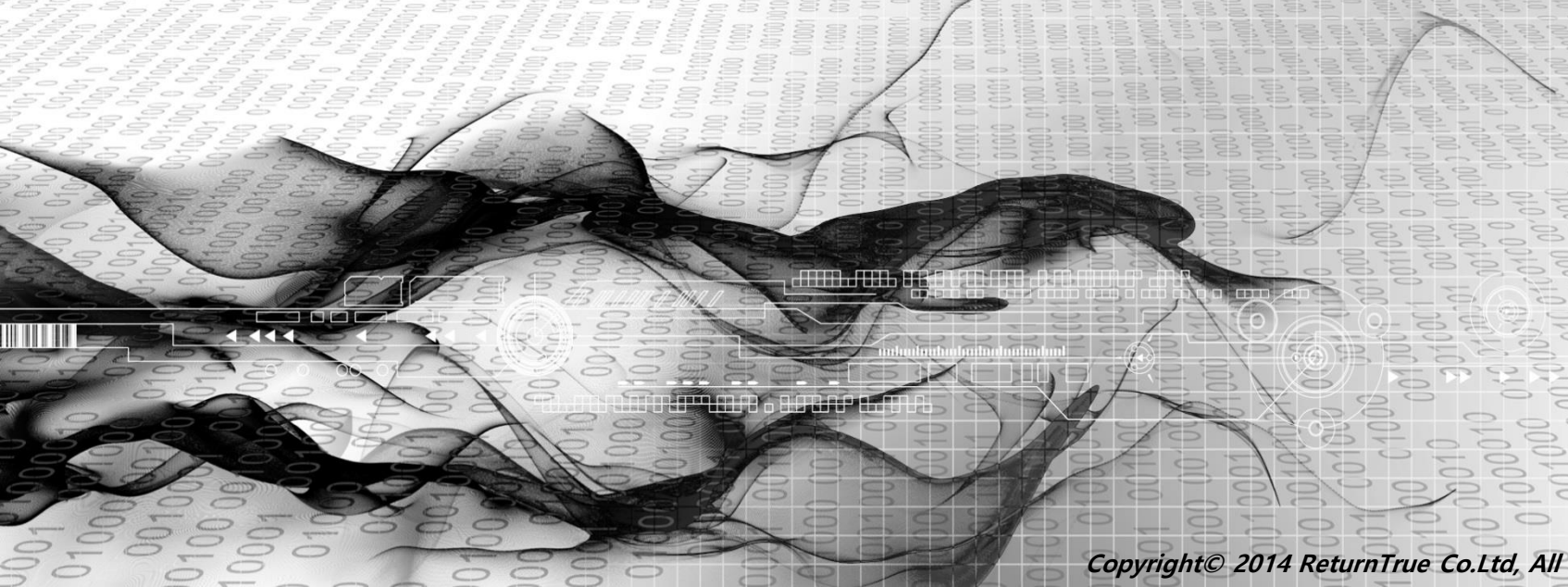
http://www.rtruesoft.kr

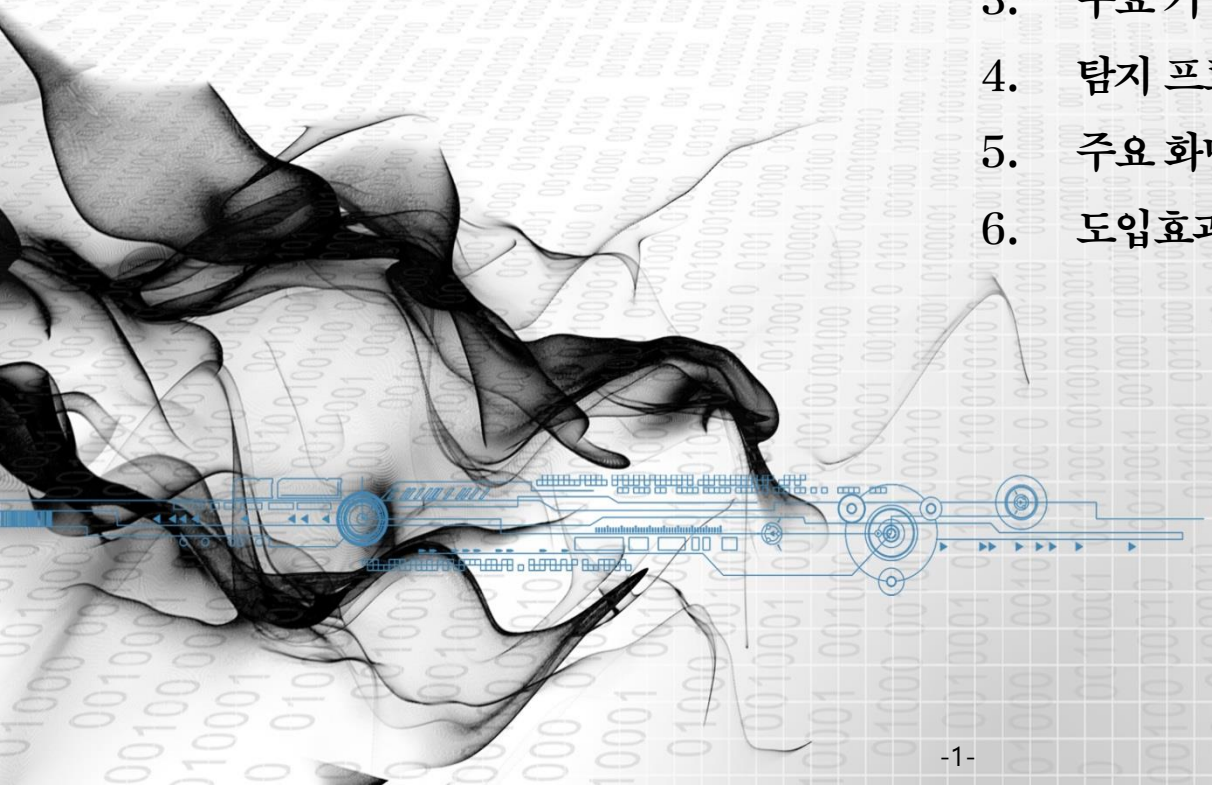
MCDetector

악성코드 탐지 솔루션 제품소개

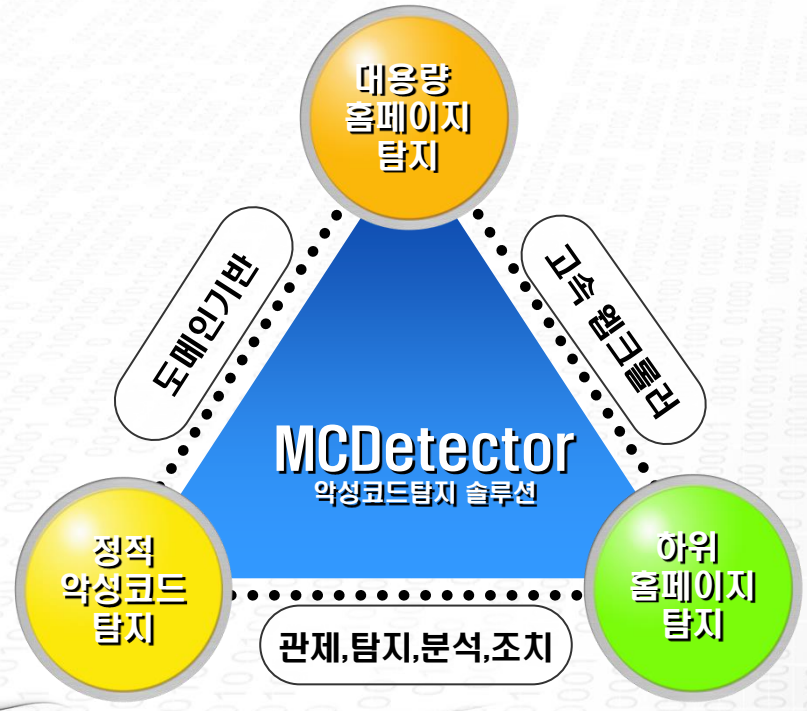


CONTENTS

1. MCDetector 개요
2. 시스템 구성
3. 주요 기능
4. 탐지 프로세스
5. 주요 화면
6. 도입효과



대용량 홈페이지내의 악성코드 점검을 위한 솔루션



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

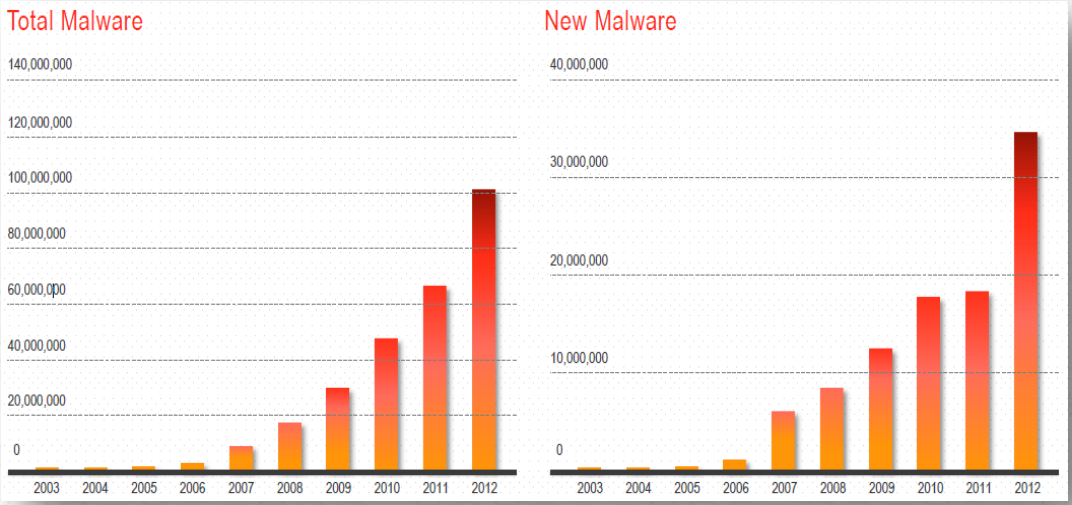
정적 악성코드 탐지

- 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

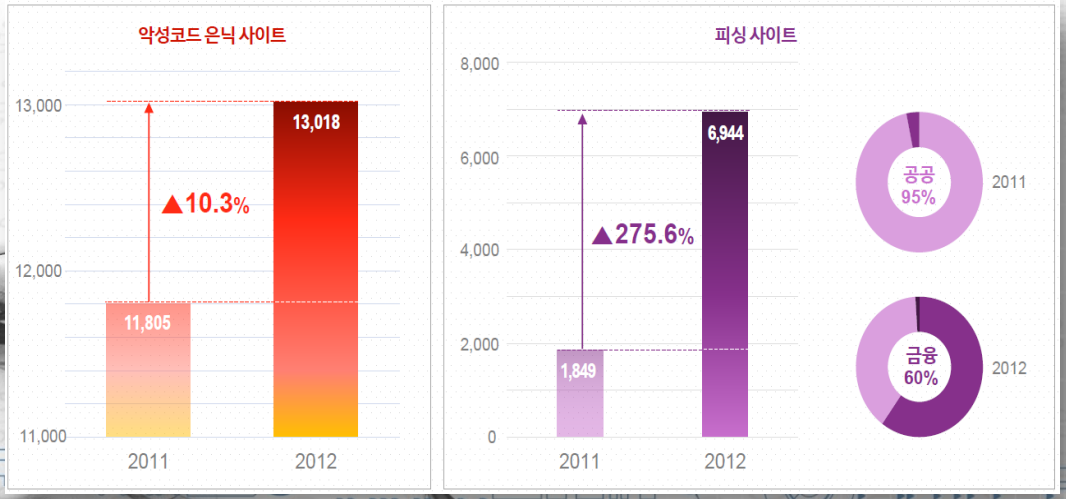
- 고속 웹크롤러를 통한 하위 페이지 탐지
- HTML 및 JavaScript내의 하위 페이지에 대한 링크 추출
- 웹페이지내의 모든 하위 페이지 탐지 가능
- 보안장비(방화벽)등에서 차단에 대한 기술적 대응
- 하위 페이지 탐지에 대한 아키텍처 제공

▼ 2013-2012년 악성코드(Malware) 증가 추이



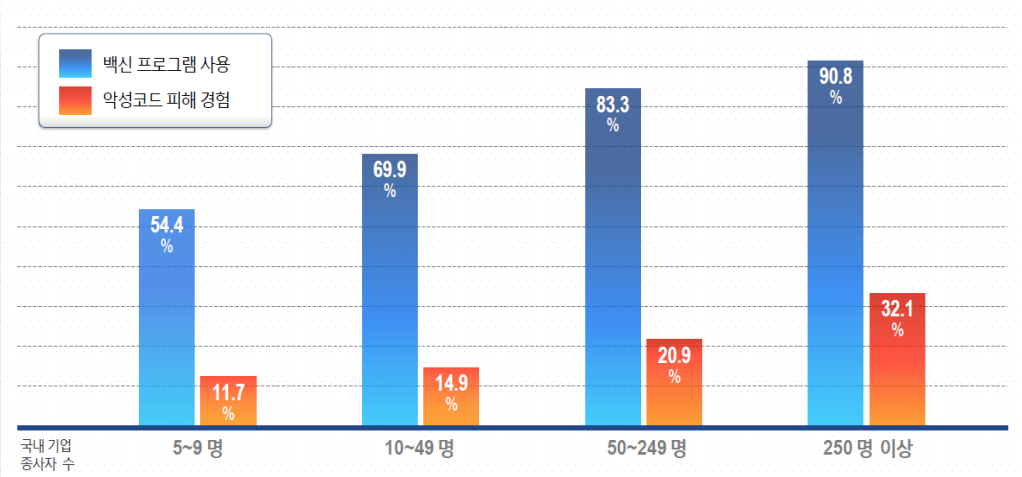
- 국내 악성코드 유포 세계 3위
  - 2013년 하반기 보안동향 리포트 (MS)
- 2013년 한 해 동안 발생되어 탐지된 악성코드 은닉사이트(경유지, 유포지)는 17,750건으로 2012년 대비 36%(13,018건) 증가하였음
- 한국인터넷진흥원에 조사에 따르면 매일 20만여 개의 악성코드가 새롭게 발견

▼ Internet & Security Focus 2013 한국인터넷진흥원



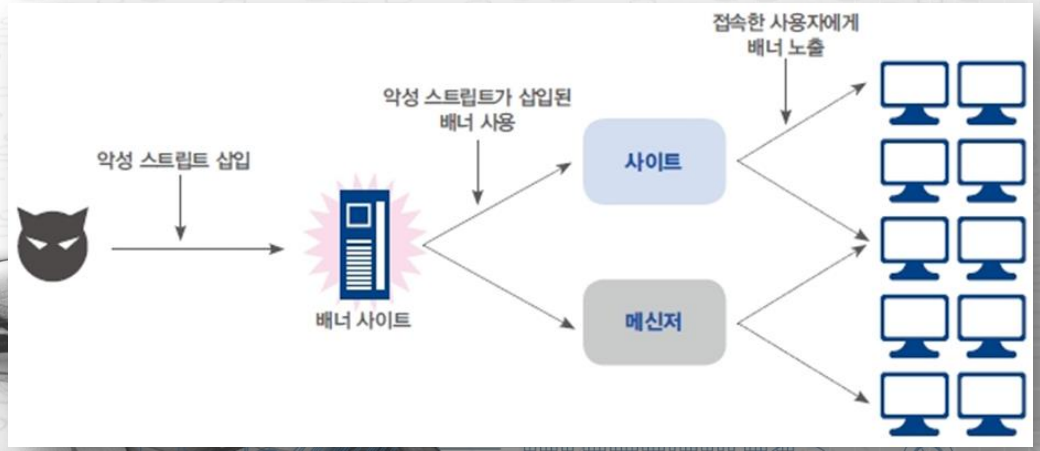
- 2012년 피싱사이트는 2011년 대비 275.6%나 증가 악성코드 은닉사이트도 전년대비 10.3%가 증가

▼ 정보화통계집 2013 (한국정보화진흥원)



- 백신프로그램이 설치된 사용자의 악성코드 피해 경험이 250명 이상일때 32.1%
- 기업 및 기관 내부의 악성코드 탐지만으로는 악성코드에 대한 방어 역부족

▼ 웹사이트를 통한 악성코드 경유 및 유포 감염 개요도



- 해커의 입장에서는 배너광고를 제공하는 사이트를 해킹한 후 악성코드(악성코드를 다운로드할 수 있는 링크)를 삽입하는 방법은 악성코드 배포 효율성 측면에서 가장 좋은 방법 중 하나
- 2013년 5월 발견된 악성코드 유포 사이트들의 경로를 살펴보면 배너광고를 통해서 악성코드가 유포됐음을 확인할 수 있었음

기하급수적인 악성코드 증가

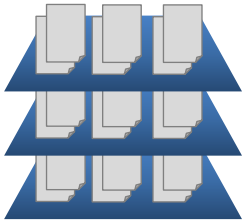
- 매일 20만여 개의 악성코드가 새롭게 발견(한국인터넷진흥원)
- 악성코드 은닉사이트 매년 10% 이상 증가

구분	2012년 합계	2013년											
		1월	2월	3월	4월	5월	6월	7월	8월	9월	10월	11월	12월	'13년 합계
유포지	3,270	353	208	355	397	429	527	415	508	466	256	318	240	4,472
경유지	9,748	1,197	785	1,489	1,189	2,535	2,029	706	556	690	424	479	1,199	13,278
합계	13,018	1,550	993	1,844	1,586	2,964	2,556	1,121	1,064	1,156	680	797	1,439	17,750

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)

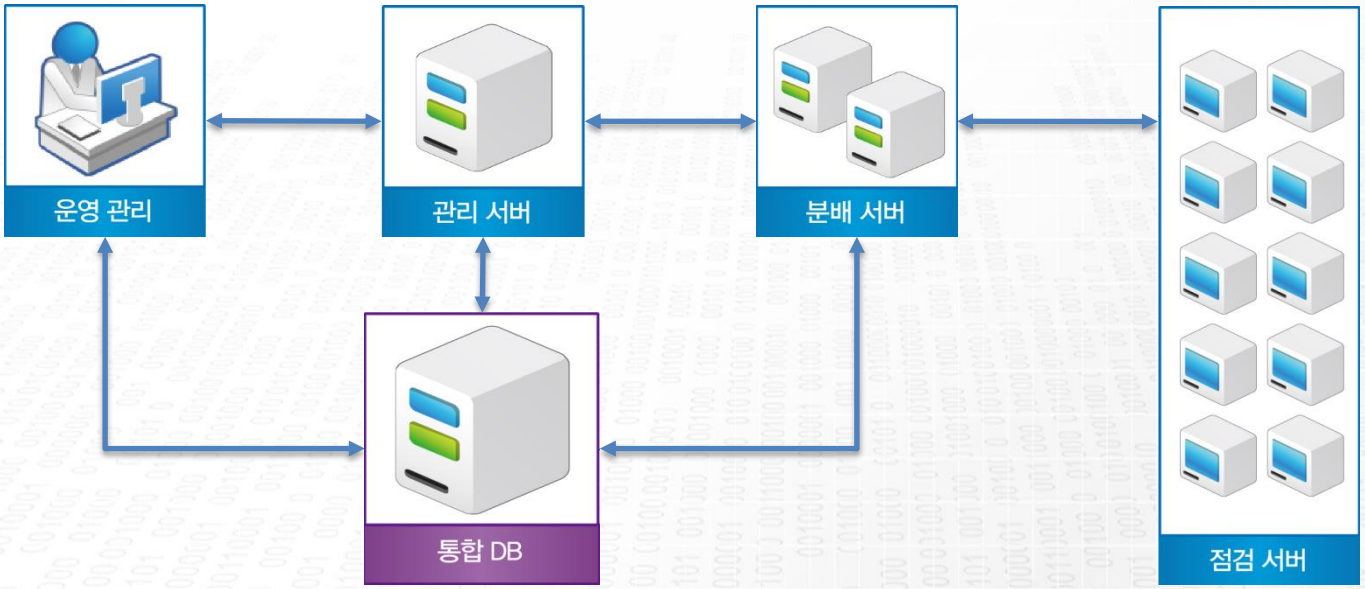
점검대상의 최대화



- 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



- 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

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

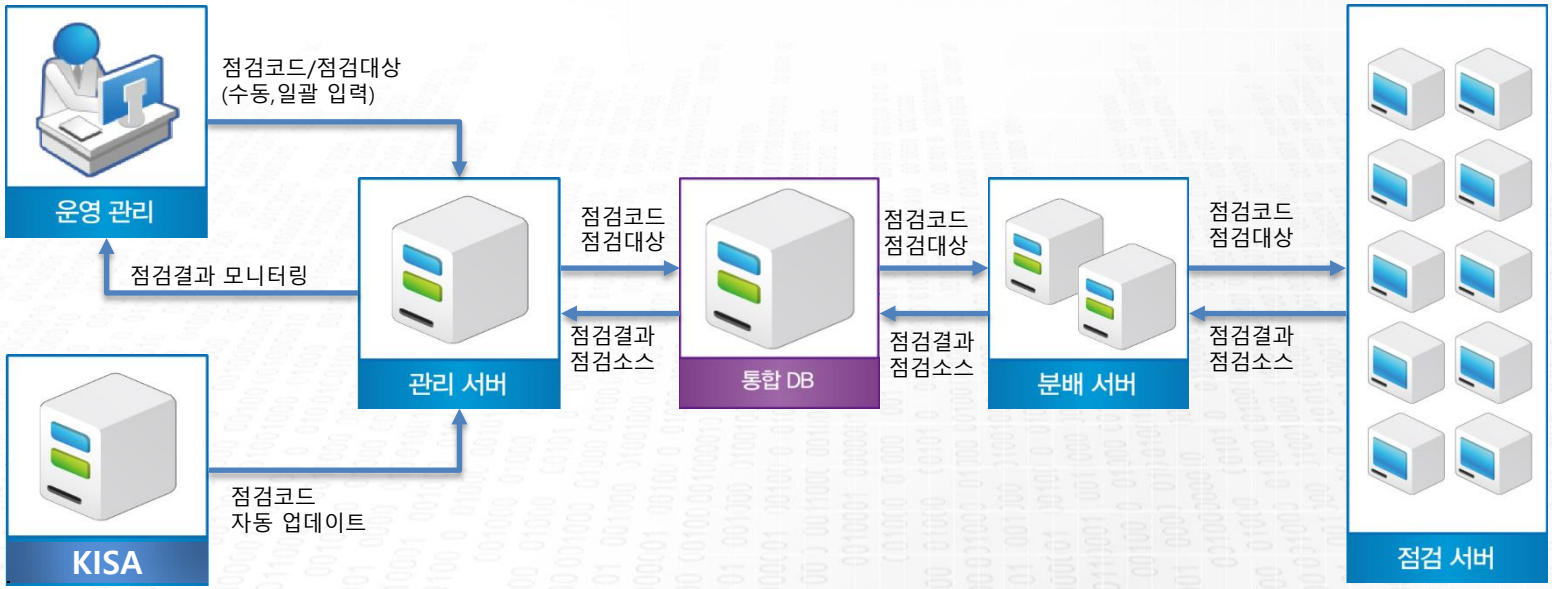
- **점검/분배/관리 Software는 install 형태로 지원**
- **H/W 사양은 점검대상 및 점검주기에 따라 변경 가능**
- **스팩은 권고 사양임**

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

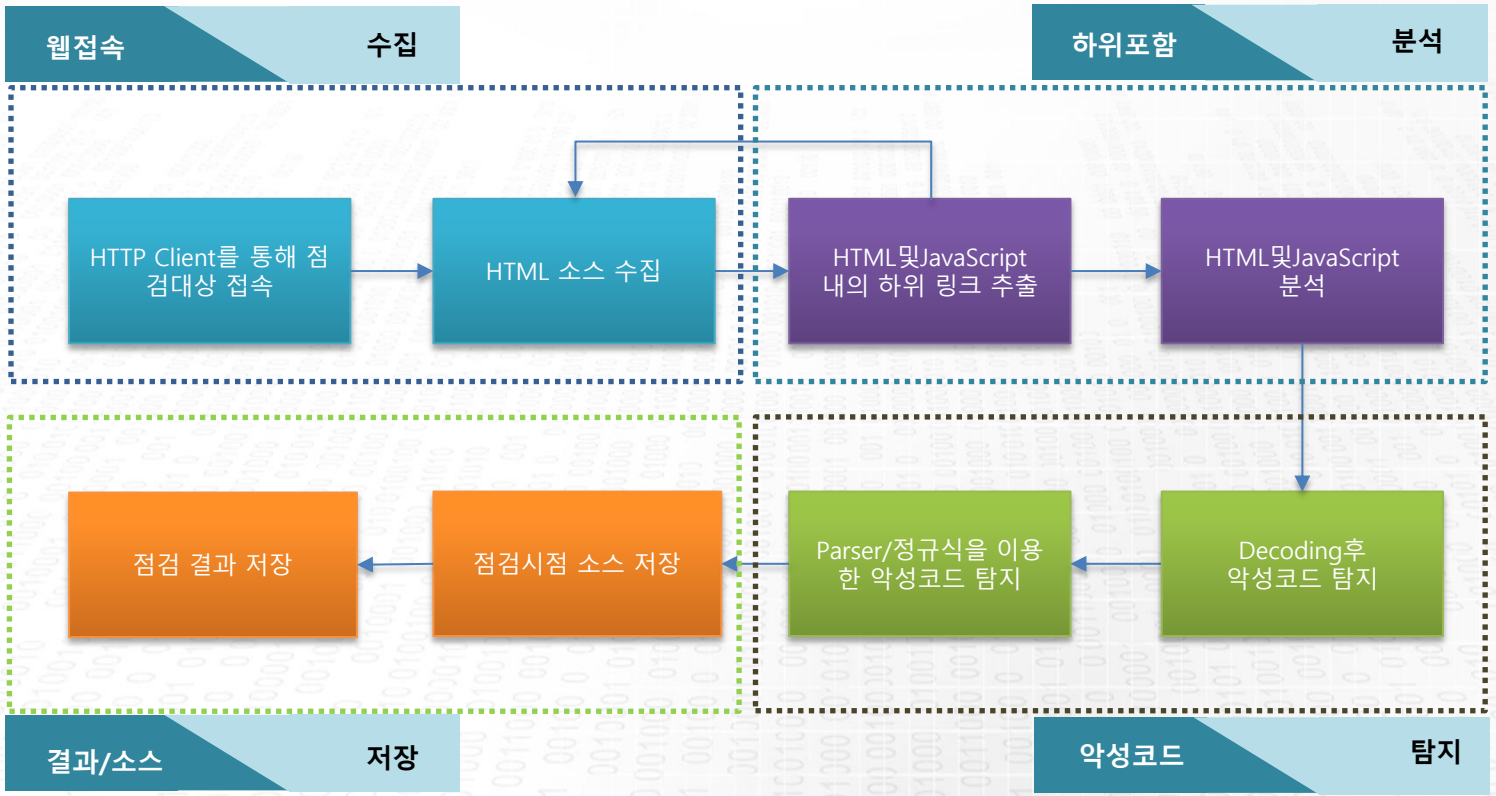
- **권고 H/W(5식) : 1일 500만 이상 URL 탐지**
  - **점검서버 (2식)**
  - **분배서버 (1식)**
  - **관리서버 (1식)**
  - **DB서버 (1식)**

- ***점검서버 1대 기준 1일 250만개 이상의 URL 탐지 (서버 스팩에 유동적)***
- ***하위 페이지 설정기준까지 탐지***
- ***점검코드 자동 업데이트***
- ***악성파일 탐지 가능(EXE,CAB,DLL,APK 등)***

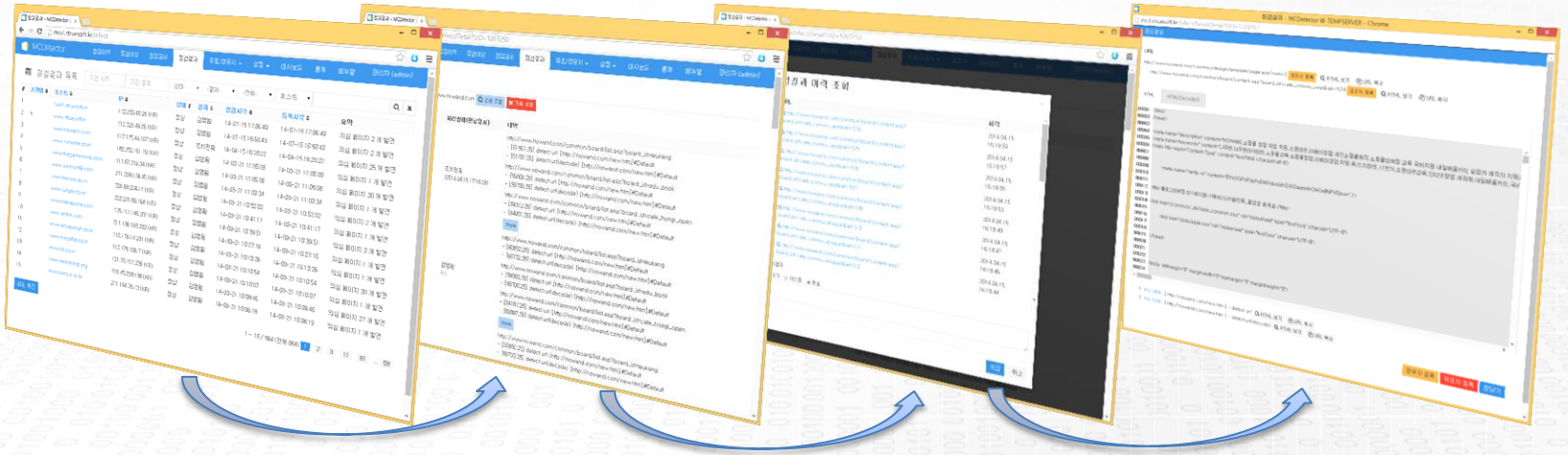
서버	주요 기능	기능 설명
점검 서버	HTML 문서수집 웹크롤러 기능	HTML 분석 (2 Depth이상의 하위페이지 수집)
	악성코드 유포지/경유지 자동 탐지기능	패턴 매칭, 난독화, Decoding을 통한 유포/경유지 자동 탐지
	악성코드 다운로드 기능	파일 다운로드후 악성코드 감염 여부 탐지 기능
	악성코드 URL 링크구조 추출	악성코드 URL 링크구조 추출
	난독화 페이지 및 Encoding 페이지 추출	Encoding 페이지 추출
분배 서버	점검대상 도메인 분배	효율적인 점검을 위한 점검서버별 도메인 분배
	경유지/유포지 결과 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



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



점검결과 목록

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

점검결과 대상 클릭시

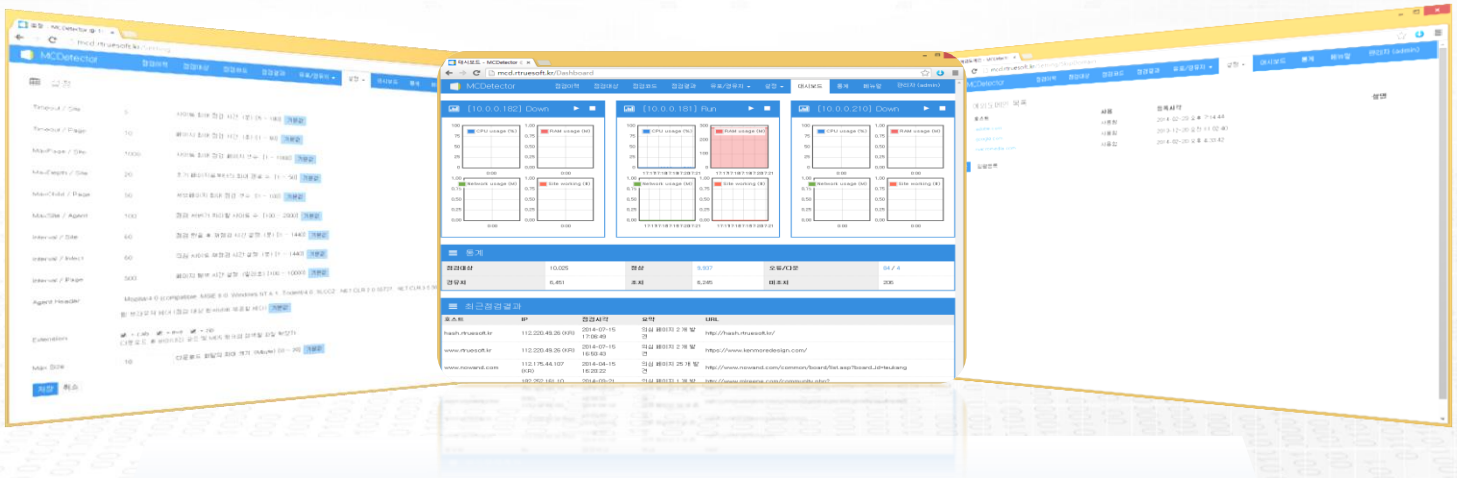
- 조회된 점검결과
- 점검대상에 대해 시간별 점검결과, 처리상태, 내역을 보여줌
- 사이트별 점검시점에 악성코드 은닉여부 판별

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



기능 설정

- Timeout/Site
- Timeout/Page
- MaxPage/Site
- MaxDepth/Site
- MaxChild/Site
- etc

대시보드

- 점검서버별 상태
- CPU
- MEM
- Network
- Site Working
- 최근결과

통계

- 점검대상
- 경유지
- 오류/다운
- 일/월/년 통계
- 기간별 통계
- etc

예외 도메인

- 점검시 제외
- 관심 도메인 제공
- 악성코드 자동 업데이트 제공

- 대용량 홈페이지에 대한 악성코드 탐지를 통한 **국내 최대 홈페이지 점검**
- 하위 페이지 탐지를 통한 **정확하고 세밀한 탐지**
- 분석 및 조치 업무를 위한 **점검결과 활용**
- 보안장비 연동 및 패턴 등록을 통한 **다양한 악성코드 탐지**
- 신종 악성코드에 대한 **대응기반 마련**

적용 기관

KISA
한국인터넷진흥원

금융결제원
금융결제원

제품 인증

GOOD Software
굿소프트웨어 인증

감사합니다

CONTACT : 이상준 대표
joonir@rtruesoft.kr
TEL : 031-291-6092
HP : 018-602-5955

ReturnTrue SOFTWARE DEVELOPMENT