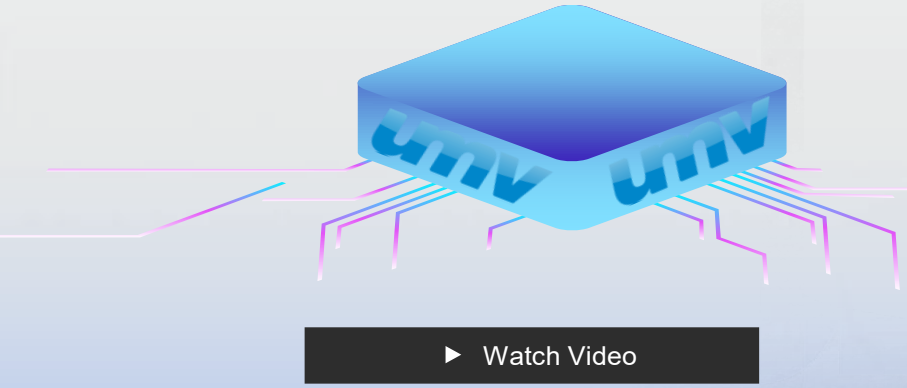
웹 서버 & Cloud VM 통합 보안을 위한

WSS (Web Server Safeguard)

실시간 탐지 및 격리를 통한
완벽한 웹서비스 보안



▶ Watch Video

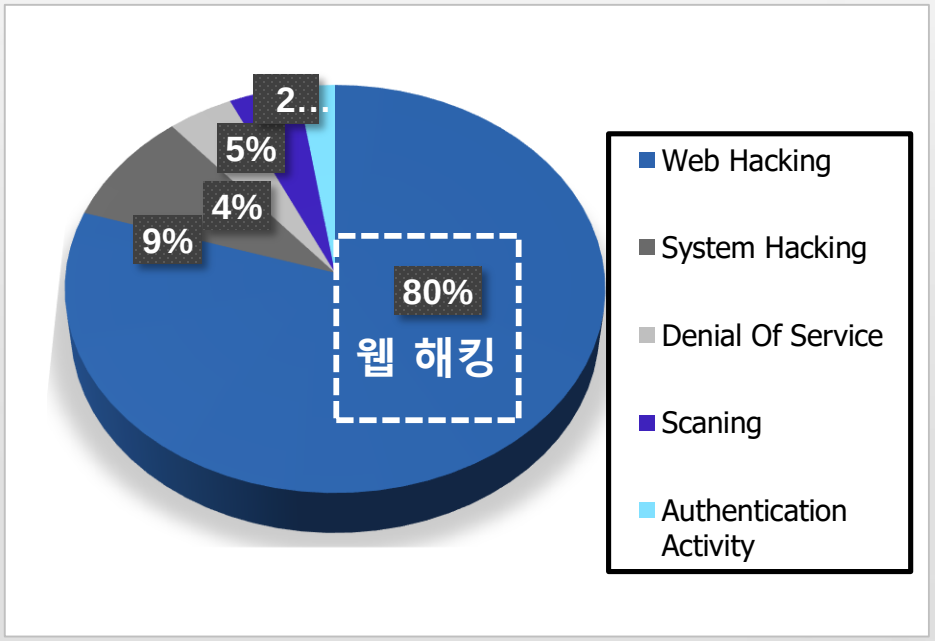
목차

1. 웹 보안 개요 및 필요성

전 세계적으로 Cyber 공격은 80%이상이 웹서비스 서버를 통하여 진행되고 있으며 그에 따른 웹서비스 보안의 중요성이 날로 커지고 있습니다. 2020년 8월부터 2021년 1월까지 매월 평균 140,000건의 웹쉘을 이용한 공격 발생 횟수를 기록했으며, 해마다 두배 이상 증가하고 있습니다

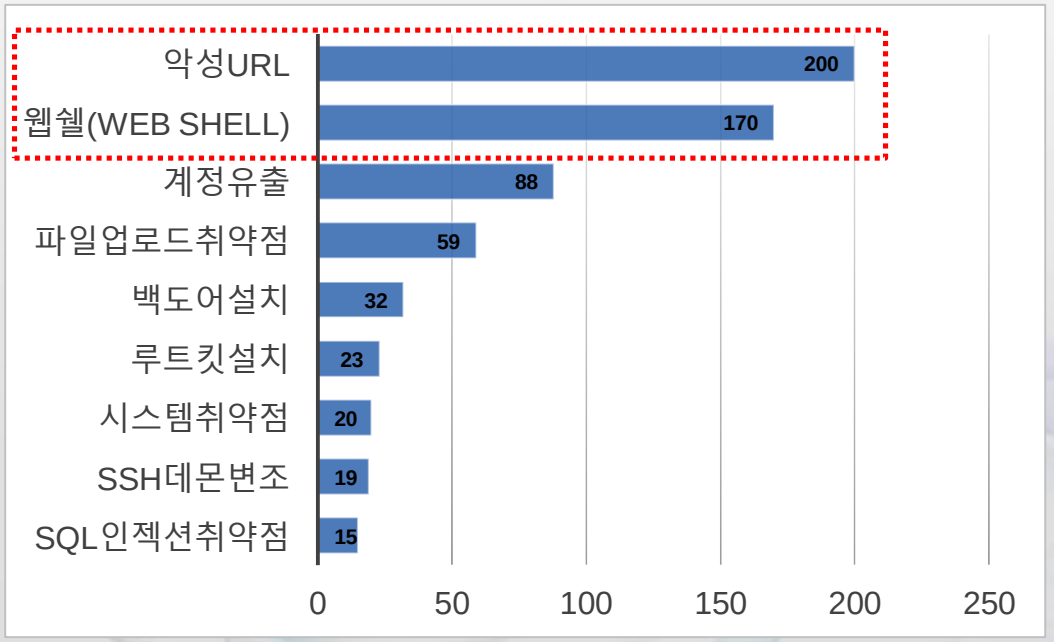
[출처: Webshell attacks continue to rise , Microsoft security Blog]

CYBER ATTACKS



[출처: KISA 보안관제 동향]

WEB ATTACKS



[출처: KISA 인터넷 침해 대응센터 / 침해사고Trend]

WebShell 공격 피해 사례

트리고나 랜섬웨어, 부적절하게 관리되는 MS-SQL 서버 통해 유포

2023-04-12 10:21

윈도 서버뿐만 아니라 데스크톱 환경에도 설치...Remcos RAT 등 악성코드 탐지. **CLR Shell 악성코드 설치 이후 관리자 권한 취득하여 트리고나 랜섬웨어 설치하여 감염.** 트리고나 바이너리를 Run 키에 등록해 재부팅 이후에도 실행될 수 있도록 하며, 이후 볼륨 쉐도 삭제 및 시스템 복원 기능을 비활성화해 랜섬웨어 감염 이후 복구를 불가능하게 한다.

▲공격에 사용된 CLR Shell 악성코드[자료=안랩 ASEC 분석팀]

중국 해커조직 샤오치잉, 해킹한 학회 3곳 개인정보 DB 다크웹에 공개

2023-01-29 14:27

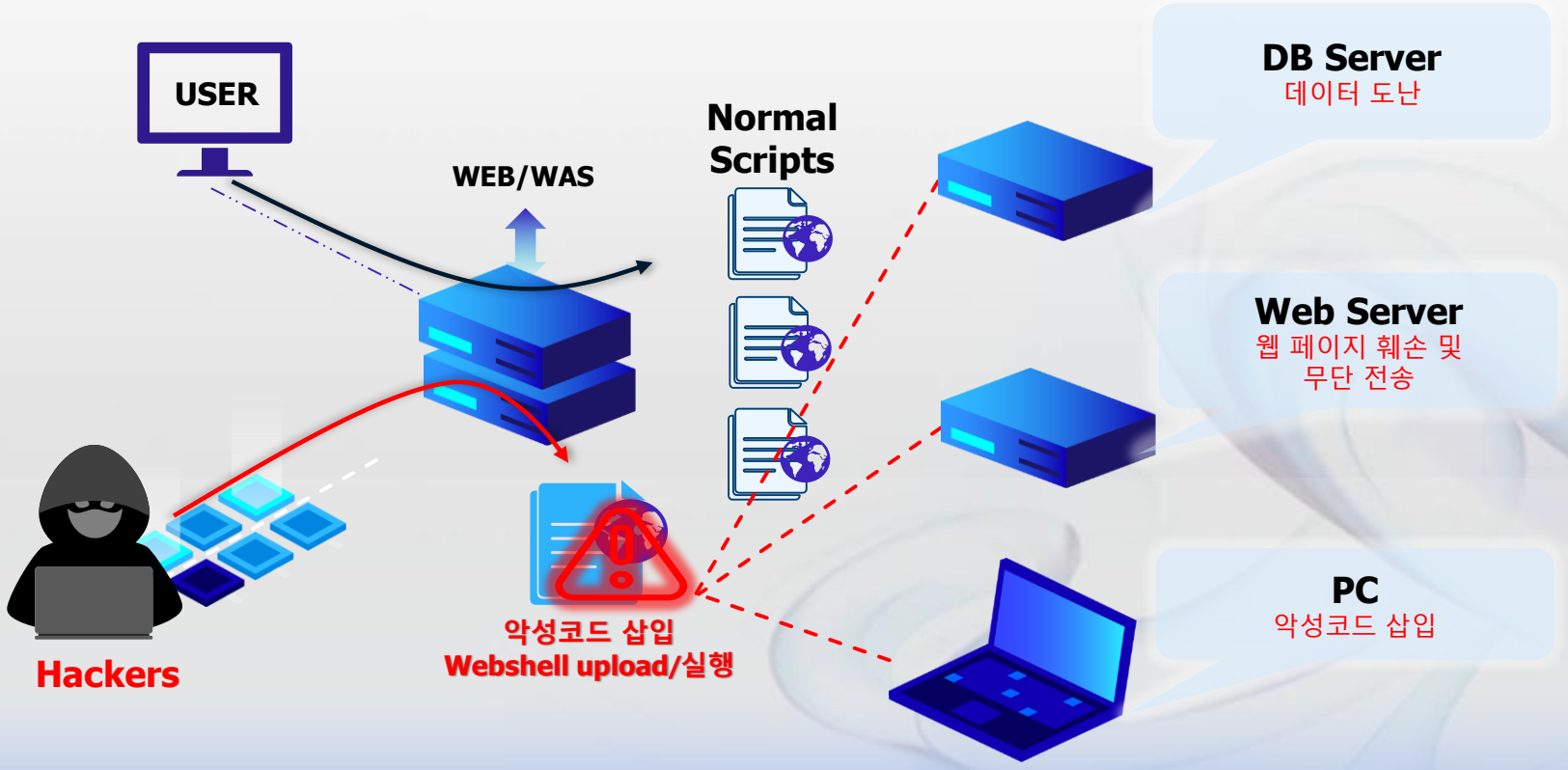
다크웹 포럼에 한국고고학회, 한국교육원리학회, 한국학부모학회 3곳 내부 DB 공개 회원정보로 보이는 휴대전화번호와 주소 등 개인정보 포함...과거 유출 정보 가능성도 있어
웹을 통해 SQL 명령어를 전달했고 데이터베이스에 저장돼 있는 웹 관리자 계정 정보를 탈취한 것이다. (웹쉘 삽입)
샤오치잉은 해킹을 통해 기업 내부 정보를 탈취하거나 삭제했다.
또 웹 사이트를 자신들이 만든 웹 페이지로 변조하거나 무단 생성하기도 했다.

◀ 샤오치잉이 해킹한 웹 사이트에 업로드한 웹 페이지 유형/사진제공=한국인터넷진흥원

1. 웹 보안 개요 및 필요성

웹 기반의 “악성코드(Malware)” 또는 “웹쉘(WebShell)”이란?

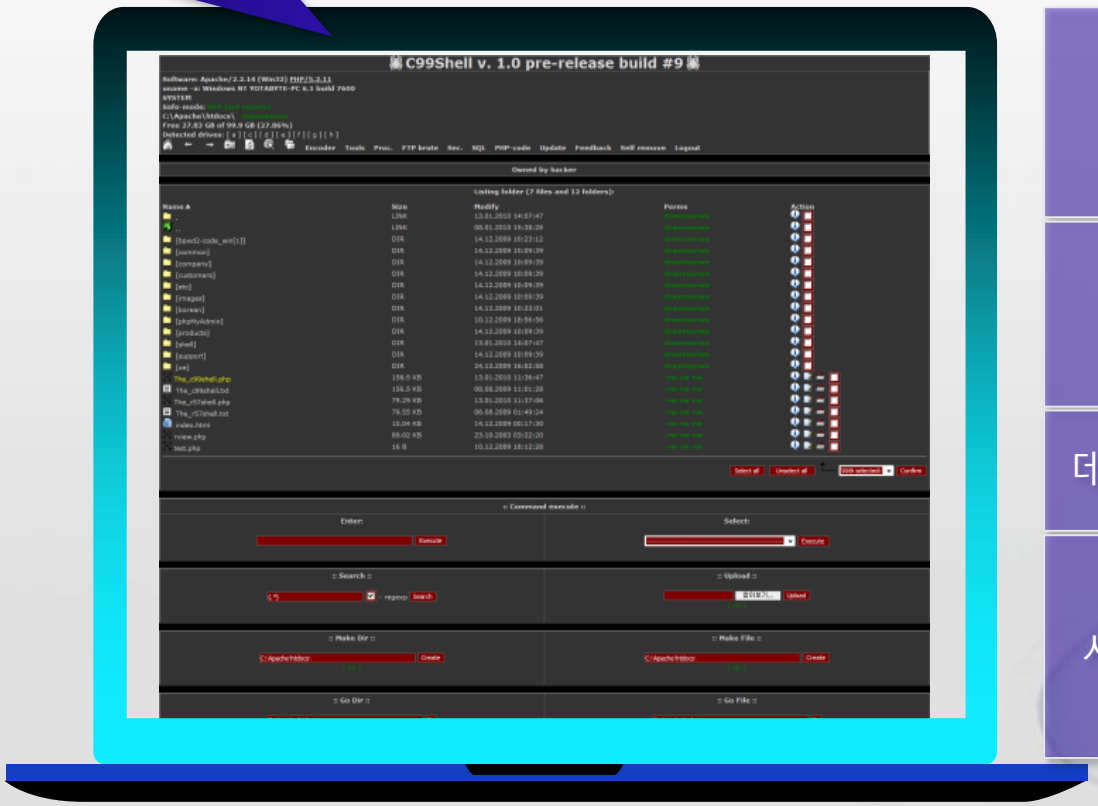
- 웹 서버의 취약점을 이용하여 삽입된 명령어 프로그램이며, 서버 사이드 스크립트(**ASP, JSP, PHP, CGI, PYTHON**) 등으로 제작되어 실행되면 **Root** 권한에 준하는 서버 제어가 가능합니다
- 웹 서비스를 위한 웹 서비스 포트(**http**(80, 8080), **https**(443))는 백도어 역할을 하여 기밀 데이터 도용, 웹 페이지 손상 및 무단 페이지로의 액세스 전달 및 악성코드 확산과 같은 심각한 해킹 공격을 당합니다



웹 기반 악성코드 / "웹쉘(Webshell)"

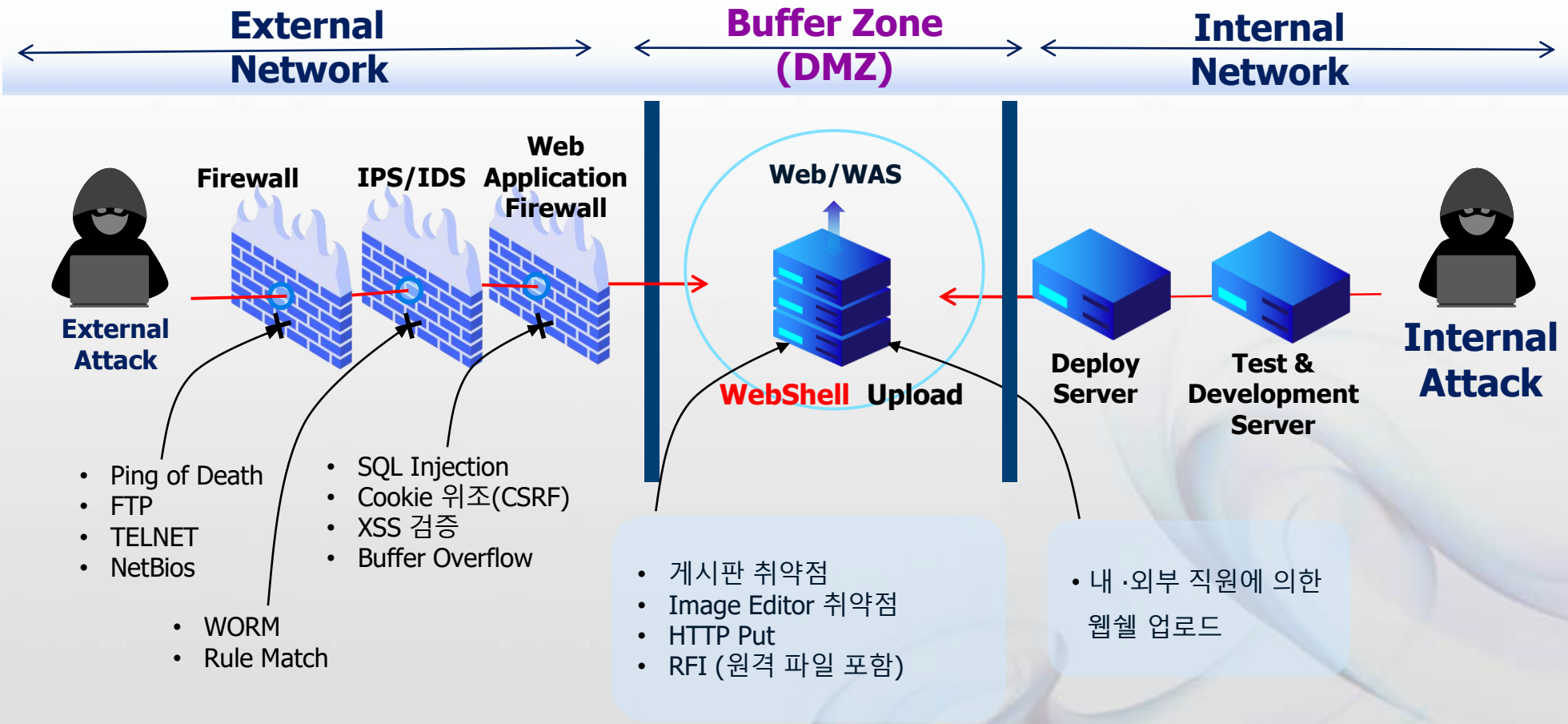
- 웹쉘은 보안 시스템을 피하여 별도의 인증없이 기존 시스템에 쉽게 접속 가능하게 합니다.
- 웹쉘은 해킹 사고가 터지지 않는 이상 인지하기가 어려워 치명적으로 위험합니다.

[Captured C99 WebShell screenshot]

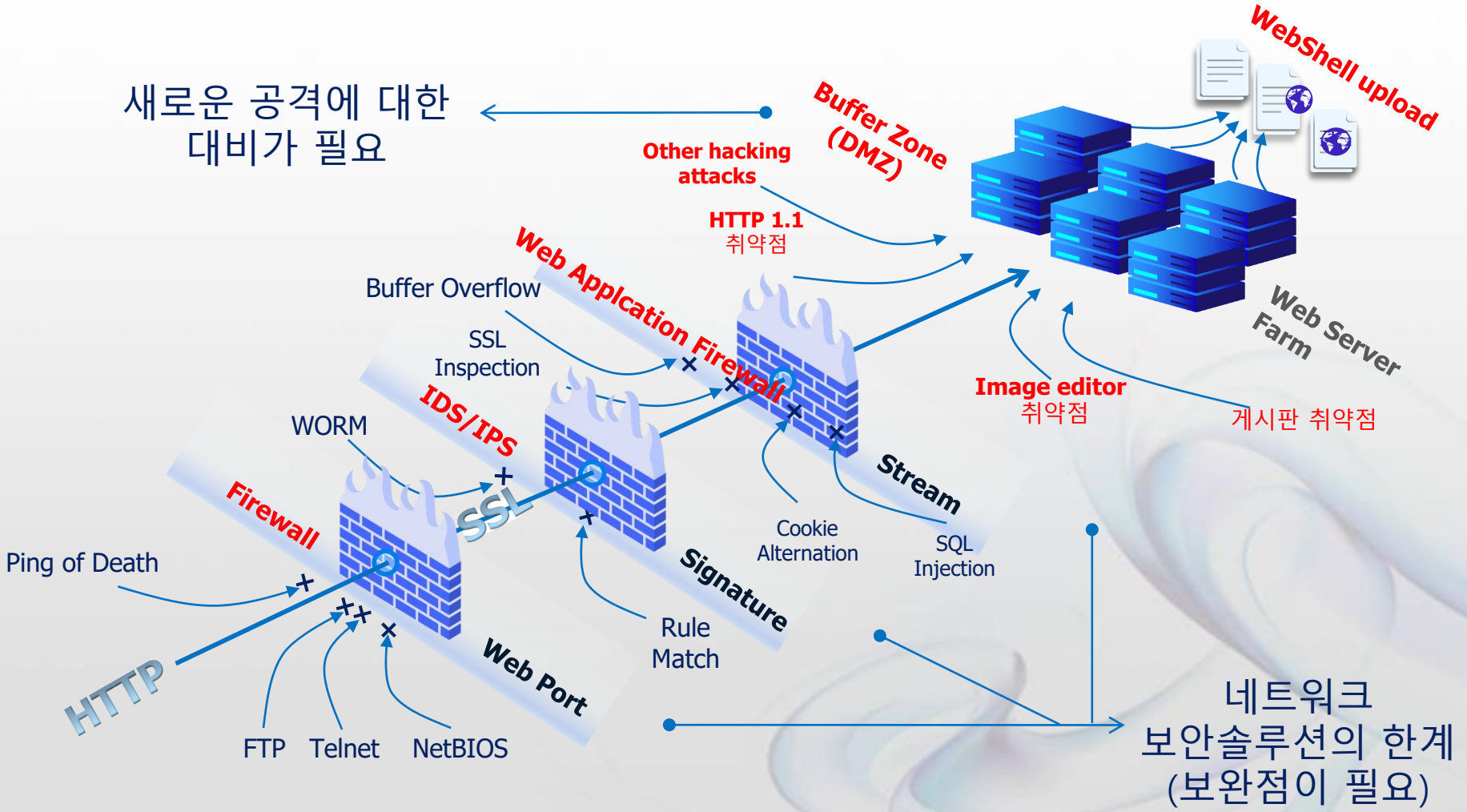


시스템 명령어	- 시스템 정보 열람 - 시스템 Shutdown - 특정 프로그램 정지/제거 (예: Anti-Virus 프로그램)
네트워크	- 포트 스캐너 - TELNET, SSH, FTP - 접속 (내부 네트워크 접근 가능)
데이터베이스	- 데이터 유출, 변경, 삭제
시스템 파일	- 해킹 툴 업로드(키로그, 백도어) - 파일 수정(악성코드 삽입) - 시스템 파일 삭제 - 모든 시스템 디렉토리 열람

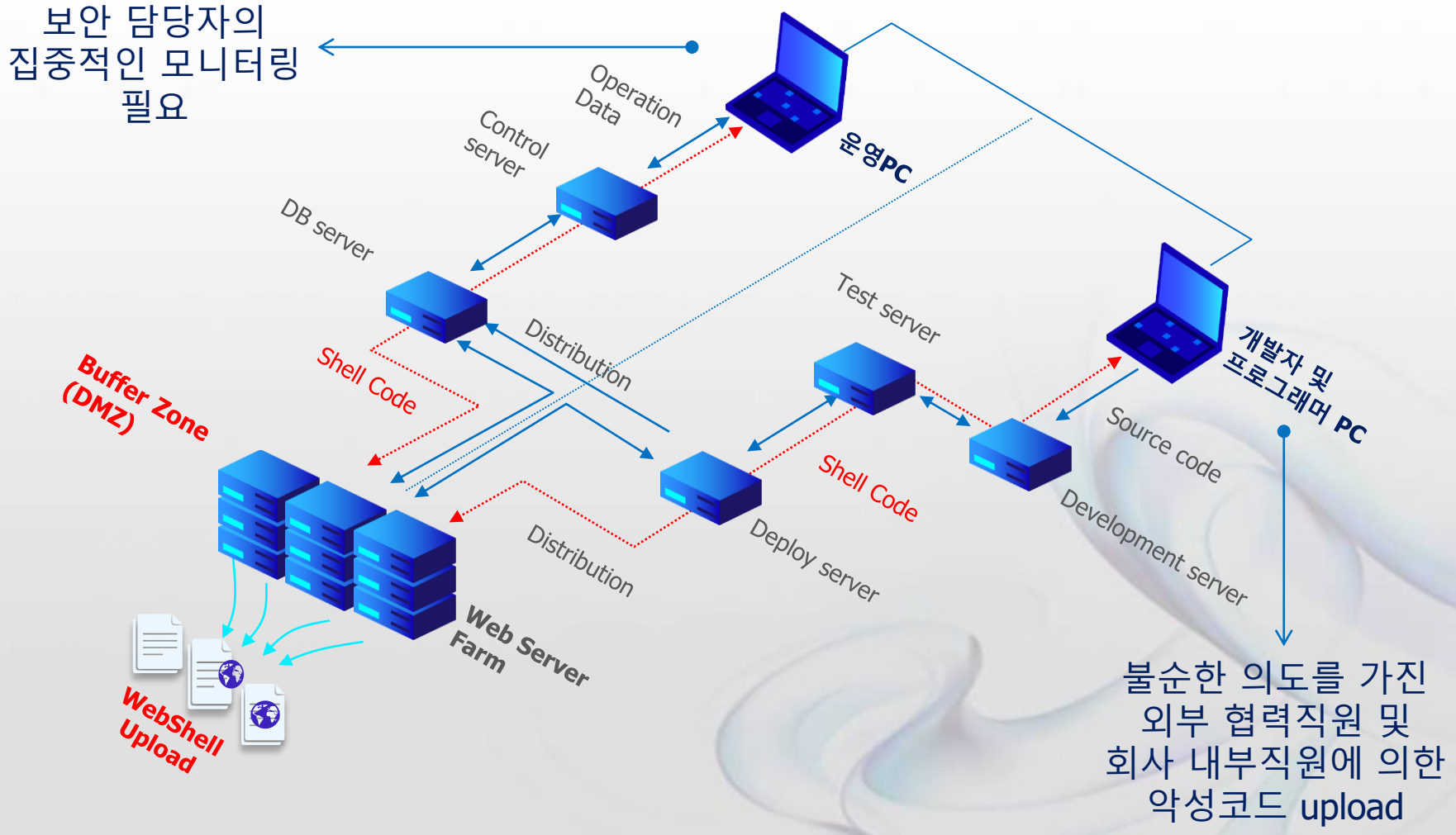
악성 코드(WebShell)의 침입경로



External Network으로 부터 침입



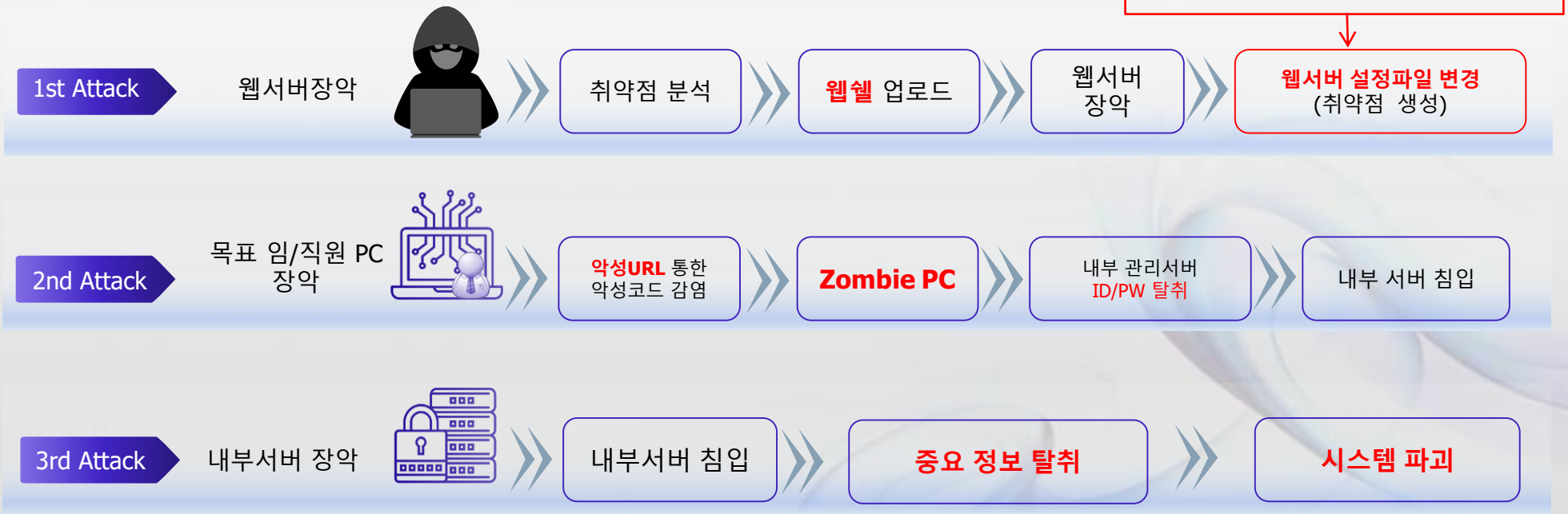
Internal Network 부터의 침입



웹 해킹 Process

최근 웹 해킹은 웹쉘을 기반으로 하여 복합적이고 지속적으로 (APT Attack) 시도되며,
정확한 공격 목표를 세워 단계적으로 진행됩니다.

- 악성코드 URL 삽입 공격
- 홈페이지 Deface 공격
- 소스코드 및 콘텐츠 위변조 공격



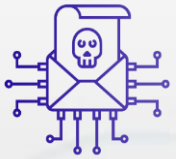
웹 공격 유형

내부 및 외부협력업체 직원에 의한
잠재 위험 요소

네트워크 보안 솔루션
취약점을 이용한 공격

- 네트워크 보안장비
  취약점(패킷 단위로 분석)
- 백신 컴파일된 Binary 기반
  악성코드 공격

Web Hacking



게시판 업로드 공격
소스코드 취약점을 이용한 업로드 공격

- 확장자 변조 취약점
- 이미지 파일을 위장한 공격

Web서버/WAS OS
Zero Day 취약점 공격

웹 공격의 종류

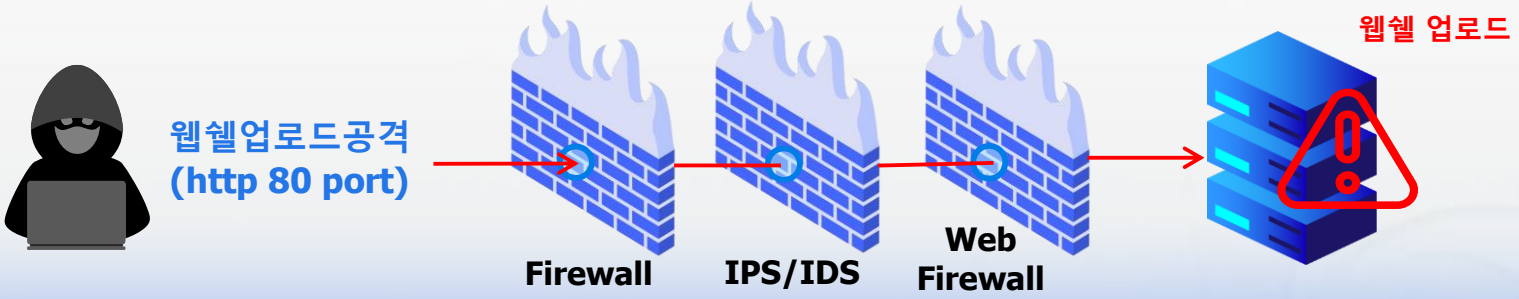
웹 기반 주요 공격은 웹 소스코드 취약점을 이용하여 소스코드 및 데이터 변조로 이어지며,

이를 통하여 웹쉘, 악성URL, 홈페이지 위변조, 웹서버 설정파일 변조 등의 공격형태로 나타납니다.

웹 공격의 종류

웹쉘 Upload 공격

웹서버에 업로드 되어 실행되면 **Root** 권한에 준하는 서버 제어가 가능합니다

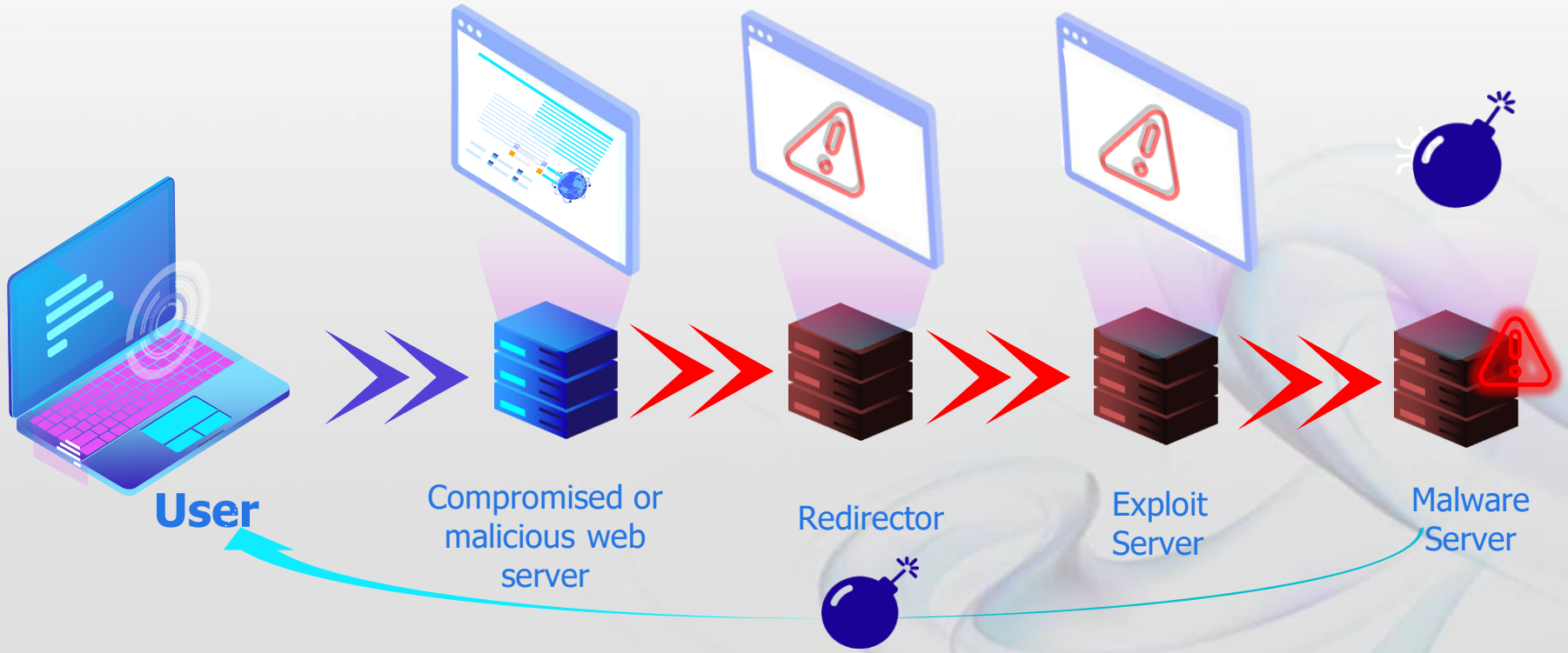


시스템 명령어	네트워크 명령어	시스템 파일 접근	DB접근	사용자 PC
• 시스템 정보열람 • 시스템 shutdown • 특정프로그램 정지/삭제 (Anti-virus software등)	• Port scanner • TELNET, SSH, FTP 접속 (내부네트워크 접근 가능)	• 해킹툴 업로드(키로그, 백도어) • 파일 수정(악성코드삽입) • 시스템 파일 삭제 • 시스템 디렉토리 열람	• 데이터 유출 • 데이터 변경 • 데이터 삭제	• 악성코드 감염 • 데이터 유출 • 관리자의 주요 시스템 접속정보 유출 • DDoS 공격 유발

웹 공격의 종류

악성 URL 삽입공격

악성URL은 웹 서버를 악성 코드의 경유지로 이용하여 바이러스, 랜섬웨어 등을 PC에 대량으로 유포하는 URL 또는 IP주소이며 파일 암호화, 개인정보유출, DDoS 공격등의 심각한 피해를 입힐 수 있습니다



출처 : MS Security intelligence report

웹 공격의 종류

웹서버 설정 파일 변조 공격

해커는 웹 서버 **Configuration** 파일을 변조하여 새로운 취약점을 생성 및 **2**차 공격 경로로 활용합니다

목차

Why WSS (Web Server Safeguard)?

WSS는 웹서버 해킹에 악용되는 악성 프로그램인 '웹쉘'을 실시간 모니터링 조치하여 웹서버의 안전한 운영을 보장하는 웹쉘 전용 보안 솔루션 입니다

웹쉘 탐지 및 조치

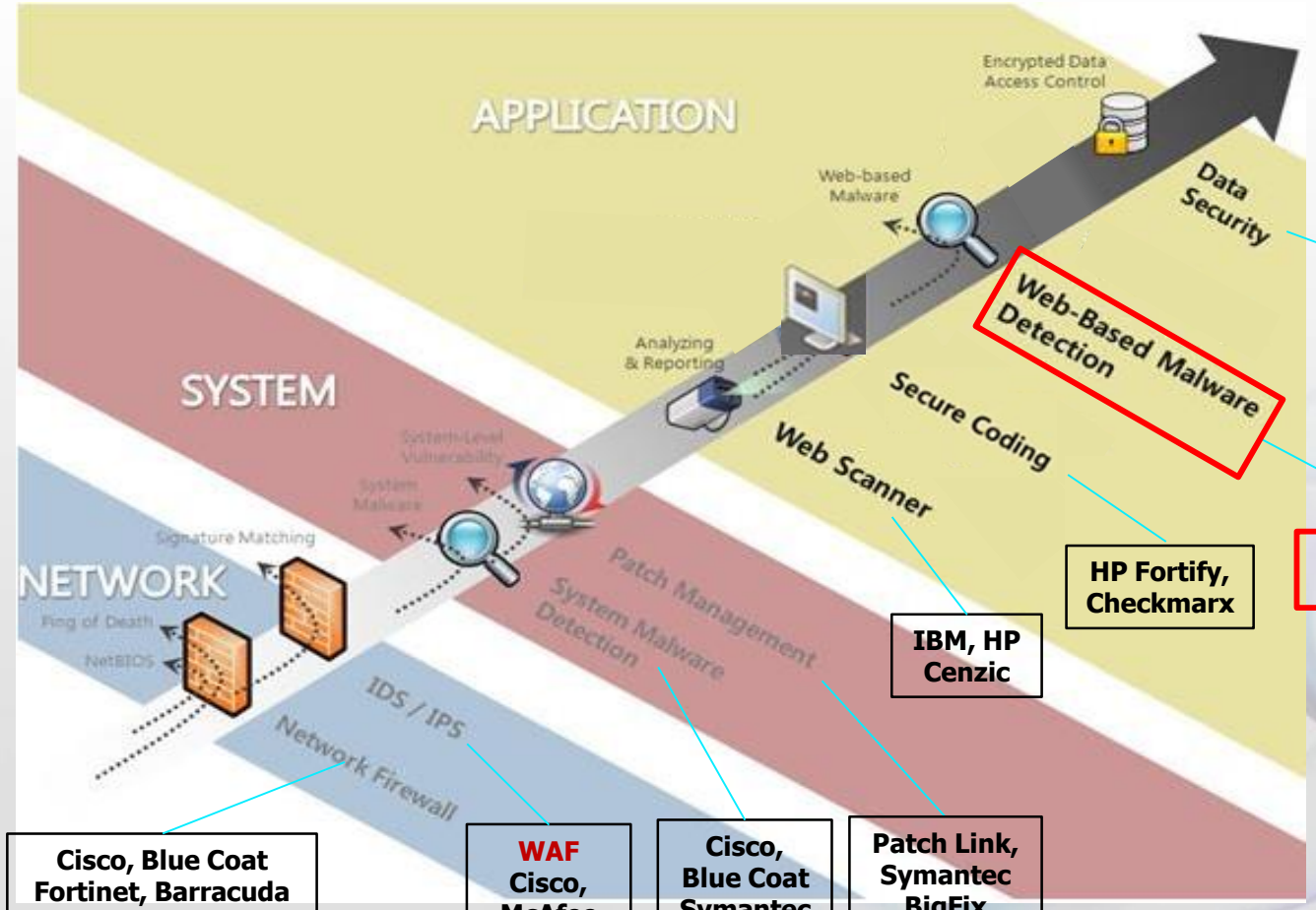
악성 URL 탐지 및 조치

웹 서버 설정파일
변경 방지

Cloud 컴퓨팅
VM, Docker 지원

WSS Positioning

Web Security 3 Tier and Solutions



WSS Positioning

WEB Application Security

- 웹 보안의 핵심은 웹 애플리케이션 보안
- 애플리케이션 보안은 개발부터 구축 후 유지보수까지 신중한 관리가 필수

▷ **Web Scanner**
웹 응용프로그램 의 설계상 취약점 및 잠재적 취약점을 분석하는 프로그램

▷ **Secure Coding**
개발 과정에서 개발자의 지식부족 및 실수 등 다양한 원인으로 발생할 수 있는 취약점을 최소화하기 위해 설계 단계부터 보안을 고려해서 코딩

▷ **Web-Based Malware Detection**
기존 동작하고 있는 웹 어플리케이션에 웹쉘이 소스코드로 중간에 삽입되는 것을 실시간으로 탐지하여 제거하고 관리자에게 통보하며 삽입된 웹쉘은 거의 탐지가 어려우며, 해커들은 이 웹쉘을 해킹을 위해 여러 용도로 사용

▷ **Data Security**
이 솔루션은 일반적으로 웹 애플리케이션 환경에서 데이터저장 및 DB구축을 하는데, 이러한 데이터를 안전하게 관리

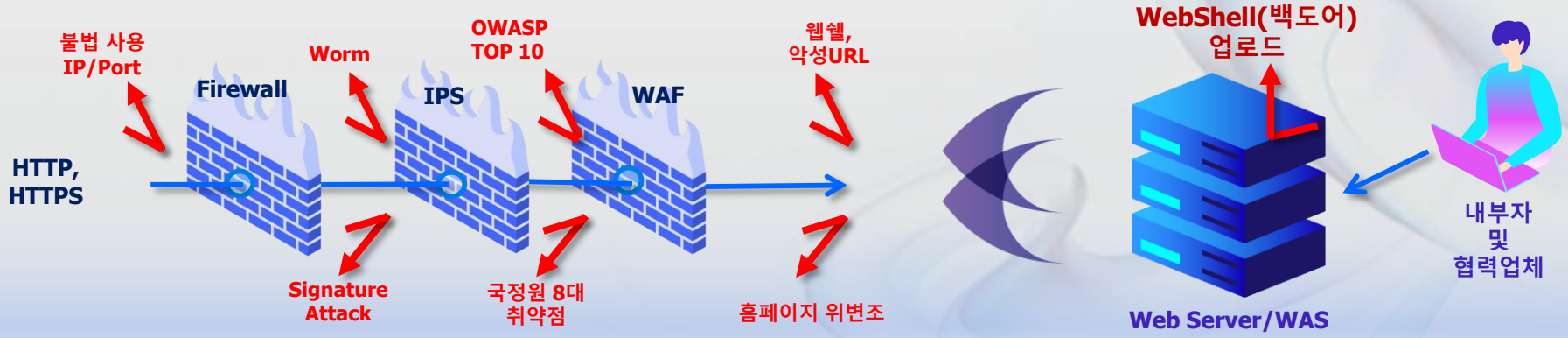
2. WSS 소개(개요 및 구조)

Why WSS (Web Server Safeguard)?

WSS는 웹 어플리케이션 취약점 등을 통한 해커의 다양한 웹 공격을 방어합니다.

* Network 보안Appliance 인 WAF (Web Application Firewall)와 상호 보완적 관계

- 침입방식의 다양화에 따라 네트워크 방어의 한계 존재(시스템 내부에서 웹 서버 악성코드 탐지/검역 필요성 대두)
- 외부 해킹 뿐만 아니라 조직 내부 사용자에 의한 정보보안 사고 증가
- 웹 방화벽 설치 이전 침투한 웹서버 악성코드 탐지 불가
- **full inspections**에 대한 과부화
- 네트워크 **Bypass** 취약점에 의한 침투 가능
- 암호화/인코딩 트래픽 및 보안정책 예외 처리에 대한 위험성



2. WSS 소개(개요 및 구조)

개요 및 주요기능

제품명	WSS (Web Server Safeguard)
최신버전	v2.7
출시연/월	2010년 05월
제조사	㈜유엠브이기술

- **웹쉘 탐지**
  - 웹쉘 탐지
  - 검역처리
  - 예외처리
- **악성URL**
  - 블랙리스트
  - 화이트리스트
  - 그레이리스트
  - URL/URI 관리
- **웹 서버 설정파일 변경 방지**
  - 파일변경 탐지
  - 파일변경 방지
- **관리기능**
  - 권한관리
  - 에이전트관리
  - 업데이트 관리
  - 홈디렉토리 자동찾기
- **클라우드 시스템 지원 기능**
  - Scale In/Out 지원
  - 이력관리
  - 네트워크 보안관리
  - Docker/ Container 지원 기능

WSS 솔루션 구성

관리서버, 에이전트, 매니저 프로그램(PC)으로 구성

WSS 관리서버	WSS 에이전트	매니저프로그램(PC)
• VM 또는 HW 에 설치하는 서버SW로 WSS Agent에 연결되어 작동 • 탐지된 이력 및 탐지 정보를 저장 • 원격 관리 제어 • 웹쉘 패턴 업데이트 및 에이전트 배포 외	• 웹서버/WAS에 설치하는 프로그램 • 웹쉘 탐지 및 악성 유포지 URL 탐지 • 웹쉘 탐지 및 필터링 경과 서버 전송 외 • JDK 1.5 지원 가능한 Unix, Linux, NT O/S 지원	• 관리자 운영 PC에 설치 (WSS관리서버에 연결) • 웹쉘 탐지 실행 • 모니터링, 원격조치, 환경설정 • 관리자 권한관리, 통계 & 리포팅 외

WSS 탐지방식

탐지성능을 향상을 위하여 악성코드를 수집

- ✓ **30,000대 이상 적용 에이전트의 탐지 내역 분석**
- ✓ **악성코드 수집 및 분석 전문 인력 운영**

패턴 탐지

- 보유한 웹쉘 패턴과 탐지된 파일의 패턴을 비교 탐지
- 시그니처로 웹쉘 패턴을 생성 / 알려진 웹쉘을 탐지

해시값 탐지

- 패턴이 지속 증가할 경우 시스템의 속도가 저하됨으로 효율적인 성능을 위해 WSS는 악성 코드 공유 포털인 www.virustotal.com 해시값을 주기적 업데이트 탐지

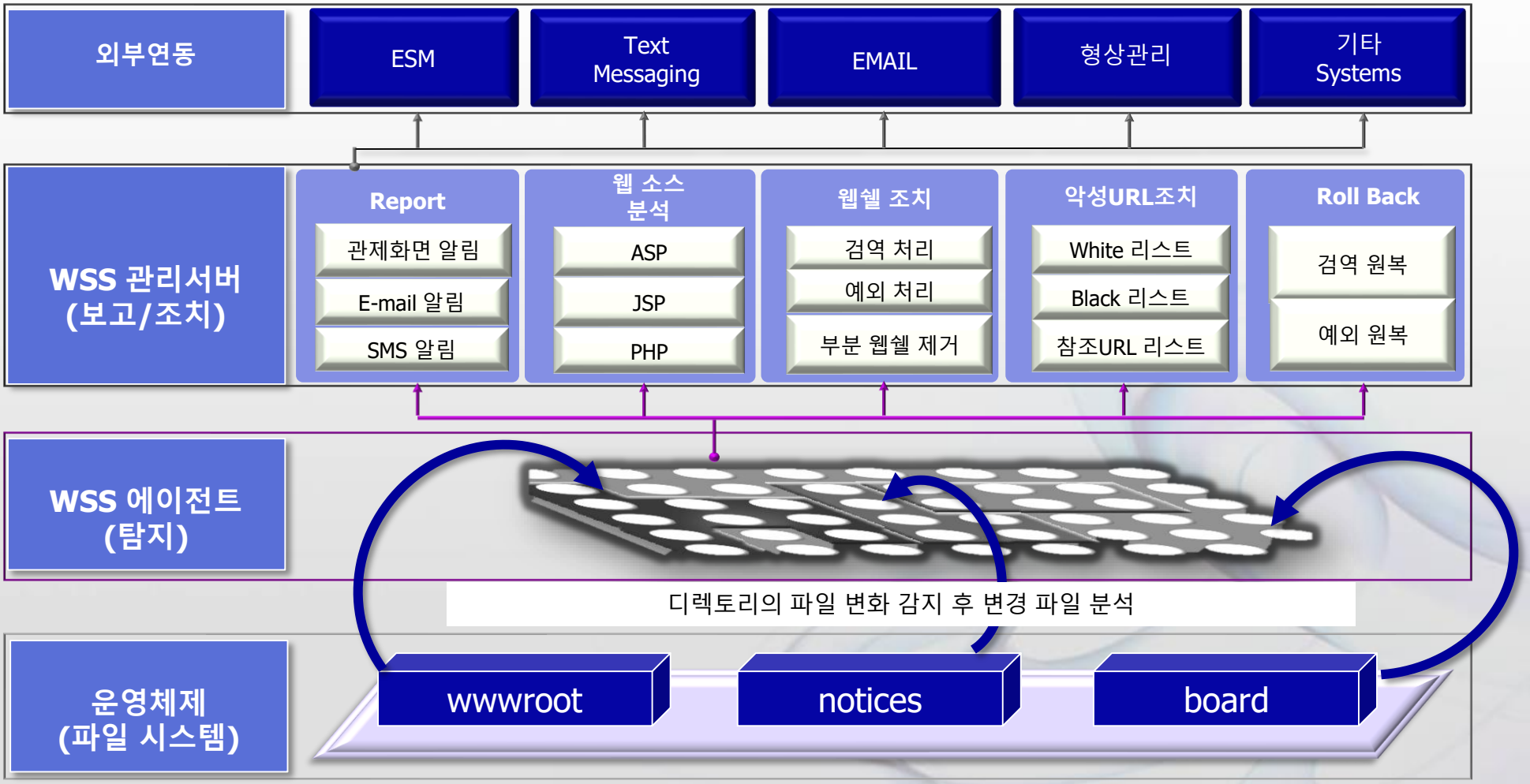
알고리즘 탐지

- JAVA Script 등 난독화된 혹은 인코딩된 웹쉘을 내부코드를 통해 탐지

2. WSS 소개(개요 및 구조)

구조 및 동작원리

파일시스템 모니터링을 통하여 변조, 생성되는 악성코드를 탐지합니다

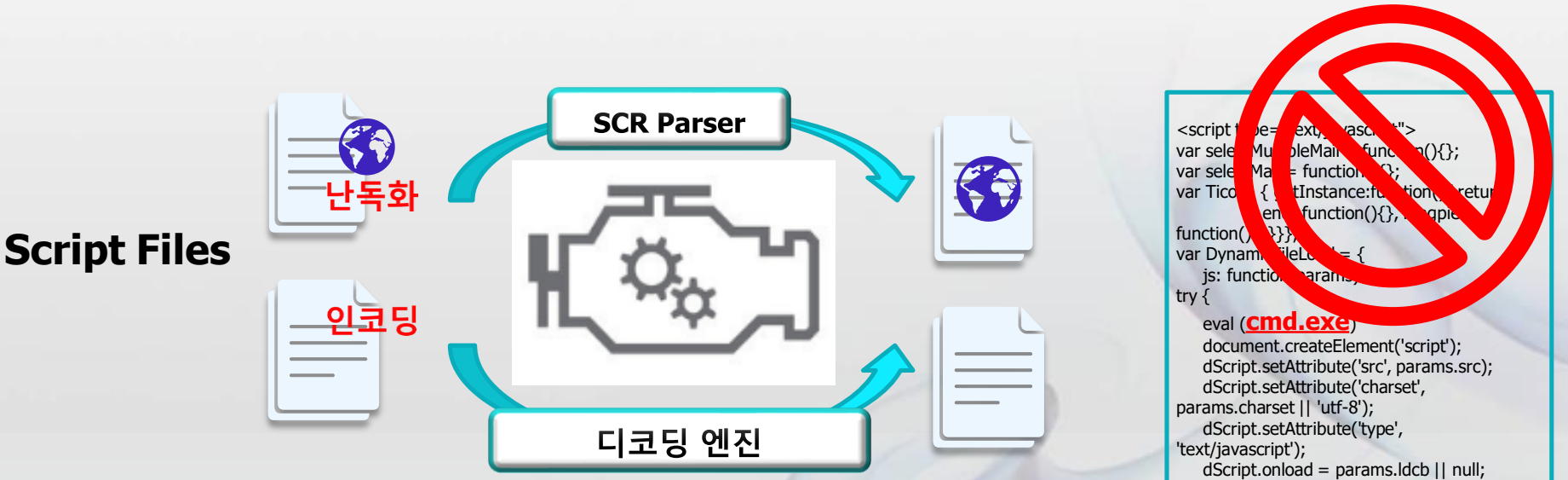


목차

3. WSS 주요 특징

탁월한 탐지성능

- **WSS는 난독화 전용 분석엔진 (SCR Parser)를 통하여 Unknown 악성코드 탐지를 지원**
- **탐지 성능 향상을 위한 악성코드 수집**
  - 30,000여대 적용 에이전트 탐지 내역 분석
  - 악성코드 수집 및 분석 전문인력 운영
- **오탐 최소화를 위한 정교한 패턴적용 및 예외처리 지원**
- **웹서버/WAS별 환경을 고려한 패턴 커스터마이징을 지원**

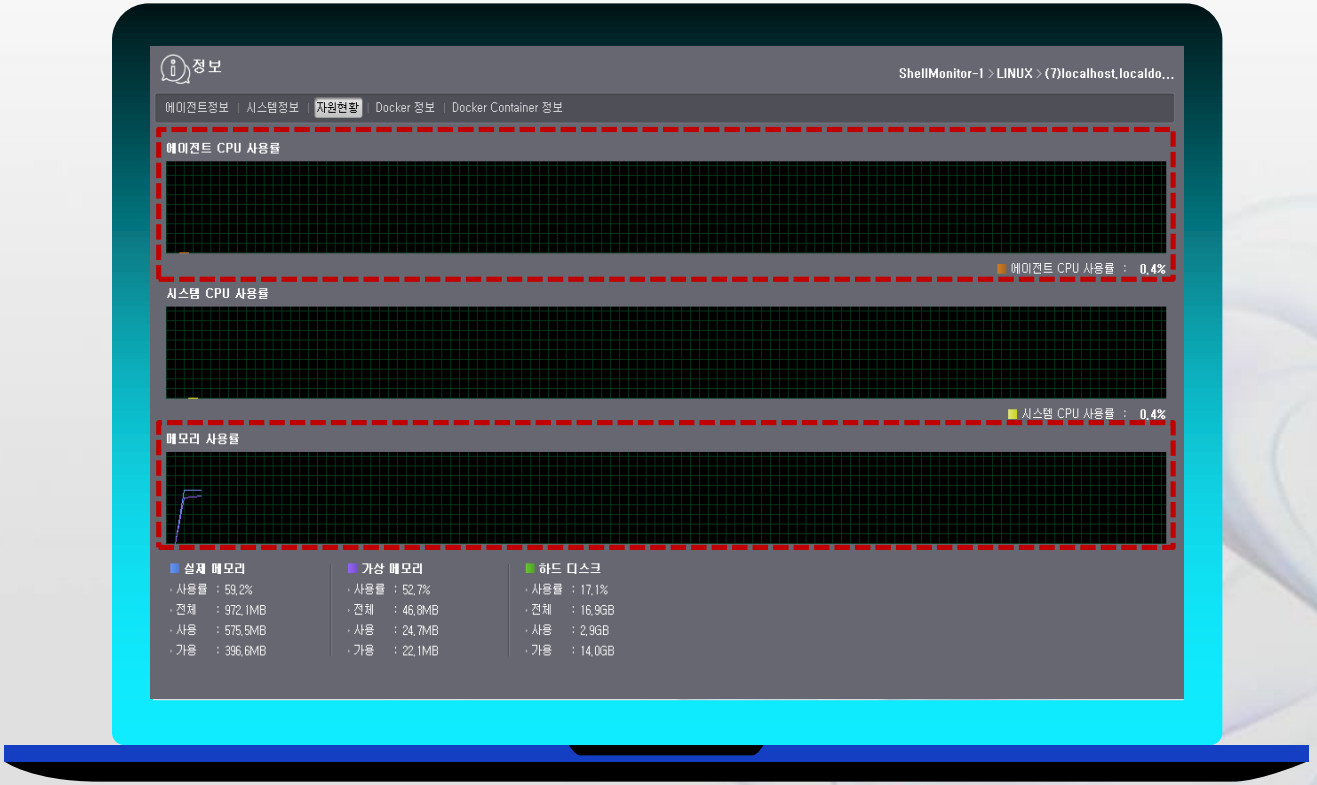


SCR Parser (Source Code Recombinant Parser)
난독화 소스코드 분석 및 탐지를 위한 전용엔진

3. WSS 주요 특징

뛰어난 안정성

- 설치대상 서버의 리소스 사용률 최소화 (CPU, memory)
- 이식성: JAVA 1.5 이상을 지원하는 모든 OS지원(Windows, Linux, Unix)
- 관리서버 HA(High Availability) 이중화 구성 지원

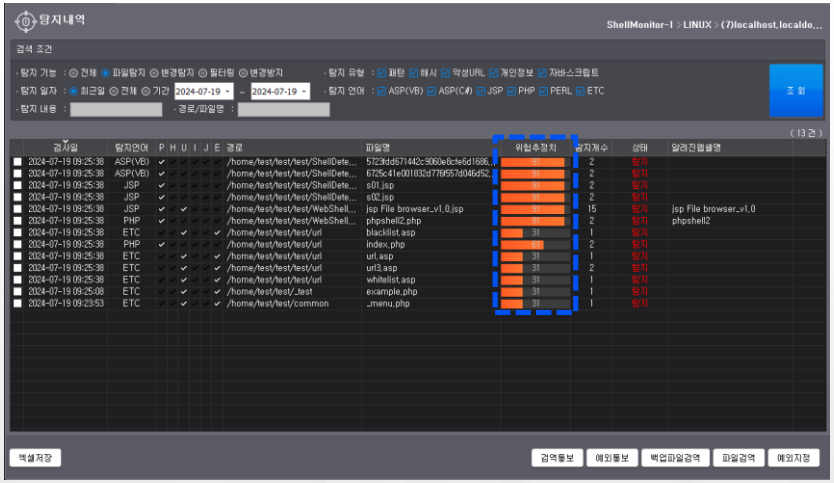


[탐지 에이전트 자원사용률 모니터링 화면]

3. WSS 주요 특징

운용 편의성

- **효율적인 탐지조치 지원**
  - 알려진 웹쉘 및 악성URL 자동검역 지원
  - UnKnown 악성코드 위험도 및 행위 내용 제공
- **편리한 업데이트 지원**
  - 패턴 및 탐지 에이전트 자동 업데이트 지원
- **R&R (Role and Responsibility) 지원 기능**
  - 검역 시 원클릭 보고기능 지원
  - 탐지대상 디렉토리 자동찾기 지원
  - 최신 탐지내역을 관리서버로 자동백업 지원
  - 관리자/관제인력/운영인력 등 업무처리 상황에 맞는 상세 권한 관리 지원
  - 운영 중 추가되는 탐지대상 디렉토리 자동 설정 및 탐지



[탐지 리스트 및 위험 추정치 정보 화면]

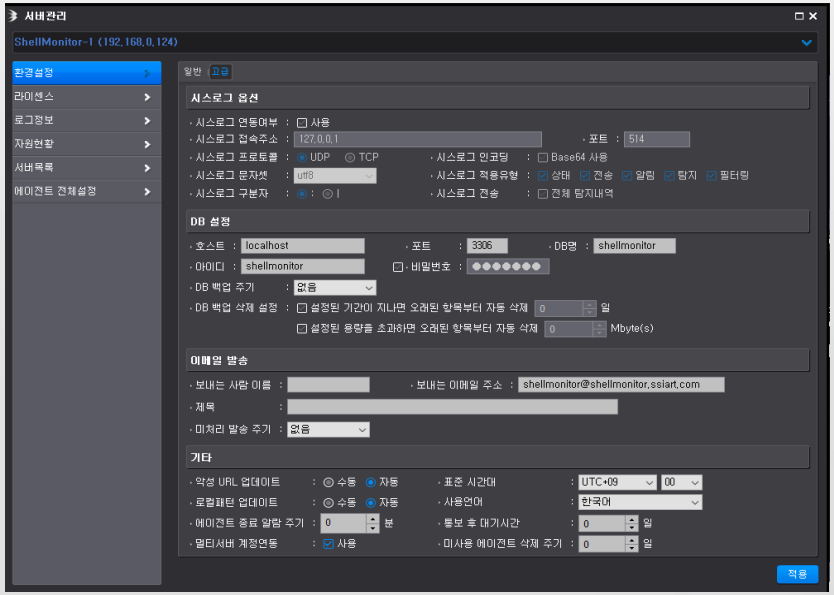
[탐지 패턴 위협정보 화면]

[탐지 상세 화면]

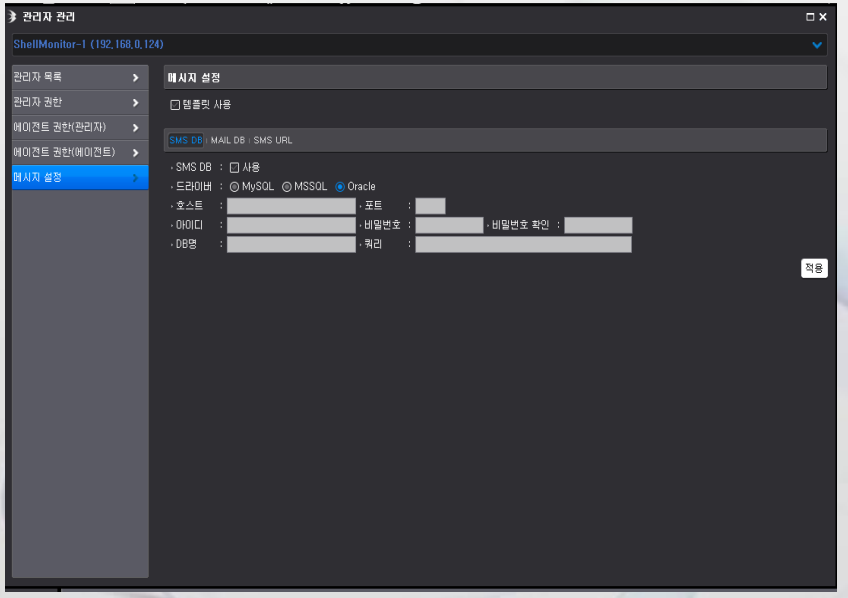
3. WSS 주요 특징

편리한 확장성

- **가상화 및 클라우드 환경 지원**
  - AWS, KT uCloud, MS Azure, G-Cloud , Naver Cloud 및 기타 클라우드에 적용가능
- **병렬 확장지원**
  - 기존 시스템 및 네트워크 구조에 변경없이 확장지원
- **외부시스템 연동지원**
  - SYSLOG, SMTP, API 등
  - ESM, SIEM, 형상관리, SMS, EMAIL 등



[SYSLOG 연동 화면]



[SMS, EMAIL 연동 화면]

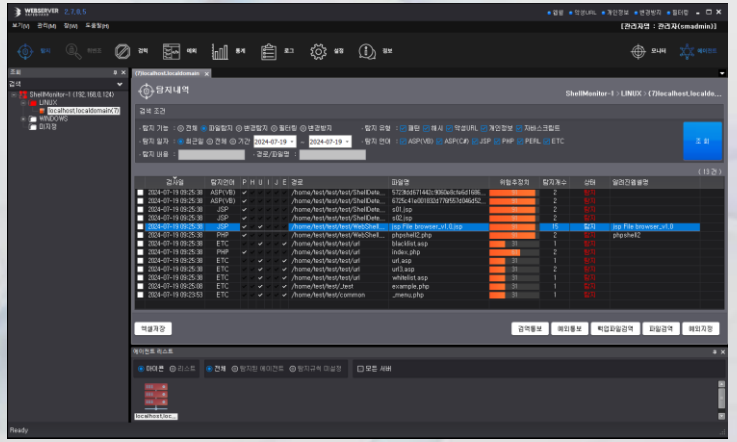
목차

4. WSS 주요 기능

웹쉘 및 악성URL 탐지기능

기능명	상세기능	설명
실시간 웹쉘 탐지	탐지	전체 탐지, 실시간 탐지를 통하여 웹쉘 파일 탐지 및 보고
	탐지내역 조치	검역, 예외조치를 통하여 탐지 내역 조치
실시간 악성 URL 탐지	탐지	전체 탐지, 실시간 탐지를 통하여 악성URL 파일 탐지 및 보고
	탐지내역 조치	탐지된 URL 검역, 부분검역, 예외조치
	관리기능	그레이, 화이트, 블랙 리스트로 URL 관리

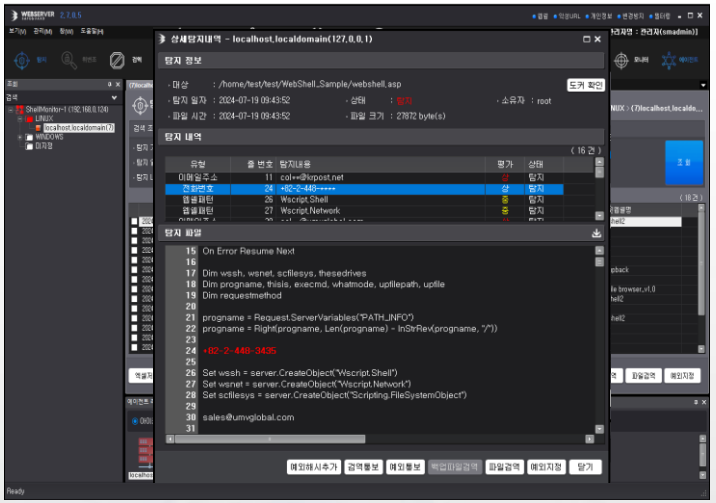
[탐지내역 정보 화면]



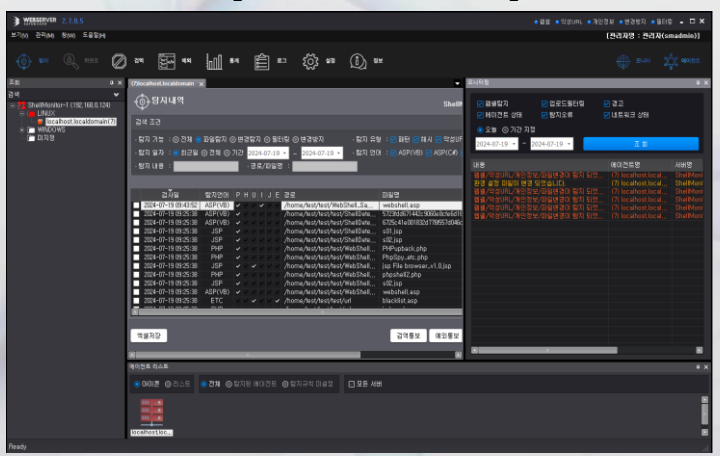
4. WSS 주요 기능

환경설정 변경탐지 및 기타 기능

기능명	상세기능	설명
웹서버/WAS 환경설정파일 변경방지	웹서버 설정파일 관리	임의 또는 악의적인 웹 서버 설정파일 변경 시 관리자에게 보고
파일 및 DB 개인정보탐지	개인정보 탐지 (파일)	웹서버 파일 내의 개인정보 탐지 및 보고 (PDF, HWP, DOC, PPT, EXCEL, TXT, etc.)
	개인정보 탐지 (DB)	DB 내의 개인정보 탐지 및 보고
업로드 파일 필터링	파일 필터링	파일 업로드 게시판 허가되지 않은 파일 필터링
침해 대응	공격자 IP탐지	웹쉘 실행 시 웹서버/WAS 로그를 분석하여 실행 IP 보고



[개인정보 탐지화면]

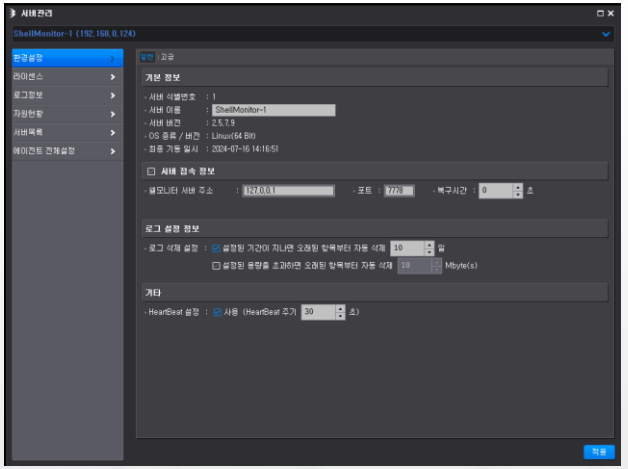


[탐지 알림 화면]

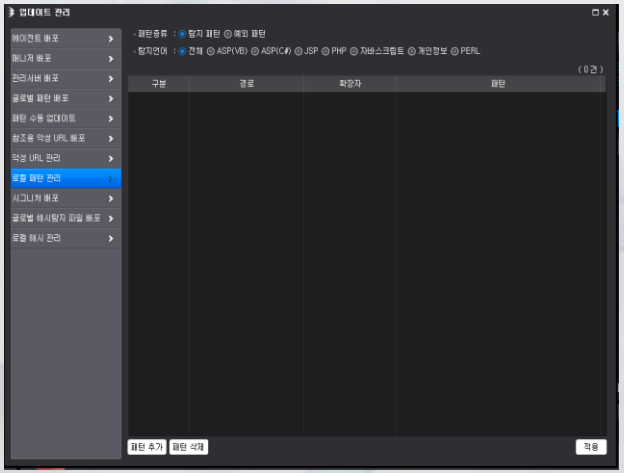
4. WSS 주요 기능

관리기능

기능명	상세기능	설명
관리기능	업데이트 관리	에이전트, 매니저, 패턴 업데이트 및 버전관리
	탐지 알림 및 외부 시스템 연동	관제화면, ESM, SMS, EMAIL 등 외부시스템 연동 및 인터페이스 제공
	계정 및 사용자 권한관리	계정 및 사용자 별 권한 관리
	통계 및 리포팅	보고서 및 통계자료 제공
	안정성	설치된 웹서버/WAS의 자원 사용 율 조정 관리서버 이중화 지원(Active/Active)



[환경설정 화면]



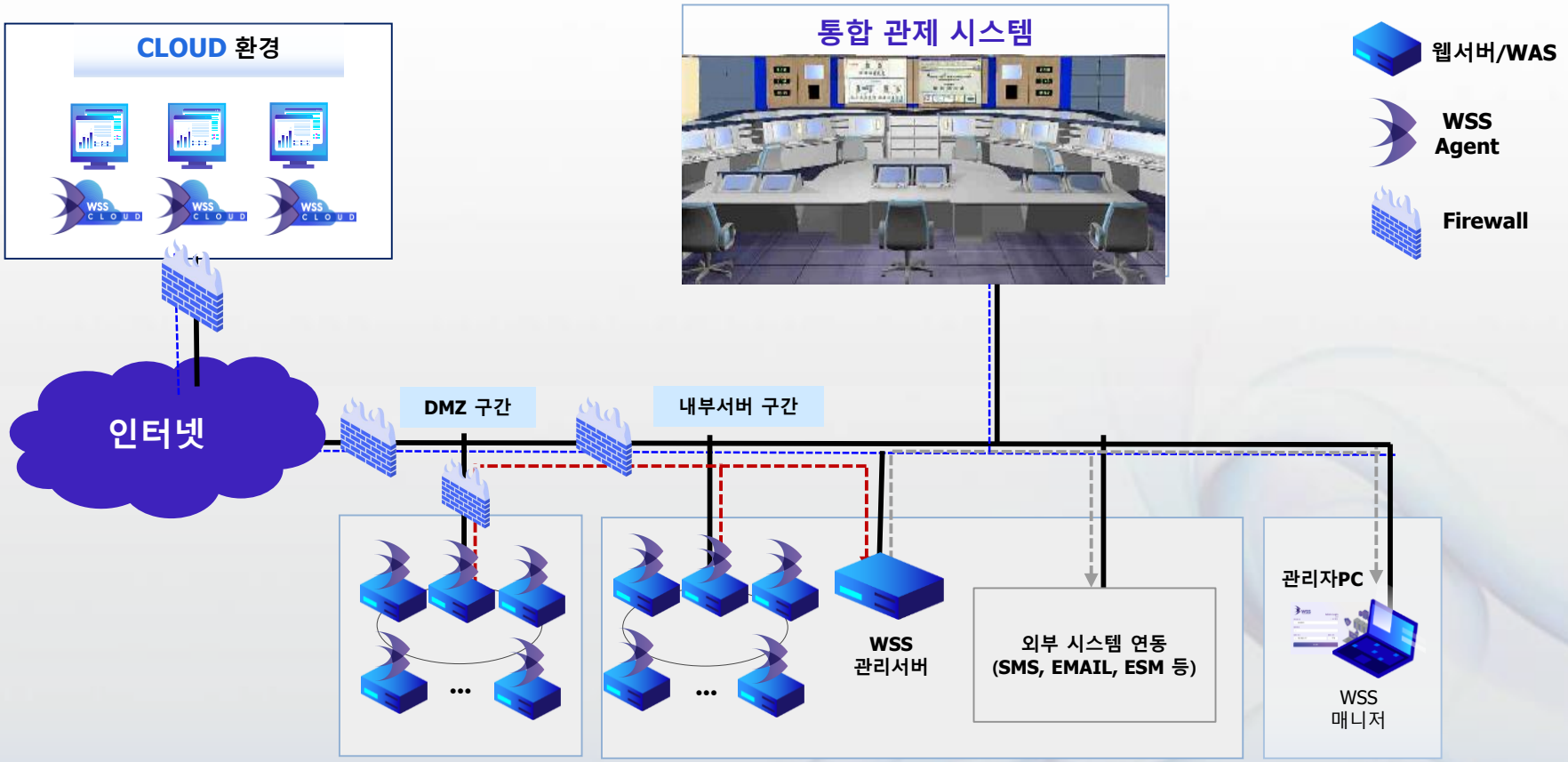
[업데이트 관리화면]

클라우드 지원 기능

기능명	상세기능	설명
Scale IN/OUT 기능 지원	Scale OUT	WEB/WAS 서비스 Scale OUT시 탐지 대상 자동 등록 후 자동 탐지
	Scale IN	WEB/WAS 서비스 Scale IN 시 삭제 Instance의 탐지/변경/삭제에 대한 이력(로그)을 관리서버로 자동 저장
Docker /Container 도커/ 컨테이너 지원	기본정보제공	Agent 기능에 Docker에 대한 기본정보제공
	구분 및 처리	탐지된 파일에 대한 Container 구분 및 처리

WSS Configuration

On-Premise/Cloud Computing/ 통합관제



주요 고객사

공공기관


Ministry of Science, ICT and Future Planning

National Radio Research Agency

Ministry of National Defense
Republic of Korea

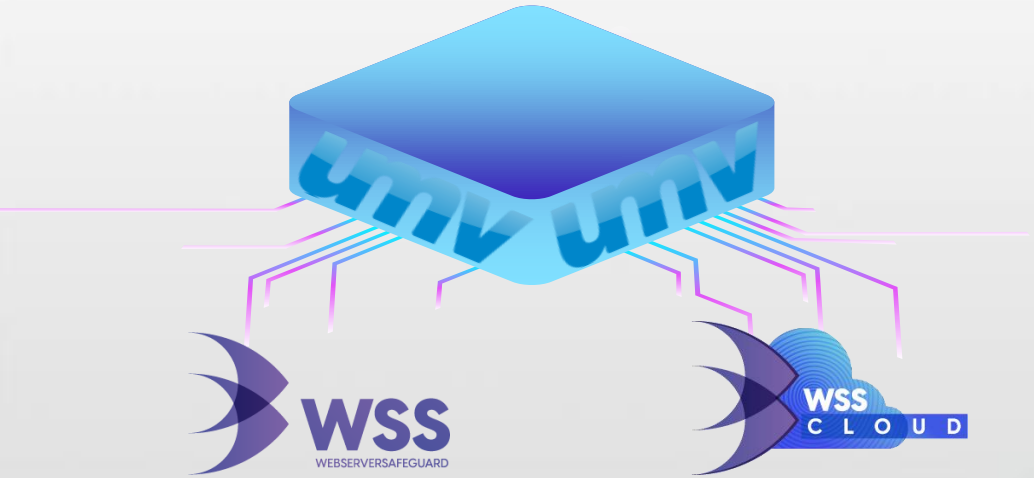
SUPREME COURT OF KOREA

금융

SAMSUNG LIFE INSURANCE


기업

실시간 탐지 및 격리를 통한
완벽한 웹서비스 보안



▶ Watch Video

감사합니다

Telephone: +82-2-448-3435
Website: www.umvglobal.com
Email: qkrtj1006@umv.co.kr