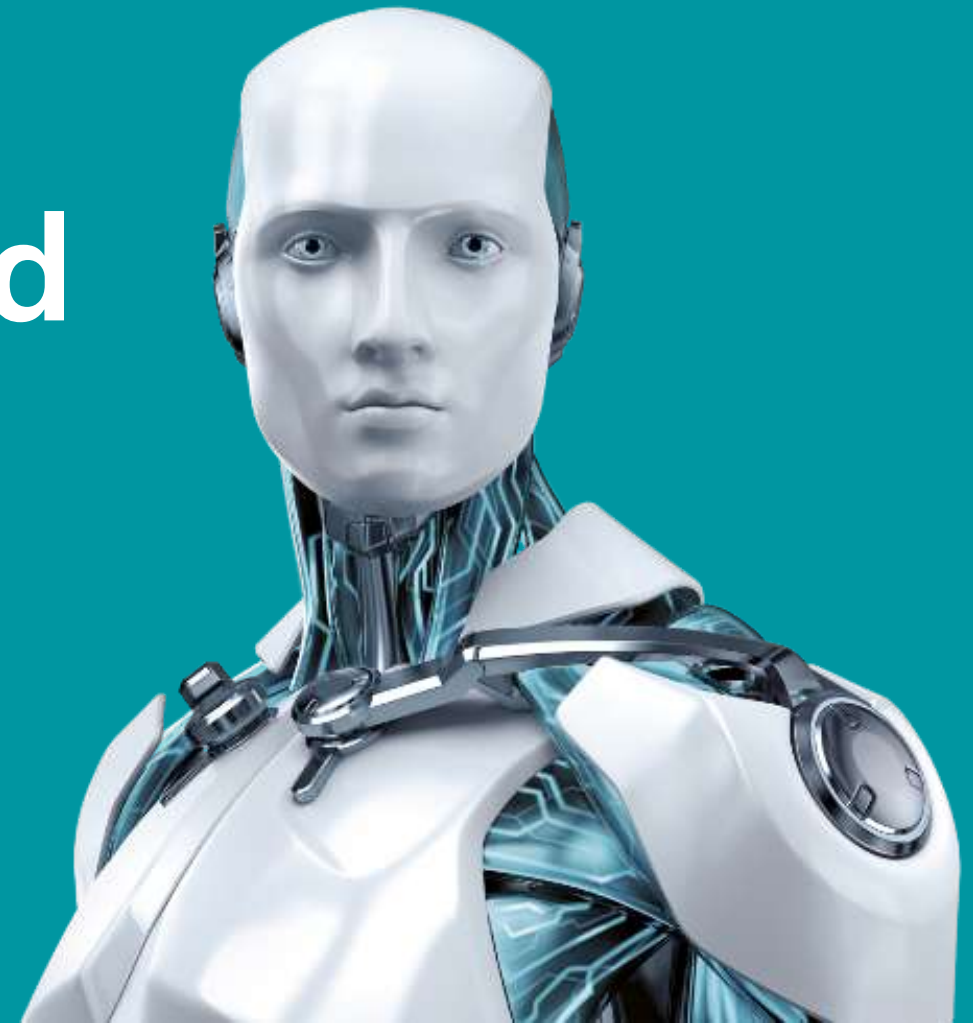
Digital Security
Progress. Protected.

ESET LiveGuard Advanced

클라우드 샌드박스 서비스



Index

Digital Security
Progress. Protected.

제안 배경

HOME > 뉴스 > 보안

“랜섬웨어, 타깃 맞춤형 공격으로 수익률 높인다”

*** 기자 | 승인 2021.01.11 10:37 | 댓글 0

공격 추이를 살펴보면, 10월과 11월 다소 증가하다 12월 다소 줄어들었다. 랜섬웨어는 2018년 3분기부터 꾸준히 감소하는 추세를 보이고 있지만, APT 공격과 결합해 피해규모는 크게 늘어나고 있는 것으로 보인다. 일례로 지난해 국내 유통기업을 대상으로 한 클롭 랜섬웨어는 사전에 기업 내부 시스템을 조사해 맞춤형 악성 파일을 공격에 사용했으며, 파일 확장명을 변경하는 이전 변종과 달리 원본 파일명을 그대로 사용해 피해자의 의심을 피하는 등 고도화된 수법을 사용했다.

- **시스템 다운으로 인한 업무 불가**
- **생산라인 다운으로 인한 막대한 손실**
- **내부 중요 정보 유출 발생**

출처 : 데일리넷 IT 정보마당
https://www.datanet.co.kr/news/articleView.html?idxno=154924

WHY ELA?

필요성		ESET LiveGuard Advaned
 최신 악성파일에 대한 방어	→	샌드박스를 통한 최신 악성파일 발견
 AI 머신러닝 등 최신 기술 필요	→	AI 머신러닝 탑재, 제로데이 위협 탐지
 보안/전산 인력 부족	→	ESET 중앙관리를 통한 통합 관리
 고가의 APT 제품	→	클라우드 샌드박스를 이용한 낮은 비용

WHY ELA?

어플라이언스
(장비형태)

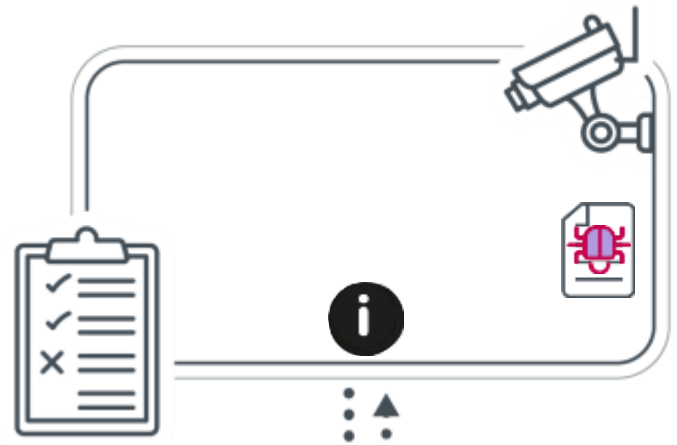
- 높은 비용
- 전담 엔지니어(분석가) 필요
- 차단을 위한
  추가 솔루션 필요
- 추가 에이전트 설치
- 장비에 대한 유지보수 필요

클라우드 기반 샌드박싱 기술을 이용한
ESET LiveGuard Advanced

ESET
Live Guard
Advanced

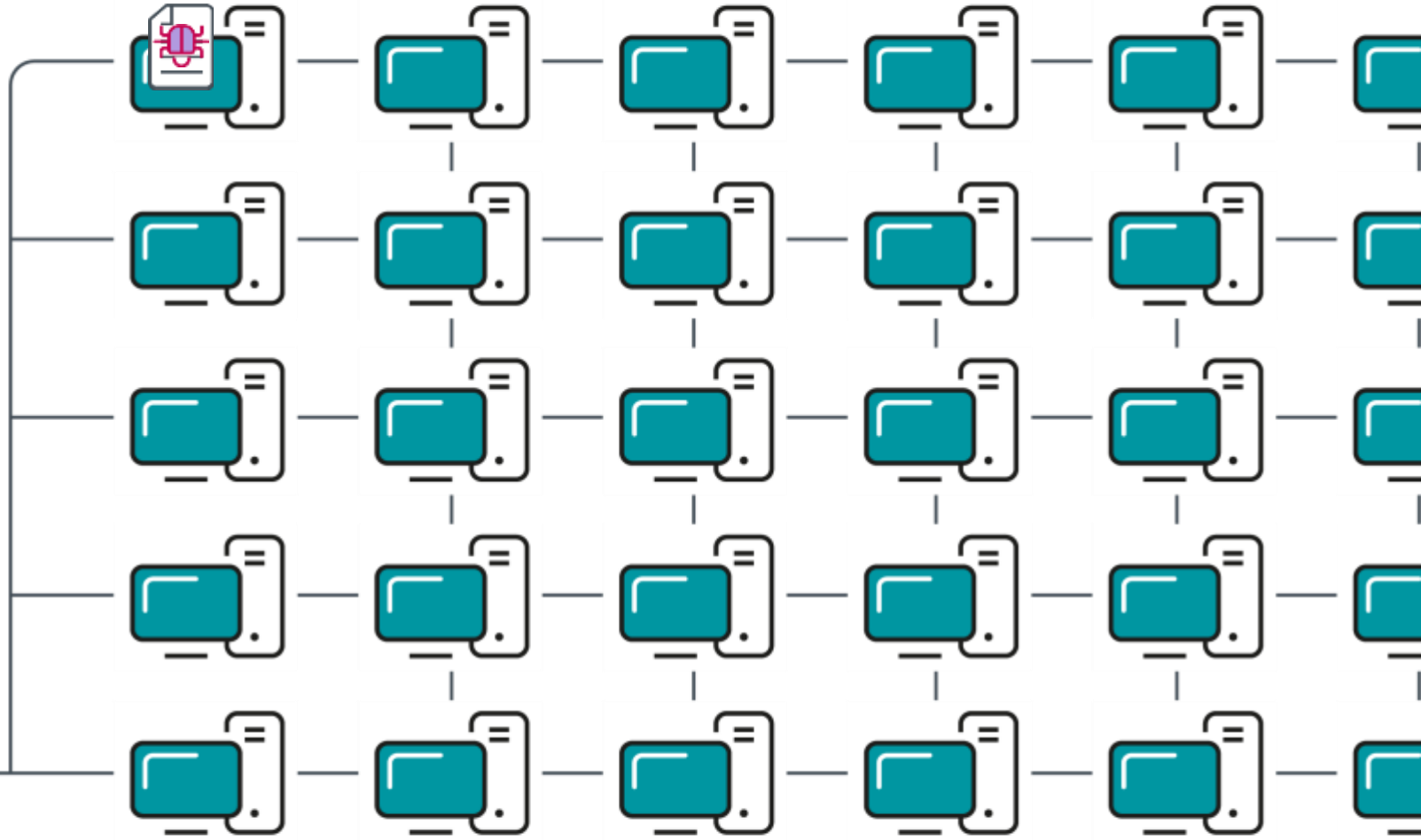
- AI 머신 러닝
- 랜섬웨어 보호
- Zero-day 위협 탐지
- 자동 보호
- High End 솔루션보다 낮은 비용
- 백신에 포함되어 있어 추가
  에이전트 설치 불필요

ESET LiveGuard Advanced (ELA)



ESET PROTECT
(중앙관리)

Threat



Endpoints

ELA 소개 (ESET PROTECT with ELA)

고급 검사 엔진

고급 압축 해제 및 검사

샘플이 정적 분석 및 최첨단 압축 해제 과정을 거친 후 강화된 위협 DB와 대조됩니다.

샘플이 깨끗합니다.

고급 머신 러닝 탐지

정적/동적 분석이 딥 러닝을 포함한 수많은 머신 러닝 알고리즘에 의해 수행됩니다.

샘플이 깨끗합니다.

동작 분석 샌드박스

실험적 탐지 엔진

샘플이 실물 크기의 사용자 장치와 매우 유사한 "스테로이드의 샌드박스"에 삽입되며, 이후에 악의적인 동작의 징후가 있는지 모니터링됩니다.

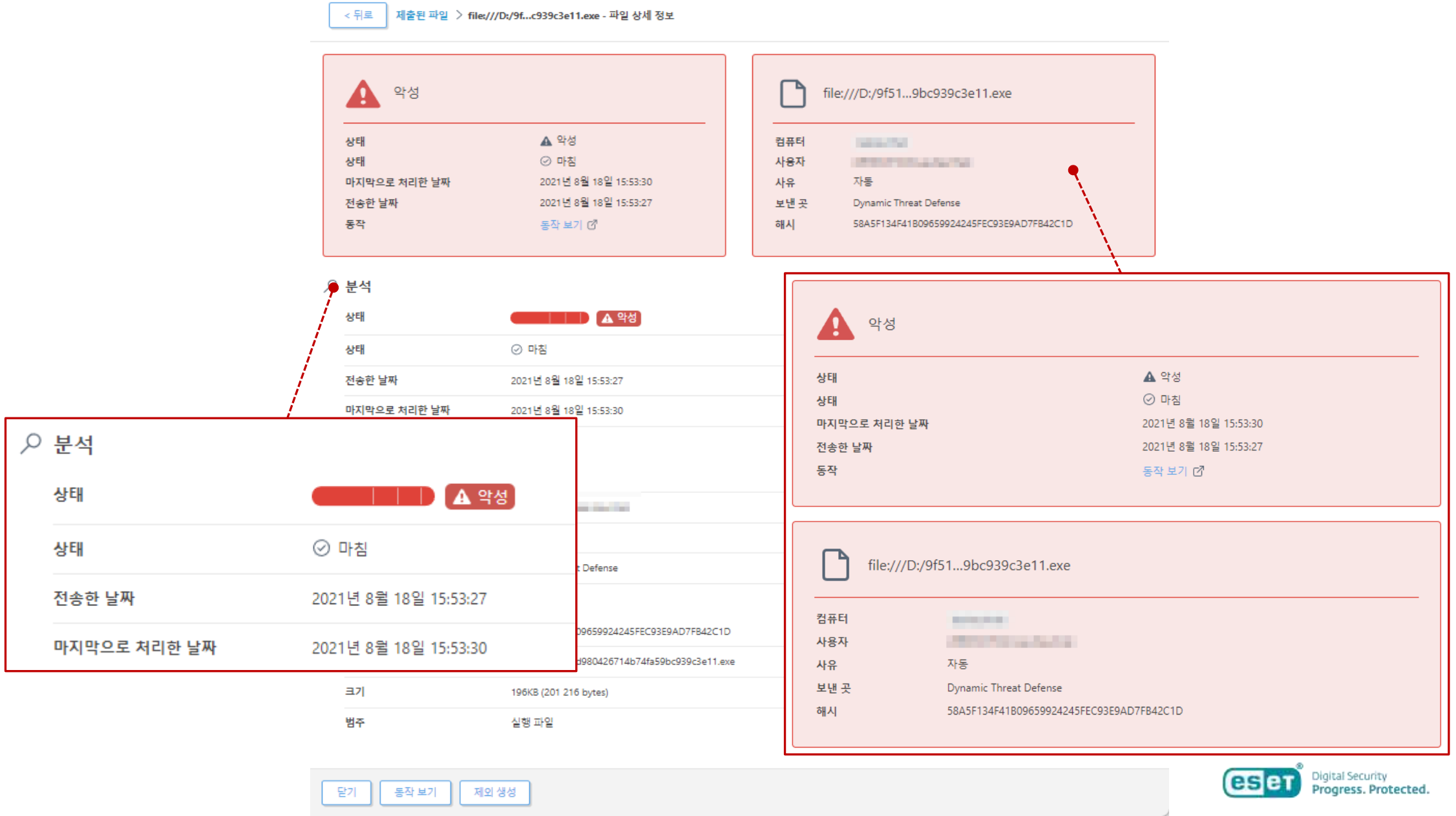
샘플이 깨끗합니다.

상세 동작 분석

모든 샌드박스 출력이 알려진 악성 패턴과 일련의 동작을 식별하는 상세 동작 분석의 대상입니다.

이 샘플에 필요하지 않음

ELA 소개 (ESET PROTECT with ELA)



ELA 소개 (ESET PROTECT with ELA - 보고서)

악의적

SHA-1 58A5F134F41B09659924245FEC93E9AD7FB42C1D

범주 실행 파일

분석된 동작

맬웨어가 실행되지 않고 탐지됨

샘플이 실행되지 않고 악의적인 것으로 검색되었습니다.

악의적 원인

ESET 검사 엔진을 통해 실행 없이 맬웨어가 검색되었습니다.

일반적 원인

정상적인 애플리케이션은 이러한 통신을 수행하지 않습니다.

✕ 샘플이 자체적으로 제거되었습니다	동작이 탐지되지 않음
✕ 안티바이러스 상호 작용	동작이 탐지되지 않음
✕ 감염 의심 암호화 작업	동작이 탐지되지 않음
✕ 바로 가기 키 등록	동작이 탐지되지 않음
✕ 부트 영역 수정	동작이 탐지되지 않음

✕ 머신 러닝 탐지	동작이 탐지되지 않음
✕ Fileless 위협	동작이 탐지되지 않음
✕ 권한 상승	동작이 탐지되지 않음
✕ Windows 폴더에 파일이 생성됨	동작이 탐지되지 않음

ELA 소개 - 장점

신종 위협에 대한 빠른 대응

추가 장비 또는
에이전트 설치 불필요
(ESET 제품에 포함)

선제적 보호
(자동 위협 분석 및 대응)

감사합니다.

- ESET –

세상에서 가장 가볍고 빠르고 정확한 백신!!

관리가 쉽고 간단합니다.

Address : 서울시 송파구 송파대로 167, A동 521. 522호
Tel : 1899-8352 | 02-567-0510
Fax : 02-402-8352
기술 문의 : tech@estc.co.kr
웹 사 이 트 : www.estc.co.kr