MCDetector

악성코드 탐지 솔루션

ReturnTrue
SOFTWARE DEVELOPMENT

CONTENT

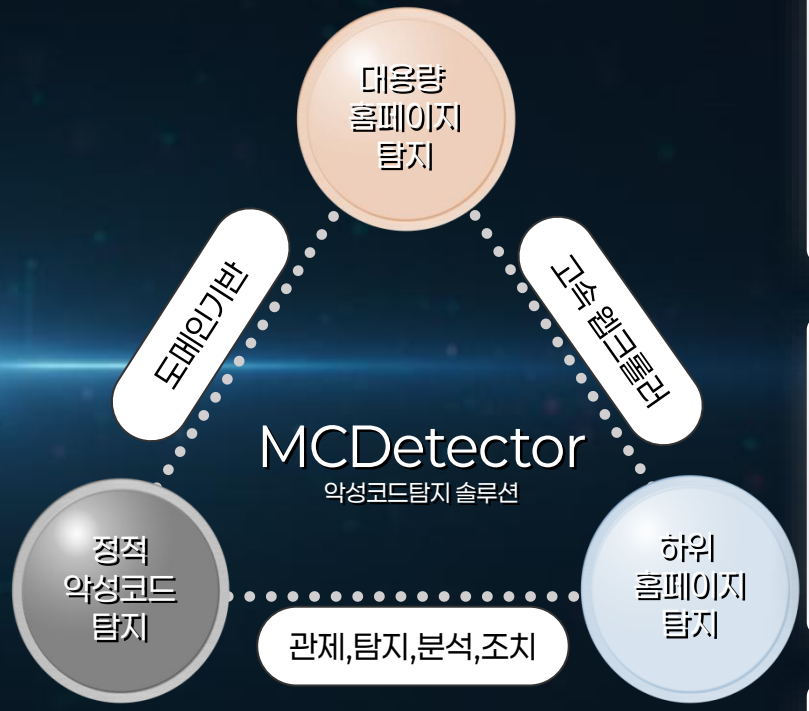
목차

ReturnTrue SOFTWARE DEVELOPMENT

MCDetector란?

홈페이지내의 악성코드를 탐지하는 솔루션

MCDetector는 하루 수백만 개의 웹사이트를 빠른 주기로 스캔하여 악성코드 유포지·경유지를 탐지하고 이력을 관리하는 국내 최대 규모의 악성코드 탐지 솔루션입니다.



대용량 홈페이지 탐지

- 1일 수백만개의 웹사이트내의 악성코드를 탐지 [국내최대]
- 악성코드 유포지/경유지에 대한 탐지 및 이력 관리
- 분석 및 조치를 위한 결과 및 탐지 소스 제공
- 타 보안시스템과 연동을 위한 결과 제공
- 관심 사이트 빠른 주기 설정을 통한 악성코드 탐지

정적 악성코드 탐지

- 시그니쳐기반 악성코드 탐지
- 악성URL 및 홈페이지내의 악성파일 탐지
- 문자열, 해쉬값, 정규식을 통한 악성코드 탐지
- JavaScript 영역탐지, HTTPS, Gzip Encoding 지원
- MS,Google 등 통합된 KISA의 탐지룰 자동 업데이트 지원

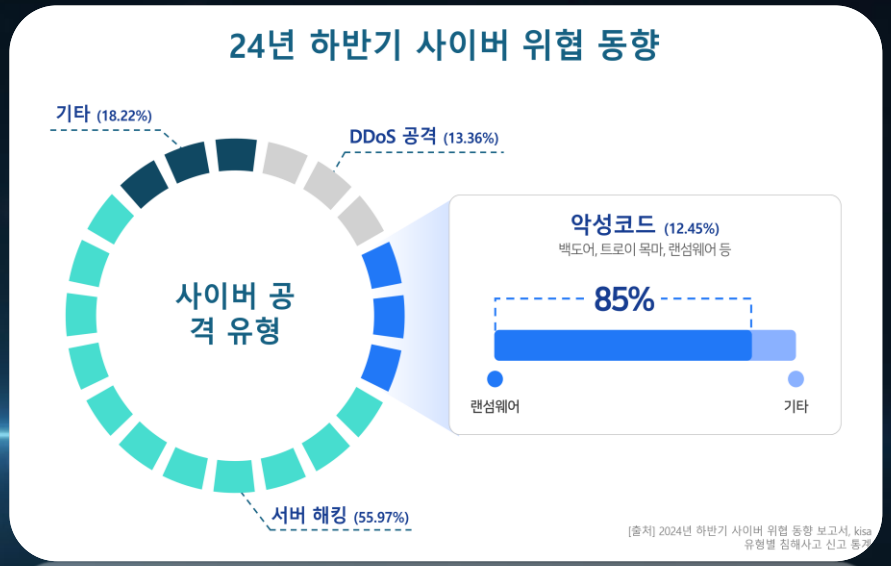
하위 홈페이지 탐지

- 고속 웹크롤러를 통한 하위 페이지 탐지
- HTML 및 JavaScriptLH의 하위 페이지에 대한 링크 추출
- 웹페이지내의 모든 하위 페이지 탐지 가능
- 보안장비(방화벽)등에서 차단에 대한 기술적 대응
- 하위 페이지 탐지에 대한 아키텍처 제공

배경

홈페이지내의 악성코드 증가
지속적인 대응 필요

웹사이트를 통한 악성코드 유포와 감염 사례가 급증하면서, 실시간 탐지와 신속한 대응의 필요성이 높아지고 있습니다.
이에 따라 인터넷 상의 수많은 웹 자원을 자동으로 분석하여 악성코드를 조기에 식별·차단하는 솔루션이 요구되고 있습니다.



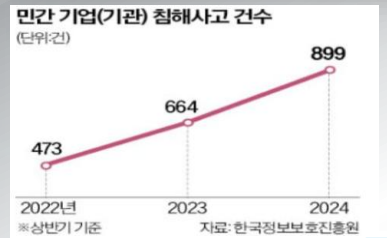
- 2024년 하반기 KISA 보고서에 따르면 침해사고 신고 유형 중에서 악성코드 감염이 전체의 약 12.1%를 차지함.
- 같은 기간 서버해킹이 전체의 약 56%로 가장 많았고, 악성코드 감염·랜섬웨어가 그 뒤를 잇는 형태로 나타났습니다
- 2025년 상반기에는 신고건수가 전년 동기 대비 약 15% 증가함(899건 → 1,034건)이며, 그중 악성코드 감염 신고 건수가 115건으로 보고됨.
- 보안업체들의 동향에서도, 최근 월별 악성코드 유형별 비율에서 Trojan이 약 60% 이상을 차지하는 등 악성코드 활동 강도가 높아지고 있습니다.

- 한국인터넷진흥원(KISA)의「2020년 상반기 악성코드 은닉사이트 탐지 동향 보고서」에 따르면, 홈페이지를 통해 악성스크립트 또는 악성코드가 삽입된 은닉사이트(유포지·경유지) 탐지·조치 건수를 통해 웹사이트 기반 유포 규모 및 변화를 확인할 수 있습니다.
- 2021년 상반기에는 유포지·경유지 포함 전체 탐지 건수가 5,005건으로 전년도 하반기 대비 약 49% 증가했습니다.
- 2022년 상반기 유포지 건수는 1,959건으로, 전년 하반기 1,424건 대비 약 38% 증가했습니다.

필요성

웹사이트를 통한 악성코드 유포가 지속적으로 증가하면서, 실시간 탐지와 조기 대응이 필수 보안 요소가 되었습니다.
이에 따라 대규모 웹 자원을 자동으로 분석해 악성코드 감염 경로를 신속히 파악·차단하는 솔루션의 필요성이 높아지고 있습니다.

기하급수적인 악성코드 증가



- 매일 20만여 개의 악성코드가 새롭게 발견(한국인터넷진흥원)
- 악성코드 은닉사이트 매년 10% 이상 증가

[표 1-2] 유형별 침해사고 신고 현황

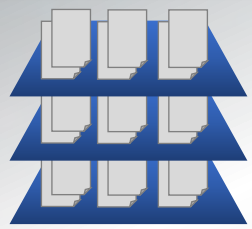
[단위 : 건수]

구분	연도	2023 (상반기)	비율	2023 (하반기)	비율	2024 (상반기)	비율	2024 (하반기)	비율
침해사고 신고	DDoS 공격	124	18.7%	89	14.5%	153	17.0%	132	13.4%
	악성코드	156	23.5%	144	23.5%	106	11.8%	123	12.4%
	(랜섬웨어)	(134)	(20.2%)	(124)	(20.2%)	(92)	(10.2%)	(103)	(10.4%)
	서버 해킹	320	48.2%	263	42.9%	504	56.1%	553	56.0%
	기타	64	9.6%	117	19.1%	136	15.1%	180	18.2%
합 계		664		613		899		988	

내부보안의 한계

- 내부 악성코드 대처에만 많은 비용 소요되나 신종 악성코드에 대해 대응 미흡
- 능동적 악성코드 탐지를 위한 탐지 솔루션 부재(정규식, 수동 탐지패턴 등록 등)

점검대상의 최대화



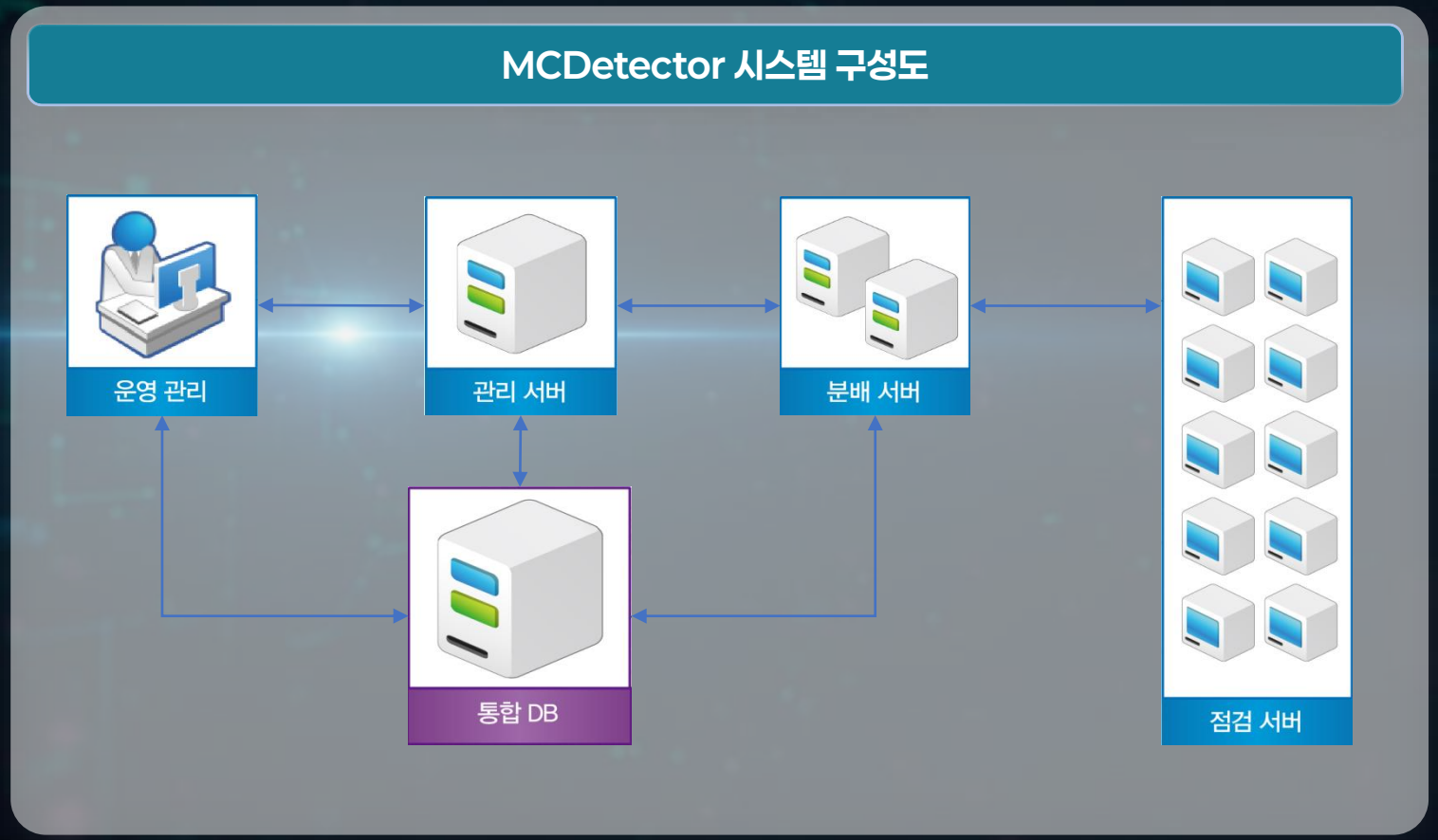
- 1Depth이상의 하위페이지에 대한 악성코드 탐지 필요
- 최단시간 많은양의 웹페이지 탐지
- 오탐 및 미탐의 최소화 필요
- 내부,유관기관 및 외부 웹페이지에 대한 악성코드 탐지 필요

최신 악성코드 업데이트

- 한국인터넷진흥원은 국내 보안기업 및 해외 MS, Google등을 통해 악성코드를 수집하여 배포하고 있음
- 국내외에서 수집된 신종 악성코드에 대해 주기적인 업데이트 필요

구성도

MCDetector의 시스템 구성도는 악성코드 탐지, 데이터 분배, 관리 및 분석 기능이 유기적으로 연결된 구조를 보여줍니다.
이를 통해 점검서버, 분배서버, 관리서버, DB서버 간의 역할과 데이터 흐름을 한눈에 이해할 수 있습니다.



- 점검대상 : 100만 URL 이상 기준
- 점검대상 및 점검주기에 따라 서버 통합 가능
- 타 보안장비와의 통합 구축 가능
- 운영체제
  - Windows Server Std 2012 R2(점검/분배/관리/DB)
  - MS-SQL ServerStd 2014

H/W 요구사항

MCDetector는 설치형 소프트웨어로 제공되며, 점검 대상과 주기에 따라 하드웨어 사양을 유연하게 조정할 수 있습니다.
제시된 사양은 권고 기준이며, 사용 환경에 따라 필수 또는 권고 하드웨어 구성을 선택하여 운영할 수 있습니다.

서버	주요 기능	기능 설명
점검 서버	CPU	Xeon E5계열 8Core+, (2소켓)
	Memory	16GB+
	HDD	1T , SATA가능
	OS	Windows server 2012 R2
분배 서버	CPU	Xeon E3계열 8Core,
	Memory	4GB+
	HDD	1T , SATA가능
	OS	Windows server 2012 R2
관리 서버	CPU	Xeon E3계열 4Core,
	Memory	16GB+
	HDD	1T , SATA가능
	OS	Windows server 2012 R2
DB 서버	CPU	Xeon E5계열 16Core+, (2소켓)
	Memory	64GB+
	HDD	4TB+, RAID 구성
	OS	Windows server 2012 R2
	DataBase	SQL Server 2014

- 점검/분배/관리 Software는 install 형태로 지원
- H/W 사양은 점검대상 및 점검주기에 따라 변경 가능
- 스팩은 권고 사양임

- 필수 H/W (2식) : 1일 50만 이하 URL 탐지
  - 점검서버 (1식)
  - DB/분배/관리 서버 (1식)

- 권고 H/W(5식) : 1일 500만 이상 URL 탐지
  - 점검서버 (2식)
  - 분배서버 (1식)
  - 관리서버 (1식)
  - DB서버 (1식)

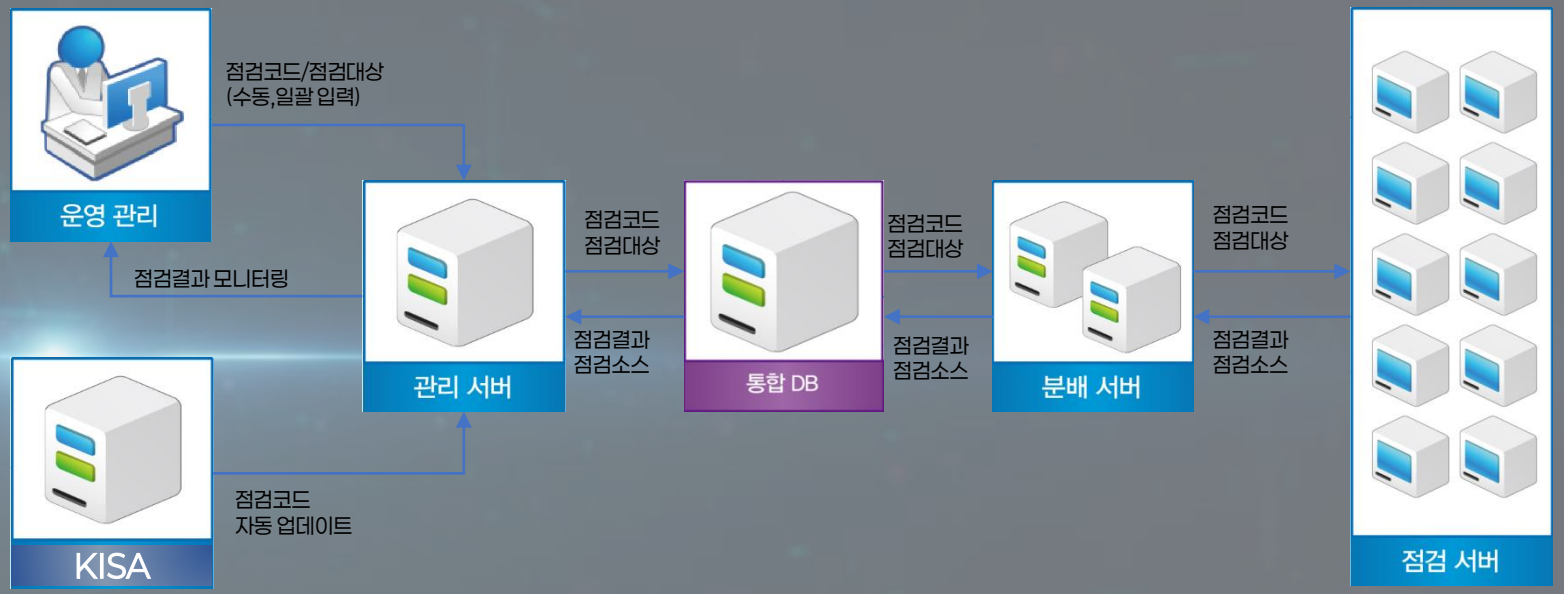
서버별 기능

MCDetector는 설치형 소프트웨어로 제공되며, 점검 대상과 주기에 따라 하드웨어 사양을 유연하게 조정할 수 있습니다.
제시된 사양은 권고 기준이며, 사용 환경에 따라 필수 또는 권고 하드웨어 구성을 선택하여 운영할 수 있습니다.

서버	주요 기능	기능 설명
점검 서버	HTML 문서수집 웹크롤러 기능	HTML 분석 (2 Depth이상의 하위페이지 수집)
	악성코드 유포지/경유지 자동 탐지기능	패턴 매칭, 난독화, Decoding을 통한 유포/경유지 자동 탐지
	악성코드 다운로드 기능	파일 다운로드후 악성코드 감염 여부 탐지 기능
	악성코드 URL 링크구조 추출	악성코드 URL 링크구조 추출
	난독화 페이지 및 Encoding 페이지 추출	Encoding 페이지 추출
분배 서버	점검대상 도메인 분배	효율적인 점검을 위한 점검서버별 도메인 분배
	경유지/유포지 결과 저장	탐지된 결과에 대한 정보 DB시스템에 저장 기능
	점검서버 상태 모니터링	점검서버의 상태를 점검후 재실행등의 기능 수행
관리 서버	점검대상 도메인 관리	웹을 통해 점검대상 도메인에 대한 입력/삭제/수정 등의 기능
	점검대상 URL에 대한 정책적 관리 기능	점검 Group에 따른 점검주기(주중/주말), Sub URL 점검 Depth 관리
	운영관리를 위한 Report/GUI	데시보드를 통한 운영상태 모니터링
	도메인 담당자 관리 기능	악성코드 결과에 대해 이메일 발송등의 관리 기능
	경유지/유포지 이력 관리	탐지된 결과에 대한 이력 관리 기능
DB 서버	운영 관리 기능	점검 도메인정보, 도메인관리 업체 정보, 경유지/유포지 정보 저장/관리

점검 절차

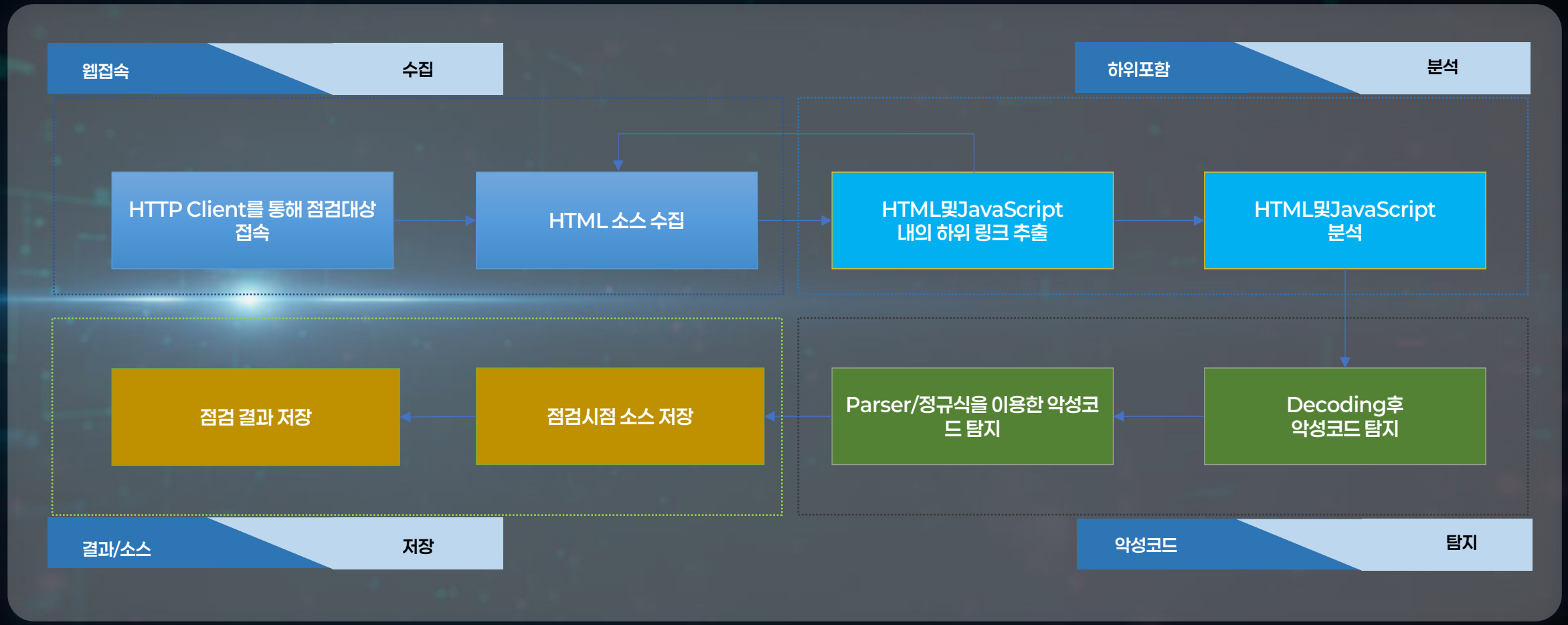
MCDetector는 설치형 소프트웨어로 제공되며, 점검 대상과 주기에 따라 하드웨어 사양을 유연하게 조정할 수 있습니다.
제시된 사양은 권고 기준이며, 사용 환경에 따라 필수 또는 권고 하드웨어 구성을 선택하여 운영할 수 있습니다.



- 점검코드 : KISA의 Krcert를 통해 자동 업데이트 또는 운영자가 점검코드(문자열,해쉬값,정규식,URL)를 입력가능
- 점검대상 : 기관에서 소유한 점검 홈페이지 도메인 등록
- 점검결과 : 악성코드 탐지 URL 및 탐지위치 그리고 탐지 Path 제공
- 점검소스 : 악성코드 탐지 시점의 소스 저장(탐지위치 하이라이팅)

점검 프로세스

MCDetector의 점검 프로세스는 수집, 분석, 탐지 결과 저장의 단계로 체계적으로 진행됩니다.
이를 통해 악성코드 탐지 과정 전반을 자동화하고, 신속하면서도 정확한 결과 관리를 지원합니다.

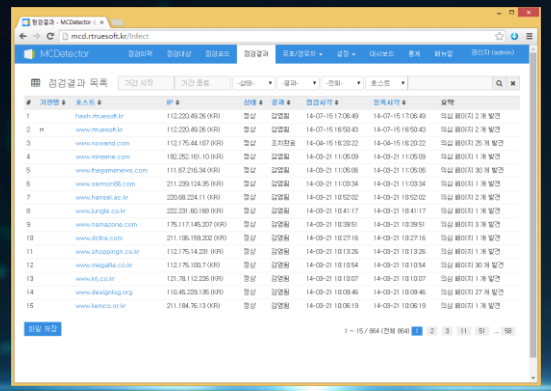


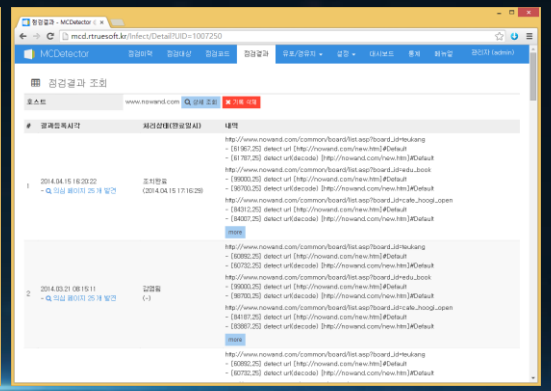
- 점검 서버별 수십개의 프로세스 생성하여 점검(시스템 성능에 변동)
- DDoS 의 공격오인을 대체하기위한 알고리즘 적용

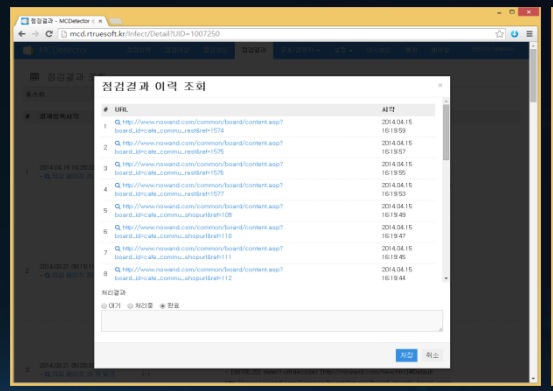
주요 화면

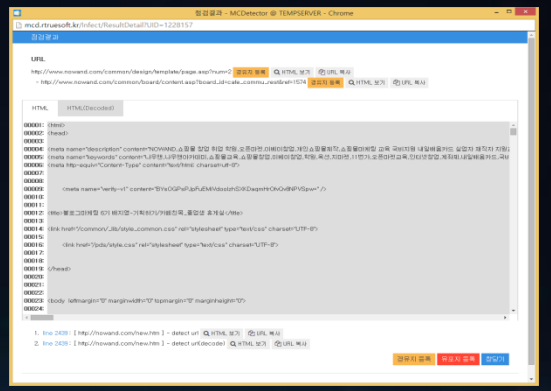
점검 결과

MCDetector의 주요 화면은 점검 대상 선택부터 결과 확인, 세부 소스 분석까지 단계별로 직관적으로 구성되어 있습니다.
이를 통해 사용자는 탐지 결과를 빠르게 확인하고, 세부 분석까지 효율적으로 수행할 수 있습니다.









점검결과 목록

- 점검대상별 점검결과 조회
- 기간별 조회
- 도메인별 상태 조회
- 악성코드 은닉 결과 조회
- 관심사이트별 조회

점검결과 대상 클릭시

- 조회된 점검결과
- 점검대상에 대해 시간별 점검결과, 처리상태, 내역을 보여줌
- 사이트별 점검시점에 악성코드 은닉여부 판별

결과 리스트 클릭시

- 의심페이지에 대한 전체 이력을 조회할 수 있음

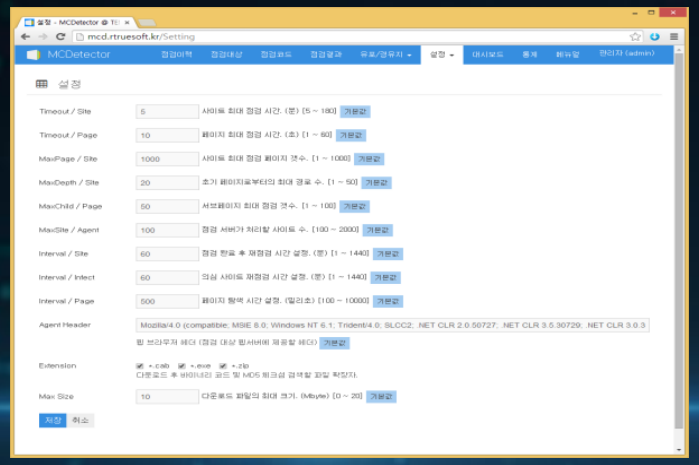
점검시점 소스 보기

- 해당 URL 클릭시 경로
- 해당시점의 소스
- 악성코드의 위치를 하일라이팅
- Decoded된 소스 제공

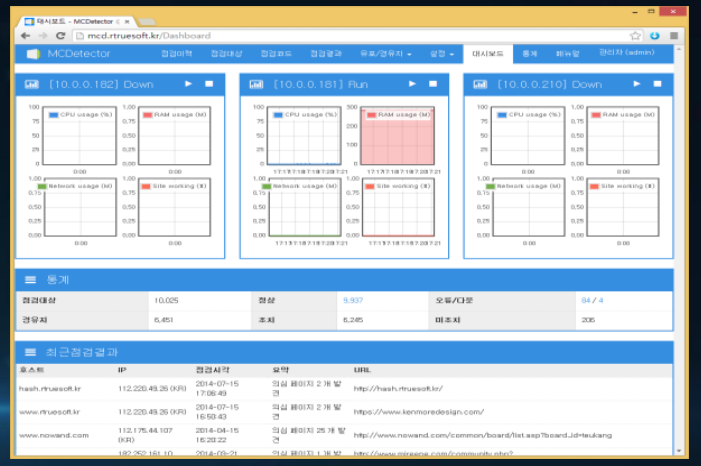
주요 화면

대시보드

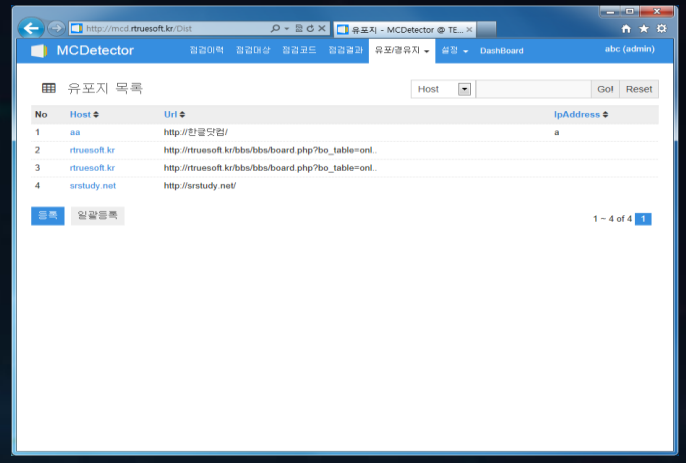
MCDetector 대시보드는 탐지 현황, 위험도, 점검 결과를 한눈에 확인할 수 있는 직관적 인터페이스를 제공합니다.
이를 통해 관리자와 보안 담당자는 실시간 모니터링과 빠른 의사결정을 효율적으로 수행할 수 있습니다.



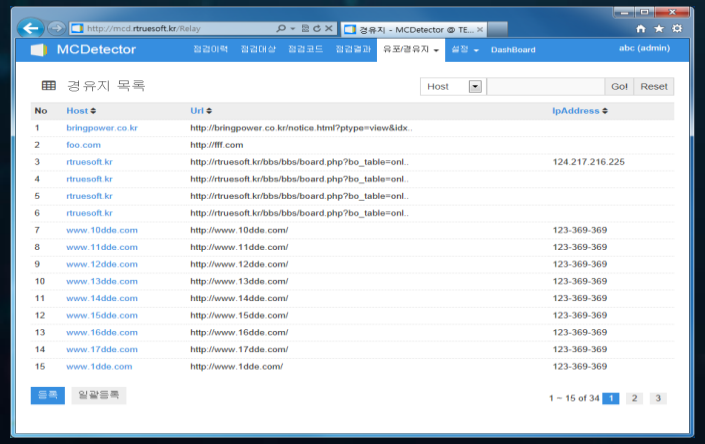
환경 설정



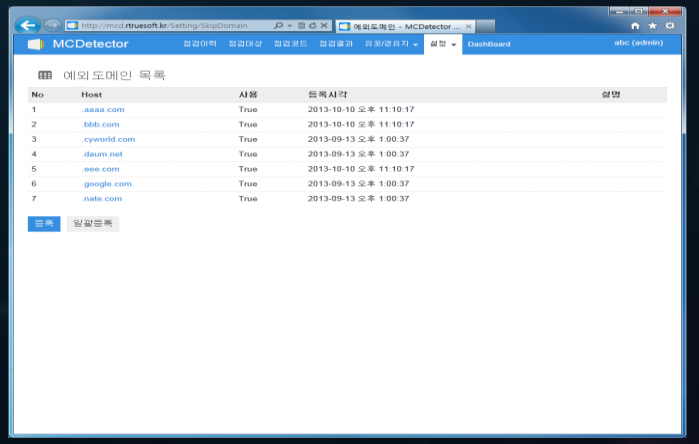
대시보드



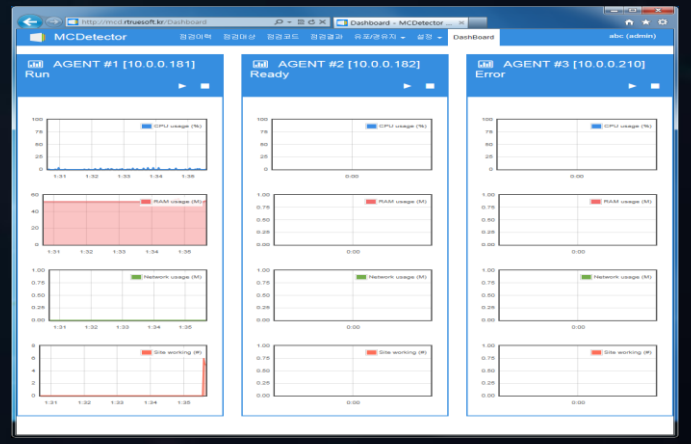
유포지 목록



경유지 목록



예외 도메인 등록

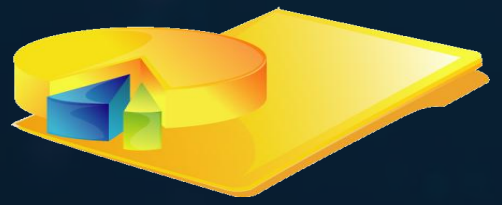


에이전트 상태 모니터링

도입 효과

MCDetector 도입으로 대용량 홈페이지와 하위 페이지까지 정확하게 악성코드를 탐지하고, 탐지 결과를 분석·조치 및 보안장비 연동에 활용할 수 있습니다. 또한 신종 악성코드 대응 기반을 마련하여 다양한 위협에 신속하고 체계적으로 대응할 수 있습니다.

도입 효과	설명 / 세부 내용
국내 최대 홈페이지 점검	대용량 웹사이트도 하루 수백만 URL 스캔 가능, 국내 최대 규모의 악성코드 탐지 환경 제공
하위 페이지 세밀 탐지	홈페이지 하위 페이지까지 탐지하여, 숨겨진 악성코드까지 정확하게 식별 가능
분석 및 조치 지원	탐지 결과를 보고서 형태로 제공하여, 악성코드 제거 및 대응 업무에 즉시 활용 가능
보안장비 연동 및 패턴 등록	타 보안 시스템과 연동 가능, 탐지된 악성코드를 기반으로 패턴 등록하여 다양한 악성코드 탐지 지원
신종 악성코드 대응 기반	기존 패턴에 없는 신종 악성코드도 탐지할 수 있는 분석·대응 체계 마련



MCDetector

악성코드 탐지 솔루션

적용 기관	제품 인증
KISA 한국인터넷진흥원	GOOD Software 굿소프트웨어 인증
금융결제원 금융결제원	

감사합니다

CONTACT : joonir@rtruesoft.kr
TEL : 031-784-8280
HP : 010-6602-5955

ReturnTrue SOFTWARE DEVELOPMENT