때문에 오픈 소스에 대한 보안 설정과 패치 등의 보안에 대한 고려가 필요하다.

오픈 소스 취약점 해킹 시연

오픈 소스 해킹 시나리오로는 젠킨스(Jenkins)와 레디스(Redis) 해킹 방법을 대표로 선정했다. 먼저 젠킨스 오픈 소스의 취약점을 이용한 공격 가상 시나리오이다. 젠킨스는 개발 시 사용하는 CI(Continuous Integration) 도구로, 형상관리 되고 있는 소스코드를 빌드하거나 배포할 때 주로 활용하는 오픈 소스이다.



[젠킨스(Jenkins) 취약점을 이용한 해킹 시나리오]

① 공격자는 VDI와 같은 환경을 통해 내부 개발 시스템에 접근 가능한 사용자에게 개인 메일로 악성 메일을 전송

② 사용자가 해당 파일을 실행하면 공격자는 내부 개발 시스템에 접근 가능한 정보를 탈취

③ 내부 PC를 이용하여 젠킨스 서버를 공격

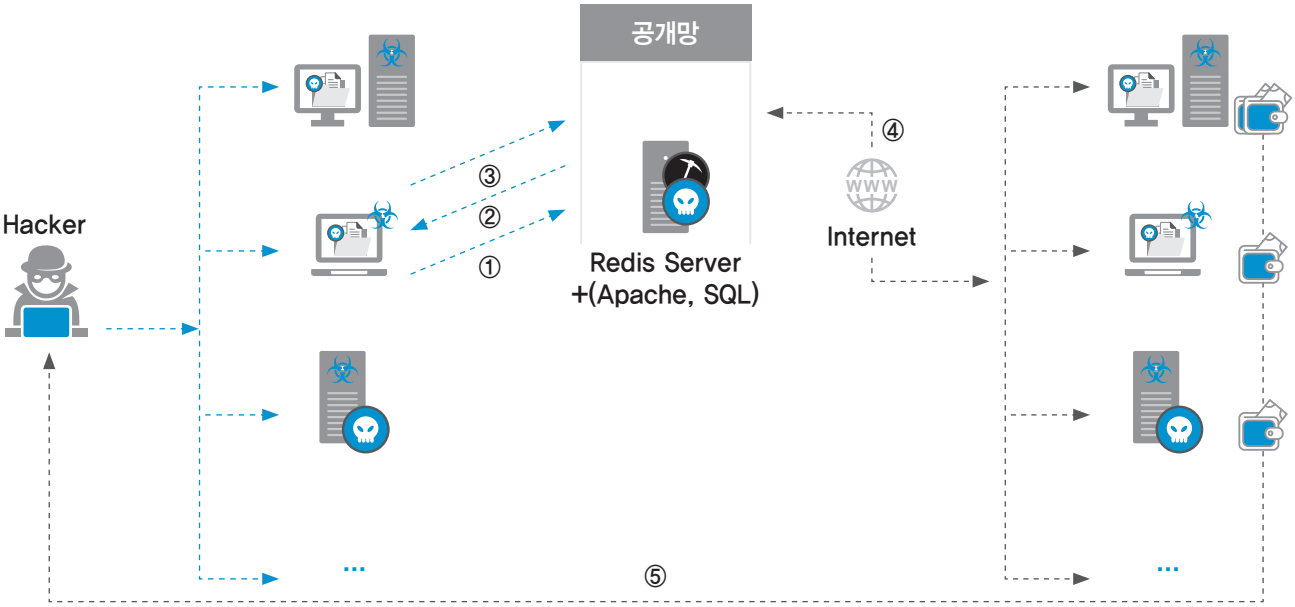
④ 젠킨스 서버 내의 패키징 과정에 사용되는 스크립트를 변조하면 악성 바이너리가 포함된 악의적인 패키지가 생성되어 자동으로 온라인에 게시됨

⑤ 불특정 다수에 해당하는 최종 사용자는 이를 정상 패키지로 생각하여 설치 및 실행

⑥ 감염된 PC의 정보를 수집하고 키로깅 등의 악성 행위를 수행, 데이터를 획득

바로가기: https://youtu.be/Jgf9hIYg6kU

다음은 레디스 오픈 소스의 취약점을 이용한 공격 가상 시나리오이다. 레디스는 Remote Dictionary Server의 약자로서, "키-값" 구조의 비정형 데이터를 저장하고 관리하기 위한 오픈 소스 기반의 비관계형 데이터베이스 관리 시스템(DBMS)이다. (참조 : 위키피디아)

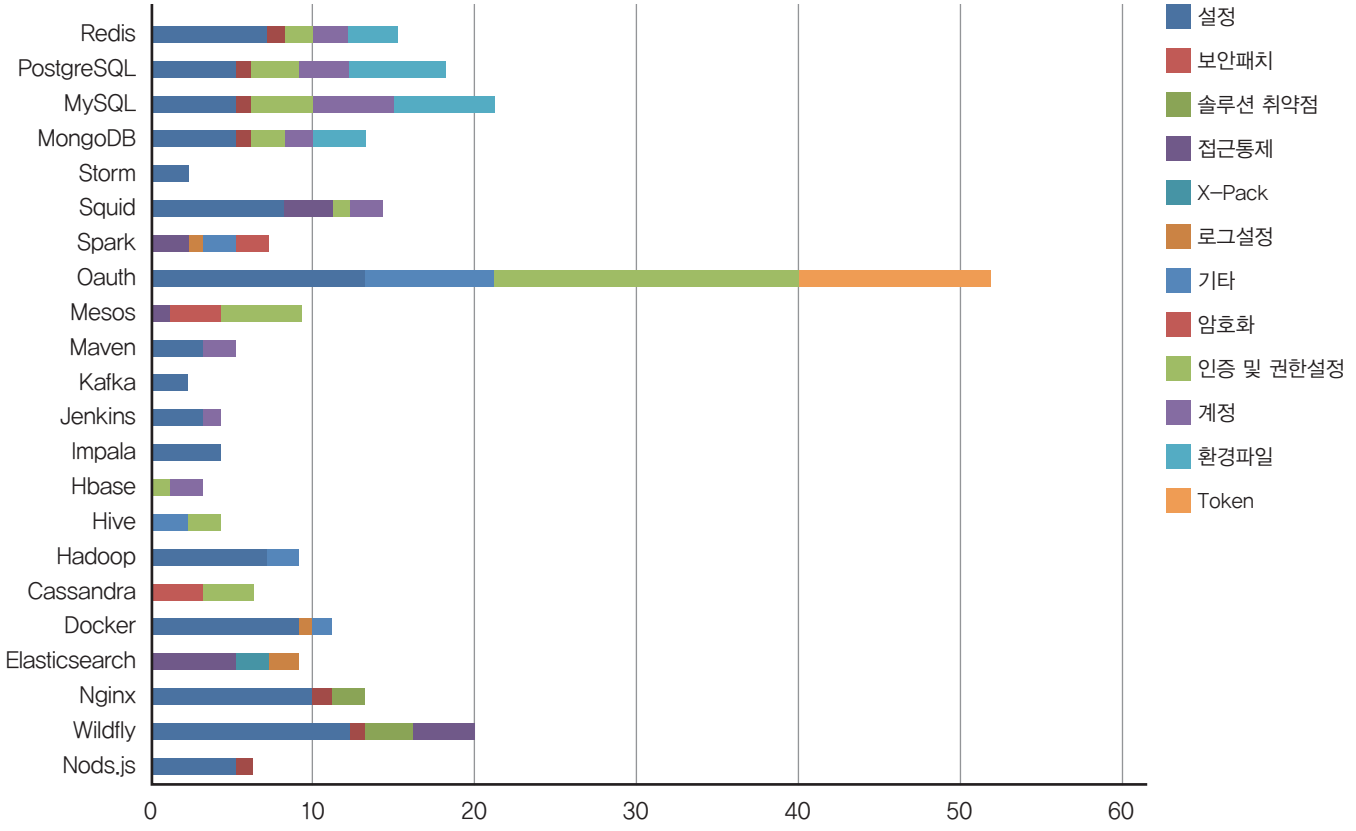


[레디스(Redis) 취약점을 이용한 해킹 시나리오]

① 공격자는 감염시킨 사용자 PC(봇)를 활용하여 포트 스캔 및 취약한 레디스 서버를 확인
② 공격자는 봇을 활용하여 Redis 취약점 공격을 수행하고, 레디스 서버의 원격 쉘을 획득
③ 추가로 서버 내의 서비스를 확인한 후 웹 서비스 내에 악성 코드를 삽입
④ 인터넷을 통해 특정 웹 사이트에 접근한 모든 클라이언트를 활용하여 암호화폐를 채굴
⑤ 공격자는 웹 서버에 접속한 클라이언트 수에 비례한 암호화폐를 획득

바로가기: https://youtu.be/zqGU3NKghnc

오픈 소스 보안 취약점 항목



[오픈 소스 소프트웨어의 보안 항목 유형]

EQST 그룹은 지난 6월 '오픈 소스 소프트웨어 보안 가이드'를 발간했다. 총 22종의 오픈 소스에 대해 12개 유형의 보안 취약점 항목을 도출하고 각 유형별 상세 설정 및 구성 변경에 대해 설명했다.

〈오픈 소스 소프트웨어 보안 가이드 다운로드〉
http://www.skinfosec.com/newsletter_skinfosec/eqstinsight/eqstinsight_201806.pdf

22종의 오픈 소스를 보면 인메모리 데이터베이스(In-Memory DB)인 레디스와 관계형 데이터베이스(R-DB)인 마이SQL(MySQL), 포스트그레SQL(PostgreSQL)이 있고 노에스큐엘 데이터베이스(No-SQL DB)인 몽고디비(MongoDB)의 취약점도 기술되어 있다. 빅데이터 관련 오픈 소스인 스톰(Storm), 스파크(Spark), 하둡(Hadoop), 카프카(Kafka), 에이치베이스(HBase), 카산드라(Cassandra)에 대한 취약점과 검색엔진인 엘라스틱서치(Elastic-search)의 보안 취약점에 대한 내용도 담았다. 빅데이터 내의 질의어인 하이브(Hive)와 임팔라(Impala), 관리 툴인 메소스(Mesos), 컨테이너 기반 가상화 툴인 도커(Docker), 웹 어플리케이션인 엔진X(NginX)와 와일드플라이(Wildfly) 등 다양한 오픈 소스 영역의 취약점에 대해 연구하였으며, 그것에 대한 상세 설정을 설명하고 있다.

와일드플라이 및 엔진X의 경우, 관리서버 홈디렉토리에 일반 사용자가 접근할 수 없도록 하는 권한 관리가 필요하다. 이는 일반 사용자가 웹 서버의 설정 파일을 삭제하거나 변경할 경우, 시스템이 오작동하여 사용 불능 상태에 빠

질 우려가 있기 때문이다. 또한, 디렉토리 검색 기능이 활성화되어 있으면 해당 디렉토리에 존재하는 모든 파일 리스트를 보여주어 웹 어플리케이션 서버(WAS) 구조 노출 및 주요 설정 파일의 내용이 유출될 가능성이 있기 때문에 디렉토리에 대한 검색 기능을 비활성화 시켜야 한다.

엘라스틱서치의 경우, 본 엔진에서 제공하는 X-Pack에 인증 및 접근 통제에 대한 모니터링 기능을 적용하여 보안을 강화해야 한다.

도커는 컨테이너 기반의 가상화 오픈 소스이므로 시스템 자원 고갈을 통한 DoS(Denial of Service) 공격을 방지하기 위해 특정 명령을 줄 인수를 사용하여 많은 리소스 제한을 적용해야 한다. 신뢰할 수 있는 인증서 설정을 통하여 안전한 통신을 보장해야 한다. 신뢰할 수 있는 컨텐츠 설정이 되어있지 않은 경우 비인가자의 악성 컨테이너가 배포될 우려가 있으므로 신뢰할 수 있는 컨테이너 설정을 하여야 한다. 컨테이너를 루트 외 사용자로 지정하여 각 컨테이너 별 권한 설정을 해야 한다.

카산드라는 노드 간(Node to Node), Client to Node SSL 암호화 통신, 인증 설정이 필요하다.

하둡은 LDAP/케브로스(Kerberos) 보안 인증과 데이터 암호화, 하둡분산파일시스템 액세스 제어 목록(HDFS ACL) 설정을 통해 평문 통신으로 인한 정보 유출 방지 및 접근 통제를 통한 부정 액세스를 차단해야 한다.

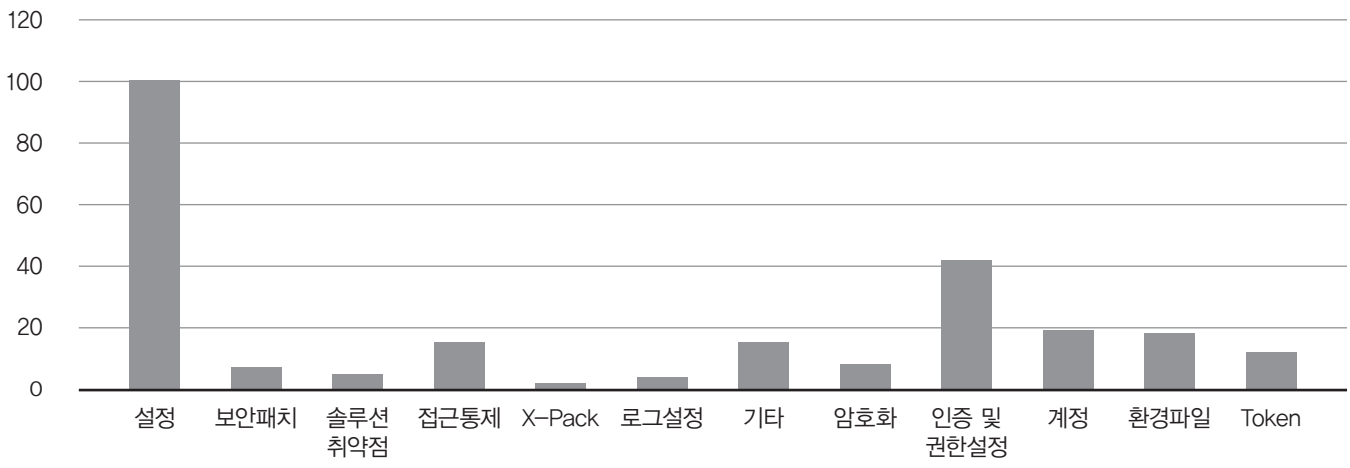
하이브, 임팔라 같은 데이터 질의어는 사용자 권한 통제를 바탕으로 데이터 질의에 대한 통제가 필요하며, CI 툴인 젠킨스에 대한 접근 통제가 중요하다.

카프카의 SSL 통신과 메이븐(Maven)의 일반 사용자 접근 설정 권한이 필요하고, 메소스(Mesos)는 인증 및 SSL이 중요한 항목이다.

오쓰(Oauth)는 인터넷 사용자들이 비밀번호를 제공하지 않고 다른 웹 사이트상의 자신의 정보에 대해 웹사이트나 애플이케이션의 접근 권한을 부여하는 소프트웨어이기 때문에 자격증명 관리가 매우 중요하다.

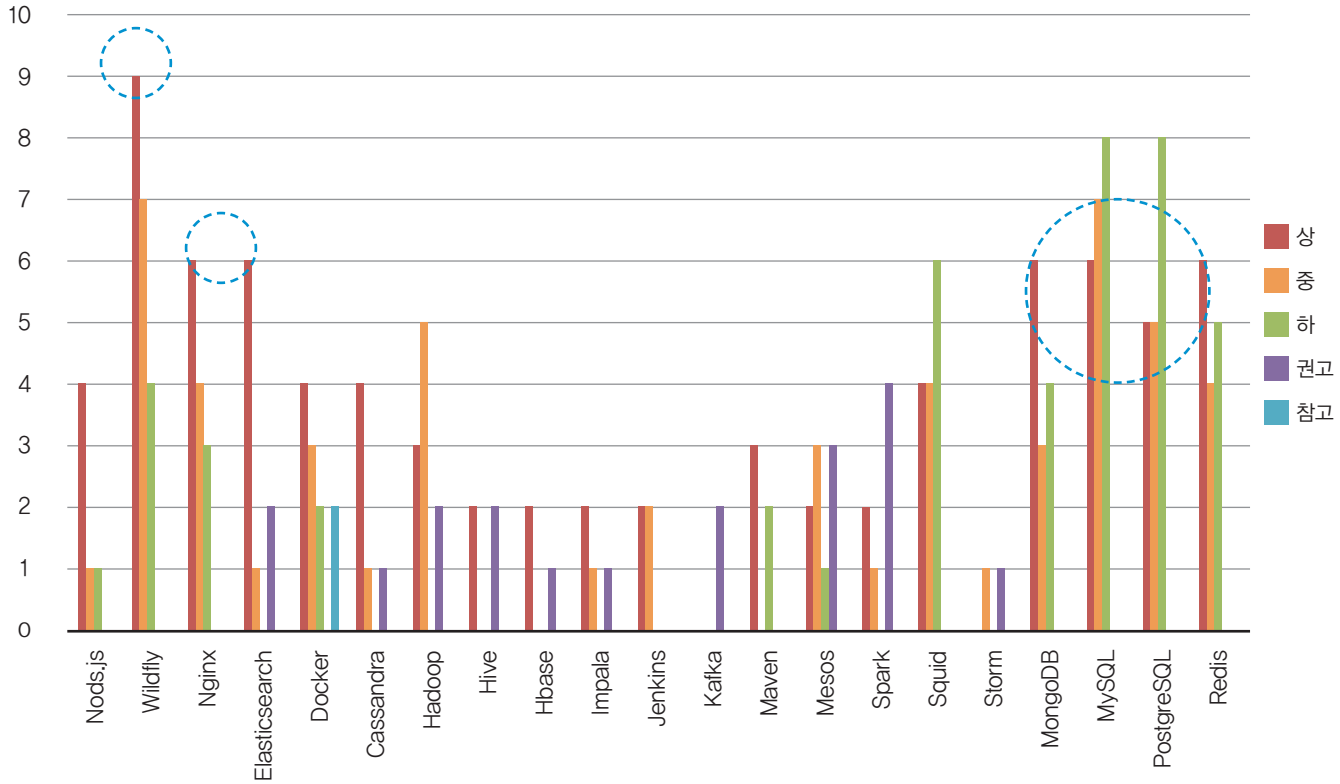
SSL 프록시(Proxy)인 스퀴드(Squid)의 경우 사용자 별로 권한을 구분하여, 주어진 권한 이외의 행동을 통제하거나 사용자 인증 설정을 설정하여 비인가 접근을 통제해야 한다.

실시간 데이터 처리 엔진인 스톰의 경우 데이터 통신에 대한 SSL암호화가 필요하며, 데이터베이스 계열 오픈 소스인 레디스, 몽고디비, 마이SQL, 포스트그레SQL인 루트 눌(Root Null) 암호 및 테이블 접근 제한 설정, 루트(Root) 권한 실행을 통제하여 기본 취약점 및 비인가 접근에 대한 통제가 필요하다.



[오픈 소스 보안 항목]

오픈 소스 보안 항목 중에는 일반 설정이 가장 많은 취약 항목을 포함하고 있으며, 인증 및 권한 설정과 계정, 접근 통제가 취약한 영역으로 확인되었다. 대부분의 해킹 사고는 디폴트 세팅이나 허술한 접근 통제, 인증 및 권한 미설정, 또는 디폴트 계정에 대한 설정 변경을 하지 않아 발생한다. 이러한 취약점을 관리하고 통제해야만 오픈 소스로 인한 해킹 사고를 방지할 수 있다.



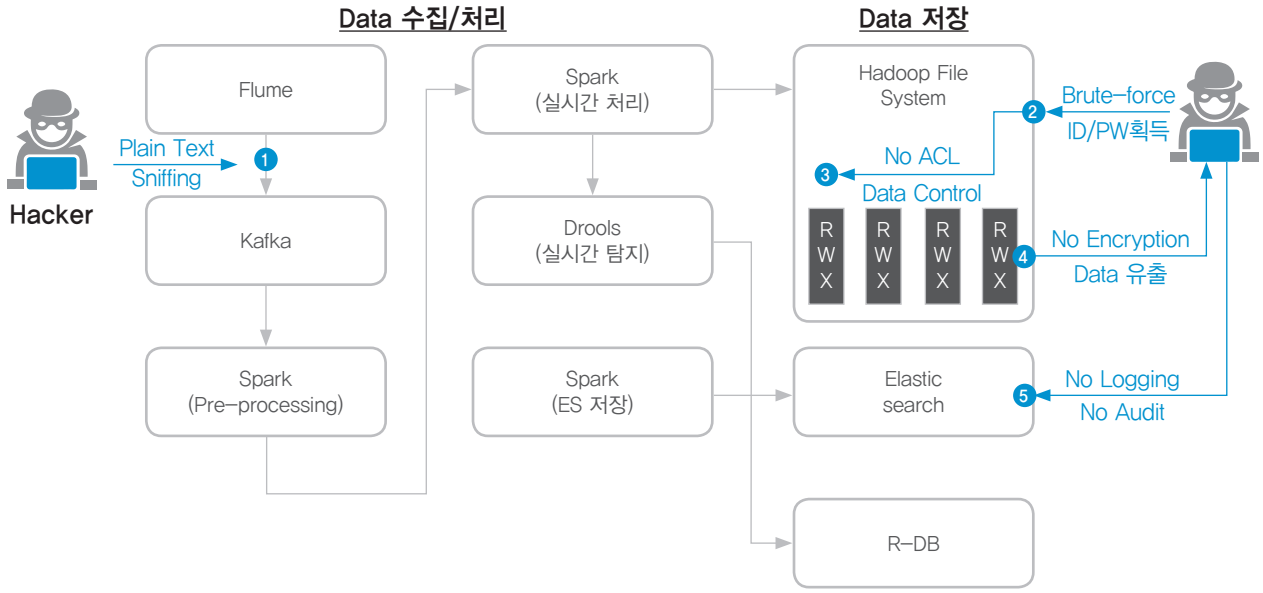
[위험도 별 항목]

위험도 별 항목을 보면 권한 통제, 로깅 설정, 계정 및 암호 관리, 암호화 통신, 보안 패치의 위험도가 높으며(상), 사용빈도가 높은 웹과 데이터베이스가 다른 오픈 소스에 비해 취약한 항목을 많이 보유하고 있는 것으로 확인되었다. 최근 해킹 사례도 이런 위험도가 높은 취약점으로 인해 발생하는 경우가 많았다.

위험도 '상' 항목 내용

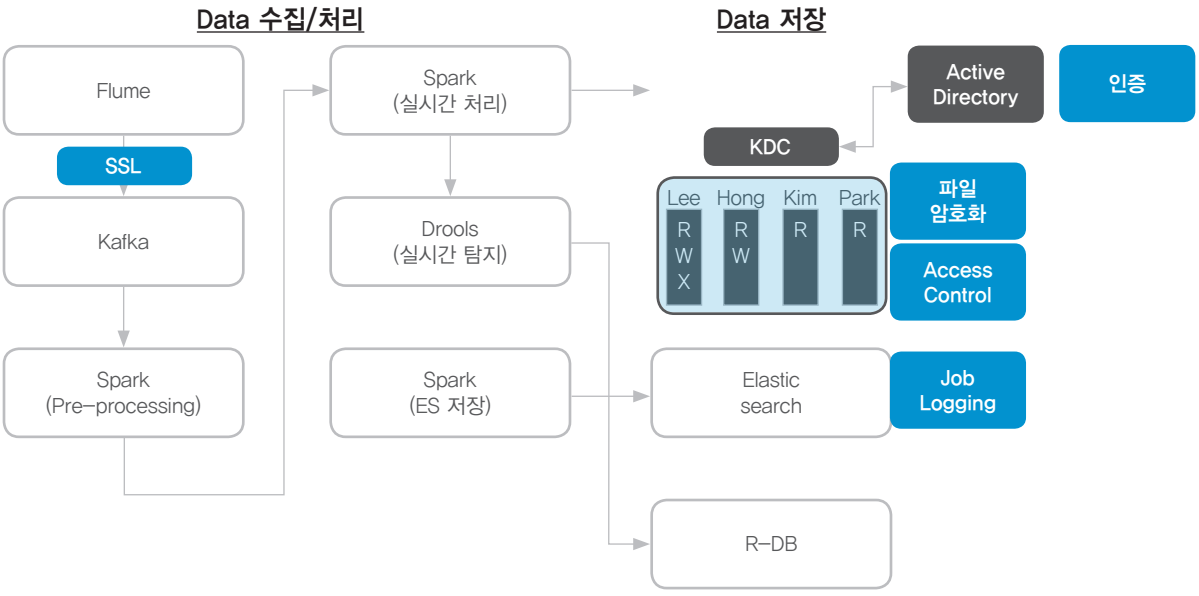
권한 통제	인증 및 계정에 대한 권한 통제 실행 권한 통제
로깅 설정	User 행위 및 작업 History
계정 및 암호 관리	Default 계정 및 Null Password
암호화 통신	암호화 통신 및 Data 암호화
보안패치	취약 Version 패치 필요

빅데이터 관련 오픈 소스 보안 방안



[빅데이터 오픈 소스 보안 취약점]

빅데이터의 경우 한가지 오픈 소스만을 사용하는 것이 아니라 여러 오픈 소스를 사용하는데, 데이터 수집 시 사용하는 플룸(Flume), 메시지 큐(Message Queue)로 사용하는 카프카, 실시간 처리 엔진인 스파크, CEP 엔진인 드룰(Drools), 데이터 저장소로 사용하는 하둡, 검색 엔진인 엘라스틱서치로 구성된다. 이렇게 구성하는 경우, 평문 통신 시에는 데이터 스니핑(Data Sniffing)에 의해 중요 정보가 노출될 가능성이 있고, 접근 통제 미적용 시에는 브루트포스(Brute-Force) 공격에 의해 아이디와 비밀번호가 탈취 될 가능성이 있다. 하둡 같은 경우 데이터 복제 때문에 같은 계정을 전체 노드에 사용하므로 접근 통제가 매우 중요하다. 데이터 미암호화 시 데이터 유출을 대응하기 어려우며, 작업에 대한 로깅 미설정 시에는 추적 관리가 어렵다.



[빅데이터 오픈 소스 보안 적용]

빅데이터 관련 오픈 소스 보안을 적용하기 위해서는 데이터 흐름 전 구간에 SSL을 적용해야 하며, 데이터 저장소와 각 구성 요소(Component)에 커베로스(Kerberos) 및 LDAP(Lightweight Directory Access Protocol)로 인증을 통합하여 적용해야 한다. 또한, 파일에 대한 사용자별 액세스 제어를 적용하여 사용자 권한을 통제해야 한다. 데이터 유출에 대한 대응을 위해서는 파일 암호화가 필요하나, 파일 암호화는 성능 저하가 매우 심하기 때문에 적용에 많은 검토가 필요하다. 그리고 모든 작업에 대한 로깅 및 로그 저장을 통해 비인가 접근에 대한 모니터링 체계를 구축해야 한다.

젠킨스와 레디스의 취약점 해킹 시연을 필두로 22종의 오픈 소스 소프트웨어의 보안 항목과 취약점 등을 살펴보았다. 오픈 소스는 어떻게 사용하는가에 따라 해당 기업에 큰 도움이 될 수 있다. 하지만 보안 적용이 되어있지 않은 상태로 사용하면 해킹 사고로 인한 어려움에 처할 수도 있다. EQST 그룹이 발간한 '오픈 소스 소프트웨어 보안 가이드'가 기업의 올바른 오픈 소스 사용에 도움이 되기를 바란다.

EQST INSIGHT

2018.07

SK infosec
경기도 성남시 분당구 판교동 255번길 46 4층
www.skinfosec.com

발행인 : SK인포섹 EQST Group
제　작 : SK인포섹 Communication팀