openbase

TARGOS

where the intelligence works 오픈베이스

위협정보 공유 및 관리 시스템

www.openbase.co.kr

TARGOS

APT탐지시스템과 연동되는 악성파일 표준 판별 체계 도입

이제 TARGOS로 구축하세요 !

위협정보 공유 체계



주요 기능

■ 배포 기관 연계시스템과 연동

- 모든 연계 시스템 표준 API 지원
- HTTPS 암호화 통신

■ 탐지 규칙 수신

- 주기적으로 탐지 규칙 업데이트
- 탐지 규칙을 샌드박스에 적용
- 탐지 결과 수집(주기적, event 발생 시)

■ 탐지 결과 송신

- 주기적으로 탐지 결과 전송
- 탐지 결과 응답(VirusTotal, MD5 등) 결과 수신

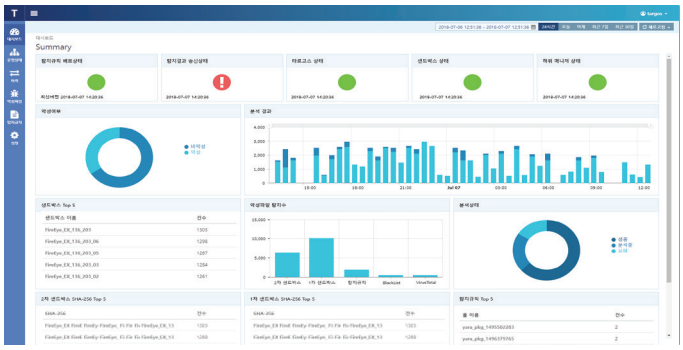
■ 탐지 결과 모니터링

- 샌드박스 탐지 결과 조회
- 배포 기관 전송 탐지 결과 조회
- 탐지 결과 응답 (Virus Total, MD5 등) 조회

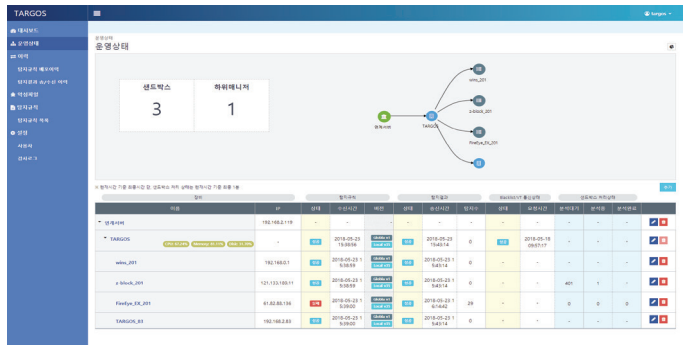
■ 대시보드

- 악성파일, 발신자, 탐지 결과 Top N 정보제공
- E-Mail 도메인 기준 탐지 결과 조회
- 장비 상태 모니터링

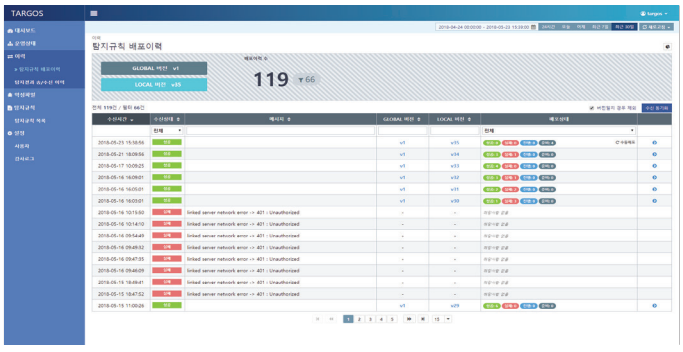
위협정보 공유 체계



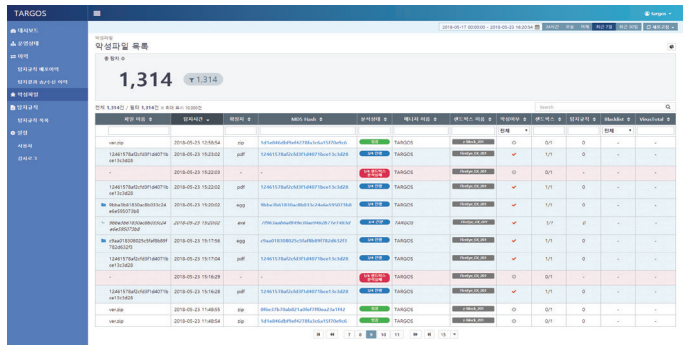
TARGOS 대시보드



TARGOS 운영상태



TARGOS 탐지규칙 배포이력



TARGOS 악성파일







구분	TARGOS S/W	TARGOS Appliance	
Model	나라장터 종합쇼핑몰 등록 (Appliance 제공 가능)	TSX2000	TSX5500
CPU	Intel 4Core x 1	Intel 4Core x 1	Intel 8Core x 2
Memory	32GB	32GB	128GB
HDD	500GB x 1	SSD 256GB x 2 SATA 500GB x 2	SSD 80GB x 2 SATA 1TB x 2
RAID	-	RAID(H/W)	RAID(H/W)
NIC	Intel 10/100/1000 x 1	Intel 10/100/1000 x 2	Intel 10GB x 2
Size(HxWxD In)	-	1.75 x 17.24 x 21.8	3.44 x 16.93 x 27.95
Stack	-	1U	2U
Power	-	AC/DC 750W x 1	AC/DC 1100W x 2
지원 샌드박스 수	별도협의	5	10

*TARGOS S/W : 최소사양



서울특별시 서초구 매헌로 16 하이브랜드빌딩 4층 (우)06771
TEL 02.3404.5700 FAX 02.3452.3654 E-Mail systemsales@openbase.co.kr

제작 : 2018년 7월