APT대응 **보안솔루션**

ZombieZERO **EDR**

NPCORE

신변종 악성코드 탐지/차단

CONTENT

1 보안현황

01 증가되는 사이버 공격

코로나19 이후
재택/원격 근무 증가로 인하여
악성코드 공격 증가

2억개
신종 **멀웨어**
2020년
Sonicwall발표

39초마다
해킹시도
메릴랜드대 보고서
2020년

매일4천건
랜섬웨어 **공격**
2019년

43%만
백신으로 **방어**
2019년

정보 보안의 최대 위협 APT (Advanced Persistent Threat)

해커가 다양한 보안 위협을 특정 기업이나 조직의 네트워크에 지속적으로 가하는 공격.
알려지지 않은 신/변종 악성코드. **고유 패턴이나 방식이 없는 비정상 행위의 공격.**
(Ransomware / Backdoor / Bootkit / Exploit 등)

백신과 같은 안티바이러스는 시그니처 기반의 패턴 매칭 방식으로
보유한 정보에 의존하여 알려진 악성코드에만 대응하기 때문에
APT 및 신변종 악성코드의 위협 대응이 어려움

02 지능형 위협 공격

최근 APT 공격의 목표는 내부 데이터에 접근,
정보를 탈취하거나 랜섬웨어 감염으로
금전적 보상 요구

APT 공격 예시

알려진 악성코드		알려지지않은 악성코드(APT)
공격분포	무차별 대량 살포	**치밀하고 조직화된 계획**
목표율	무작위 다수	**정부기관, 단체, 기업**
공격빈도	일회성	**지속성**
공격기술	기본적인 악성코드 디자인	Ransomeware / Bootkit / Backdoor 등
탐지율	샘플 발견시 99% 탐지룰 작성	**샘플이 발견되어도 10% 탐지룰 작성 (변종이 다양함)**

주요 공격대상	
정부기관	기밀문서 탈취, 시스템 작동 불능
정보통신	첨단 기술자산 탈취,원천 기술 관련 기밀 탈취
제조기업	기업 지적 자산 및 영업 정보 탈취
금융기업	금융 시스템 작동 불능, 기업 금융 자산 정보 탈취

CONTENT

2 좀비제로

NPCORE

01 제품 개요

ZombieZERO EDR

APT 및 신/변종 악성코드에 대응하는 Endpoint 전용 보안 솔루션

1 위치
사용자 구간(PC/서버) 에이전트 형태로 설치

2 APT / 랜섬웨어 대응
단말의 파일 암호화 및 위변조 탐지/차단

3 ZeroTrust 보안
검증되지 않은 프로그램 실행보류 / 분석

4 IOC 침해지표 분석
침해지표에 따른 탐지 및 가시화 제공

5 실시간 순간 백업
파일 위협 감지시 실시간 순간 백업

6 구축 형태
온프레미스 / 클라우드 2가지 선택 가능

01 제품 개요

- Manager 서버와 연동하여 악성코드를 탐지 / 차단
- 온프레미스 / 클라우드 2가지 방식으로 구축 가능

ZombieZERO Manager

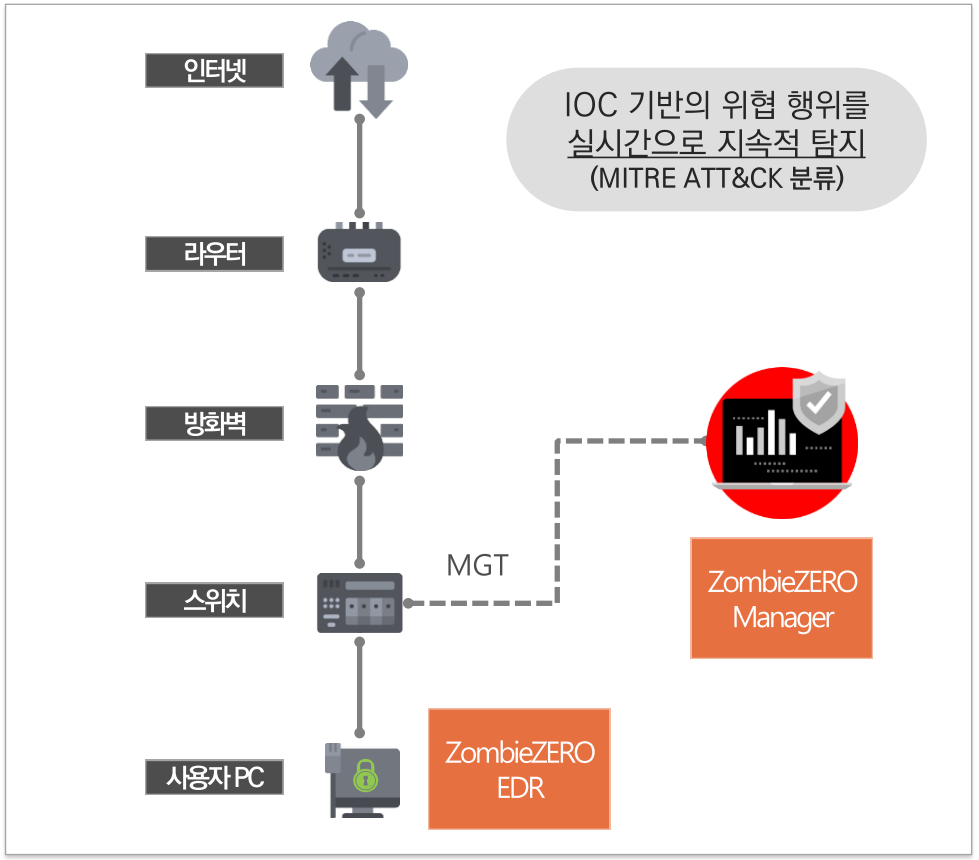
- 엔드포인트 에이전트 관리
- 보안정책 관리 및 배포
- 악성 실행파일 수집 및 정밀분석
- Virtual Machine Sandbox 생성 / 관리
- Yara Rule 업데이트 관리
- 국내 · 외 사이버위협 침해지표(Indicator of Compromise) 수집

ZombieZERO EDR

- 사용자 PC 악성 프로세스 실시간 감시
- 악성 실행파일 탐지 및 차단
- 파일 훼손(Ransomware) 대비 파일 백업/복구
- 매니저 서버 정책에 의한 사용자 PC 보안위협 통제
- 기타 악성코드 관련 아티팩트 실시간 수집

01 제품 개요

- Endpoint(사용자PC)단에서 APT 및 신변종 악성코드를 탐지/차단
- 랜섬웨어 / 백신 등 다양한 보안 솔루션으로의 확장 운영 가능



1. 사용자 PC에 신규 파일 유입 및 실행
2. ZeroTrust 보안 기능을 통한 실행보류
3. 파일 정보를 분석 서버로 업로드
   (*전체 파일 아님. 정보 유출 위험 없음)
4. 4단계 체계적 파일 분석 진행
5. 분석 결과 정책 배포
6. 정상 파일 경우 파일 실행
   악성 파일 경우 차단 / 격리

02 주요 특징 – 단말 집중 보안

- 단말단에서 발생 되는 **랜섬웨어 행위 탐지/차단**
- **실행보류** 기능을 통해 검증된 파일만 실행 및 Bitdefender의 AV 기능 지원

랜섬웨어 행위 탐지/차단

실시간 랜섬웨어 행위를 탐지하며 차단
파일 암호화 및 위변조 대응

ZeroTrust 보안

신규 파일의 유입 또는 위협 파일 실행 시
파일의 실행을 보류하여 분석 서버로 정보 업로드

Bitdefender의 AV 기능

글로벌 백신 Bitdefender의 AV 기능 지원
악성코드의 신속한 사전 탐지

02 주요 특징 – 실시간 순간 백업

- 파일 변조 직전의 순간, 일반 프로세스가 접근 할 수 없는 보안 폴더에 파일 백업
- 커널 드라이버단에서의 백업 실행으로 어플리케이션간 충돌 이슈와 성능 저하 없음

실시간 순간 백업

EDR은 악성코드를 사전에 탐지/차단하는 보안솔루션 이지만,
순간 백업 기능을 통하여 더욱 완벽한 정보 보안을 제공함

02 주요 특징 – IOC 침해 지표 탐지

- IOC 최신 인텔리전스 적용을 통한 **상시 위협 탐지**
- 사용자 단말의 네트워크, 파일, 프로세스, 레지스트리 행위에 대한 **IOC 침해지표 탐지**

타입 : Process

이벤트 : Create
Parent-PID : 2068
Parent-경로 : C:\Windows\System32\svchost.exe
Parent-MD5 : f586835082f632dc8d9404d83bc16316
PID : 2296
경로 : C:\Program Files (x86)\Google\Update\GoogleUpdate.exe
MD5 : 59ea38acbca05610bfee326da3f2d96b
Params : "C:\Program Files (x86)\Google\Update\GoogleUpdate.exe" /ua /installsource scheduler
Dll Name : null
Thread : null
세션 : A59819EC07998E50C0797171EB280E3C
위험도 :

MITRE	설명	Tactics

타입 : File

PID : 2652
경로 : C:\Users\npcore\Desktop\그램전달\gocleansetup151.exe
MD5 : 96d8c9c4e312607487561c6391508941
이벤트 : Write
파일 : C:\Users\npcore\AppData\Local\Temp\nshCA4C.tmp\UserInfo.dll
세션 : A59819EC07998E50C0797171EB280E3C
위험도 :

MITRE	설명	Tactics
T1204	User Execution	Execution

타입 : Network

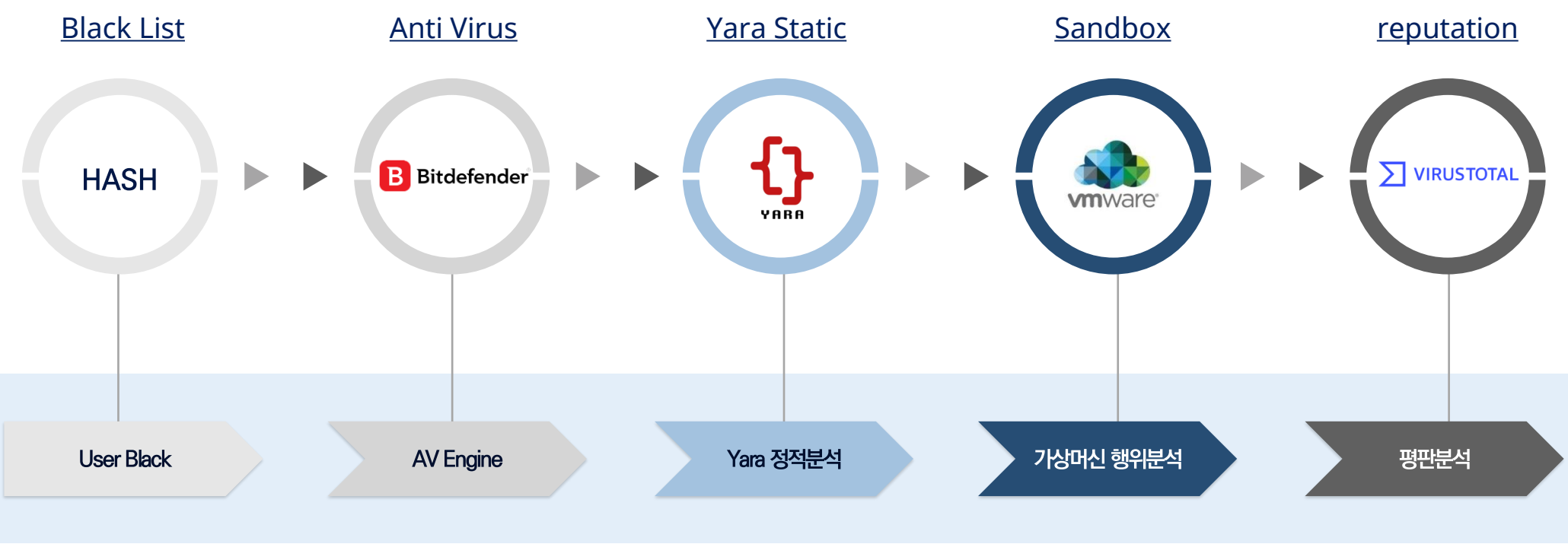
PID : 2560
경로 : C:\Program Files\Google\Chrome\Application\chrome.exe
MD5 : aa2e522a405cb5a295d3502c4ff6ca39
이벤트 : HTTP
URL : www.ten-1097.comwww.ten-1097.com /ajax.jongmok_list.php
IP : 107.154.131.98
포트 : 80
세션 : A59819EC07998E50C0797171EB280E3C
위험도 :

MITRE	설명	Tactics
T1041	Exfiltration Over C2 Channel	Exfiltration

※ IOC 침해지표 탐지 로그

02 주요 특징 – 다차원 분석

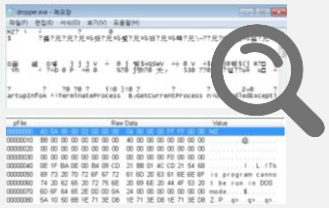
- 시그니처/정적/동적분석 등의 알려지지 않은 악성코드 다차원 분석



02 주요 특징 – 다차원 분석

- Yara Rule 기반 **정적 분석**을 이용한 악성 패턴 탐지
- 사용자 환경과 유사한 가상머신를 이용한 파일 실행 및 **행위 분석**

약 10,000여개 이상의 Yara 비교



정적분석 : 문자 패턴 분석

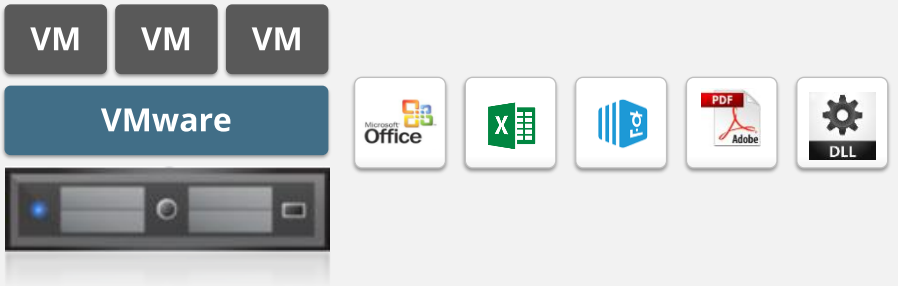
```
rule CEO_Fraud
{
    meta:
        author = "Natalie"
        date = "11/06/2018"
        description = "This is a basic YARA rule for CEO fraud."

    strings:
        $text_a = "wire transfer"
        $text_b = "CEO"
        $hex = { E2 34 A1 C8 23 FB }

    condition:
        $text_a or $text_b or $hex
}
```

Sandbox 안에 해당 어플리케이션 실행

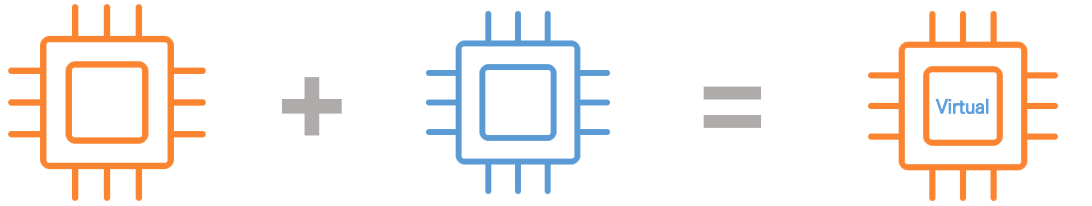
동적분석 : 악성 행위 분석



02 주요 특징 – 가상머신 우회 방지

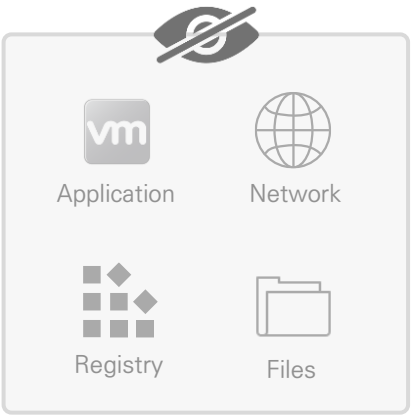
- 적은 비용의 가상머신 구성으로 리얼머신 구성과의 동일 효과 제공
- 가상머신을 우회하는 악성코드의 행위를 유도하여 동적 행위 탐지 분석

가상머신 우회 방지 기술



Real Machine	Virtual	Fake Real Machine
BFEBFBFF000306C3 Physical CPU ID	0FABFBFF000306C3 Running Inside Hypervisor	BFEBFBFF000306C3 Running Inside Real Machine

리얼 머신의 CPU ID 정보로 변경
(EAX/EBX/ECX/EDX)



가상머신 고유정보 숨기기

- 가상머신의 CPU ID 정보를 **리얼 머신의 CPU ID 정보로 변경, 가상머신 고유정보 숨기기** 등의 우회 방지 기술
- 가상머신 우회 방지 기술을 통하여 악성코드는 **가상머신을 리얼 머신으로 인식**하여 악성 행위를 실행

02 주요 특징 – ECSC 공식 연동

- 2018년 부터 MTM(APT)제품군 '적합'판정을 받은 유일한 업체
- 서울/ 경기 / 전남 / 경북 / 대구교육청의 **ECSC 연동 실적 보유**

02 주요 특징 – MITRE ATT&CK 분류

- 표준화된 MITRE ATT&CK 분류에 맞는 악성 코드의 카테고리화 적용
- 악성코드의 공격 방법(전술)에 대해 확인 가능

MITRE

ATT&CK™

Adversarial Tactics, Techniques & Common Knowledge

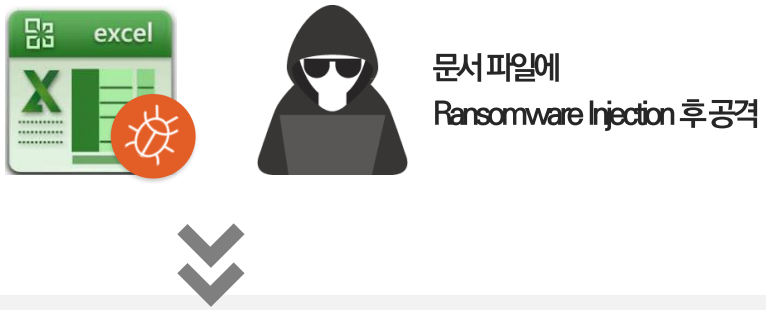
공격의 결과가 아닌
진행 중 공격에 대한 기술 및 방법의 형태 모니터링

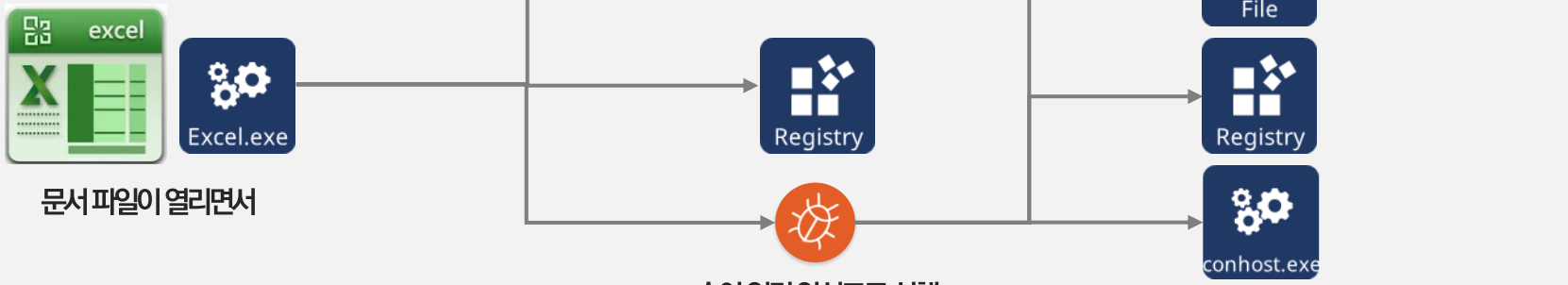
공격형태 분류

RECONNAISSANCE	WEAPONIZATION	DELIVERY	EXPOITATION	INSTALLATION	COMMAND & CONTROL	ACTIONS ON OBJECTIVES
초기 엑세스	실행	영속성	권한 확대	명령 & 통제	유출	타격

02 주요 특징 – 악성코드 공격 형태 분석

- 악성 행위 공격에 대한 흐름도 제공
- 탐지된 근거 정보를 확인 할 수 있는 페이지(링크) 제공



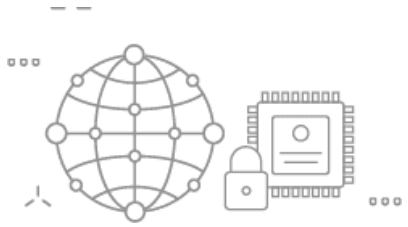


02 주요 특징 – 글로벌 탐지 패턴

- 국내 및 글로벌 패턴 라이브 업데이트 지원
- 위협에 대한 증거 기반의 지식(위협 인텔리전스)를 활용한 대응

Pattern, Rule, Detect, Malware

US	United States	167794
RU	Russian Federation	27473
DE	Germany	21267
GB	United Kingdom	12870
NL	Netherlands	12173
CN	China	11903
CA	Canada	7494
JP	Japan	7402
FR	France	5916
RO	Romania	5255



MALSHARE | Bitdefender | VirusShare | SHODAN | VIRUSTOTAL

Spyse | VirusSign | c-tas 위협정보 종합분석 | 교육사이버위협 정보공유시스템

03 세부 기능 요약

악성코드 탐지	**APT 및 신변종 악성코드 탐지·차단** · IOC 침해지표 기반, 단말 행위에 대한 악성 행위 분석 · 행위기반에 따른 실시간 랜섬웨어를 탐지/차단하며 파일 암호화 및 위변조 대응 · ZeroTrust 보안 기능을 통하여 검증되지 않은 프로그램 실행보류하고 검증된 파일만 실행 · 교육부 사이버안전센터 ECSC 공식 연동을 이용한 YARA Rule 패턴 활용 악성코드 정적 분석
VM Sandbox 운영	**가상머신 샌드박스 동적 분석시스템** · 가상머신을 통해 폐쇄 환경에서 분석 기능을 제공하며, 다양한 Windows OS 버전의 샌드박스 생성 지원 · 인터넷 차단 환경에서 수동 업데이트 기능 지원 및 의심파일 수동분석 기능 지원 · 가상머신 우회방지 기능을 통한 리얼머신 구성과 동일한 동적 행위 분석 제공
보안성	**검증된 안정성을 통한단말 집중 보호** · 최초 실행파일 실행 보류 및 분석 기능으로 악성코드 감염 가능성 원천 차단 · 파일 변조 직전의 순간, 일반 프로세스가 접근 할 수 없는 보안 폴더에 파일을 백업하는 기능 · 커널 드라이버단에서의 백업 실행으로 어플리케이션간 충돌 이슈와 성능 저하 없음 · 확장자 중심의 파일 백업 / 별도의 UI를 통한 백업 파일 복원
편의성	**기술집약적 설계를 통한 편의성 제공** · 조직 / 그룹별 보안 정책 차등 적용 기능 제공 · 화이트리스트 기반 검증된 프로세스만 운영 가능 · 실시간 Agent 모니터링 사용 / 중지 기능 차단 · 분석 보고서 제공 및 주요 알림 제공 / Syslog 를 이용한 관제 솔루션과의 연동 기능 제공
연동 API 활용	**연동 API를 통한 탐지율 확보** · 내장 AV엔진(Bit-defender)을 통한 알려진 악성코드에 대한 빠른 탐지/차단 기능 · 바이러스 토탈을 이용한 추가 검색 기능 (라이선스 별도 구매 필요) · 국내 및 글로벌 패턴 연동을 통한 평판 분석 진행

04 기대 효과

Security
다차원 탐지/분석
AV+동적+정적+평판

Profit
경쟁사 대비
합리적비용

Flexibility
교육부 사이버안전센터
ECSC 공식 연동

Safety
가상머신 우회 방지
IOC 침해지표 탐지

Innovation
MITRE ATT&CK 분류
실시간 순간 백업

정확한 분석·빈틈없는 차단
다차원의 탐지/분석 기술력
가상머신 우회방지 기능
IOC 침해지표 탐지

교육부 ECSC 공식 연동
교육부 사이버안전센터 ECSC
Yara Rule 공식 연동
국내 및 글로벌 패턴 라이브 업데이트

전문성 및 가시성 향상
MITRE ATT&CK 분류
변조직전의 실시간 순간 백업
악성 행위 흐름도 제공

CONTENT

3 엔피코어

01 인증 및 특허

국제 CC인증 / 국내 CC인증 / GS인증 보유
미국 특허 2건을 포함한 12건 이상의 특허 등록

인증내역

- “ZombieZERO Inspector V3.0” 국내CC EAL2 인증
- “ZombieZERO Inspector V3.0” GS 인증
- “ZombieZERO Inspector V4.0” 국제CC EAL2 인증
- “ZombieZERO Inspector V4.0” GS 인증

국내외 특허등록 – 12건

- APPARATUS AND METHOD FOR BLOCKING ZOMBIE BEHAVIOR PROCESS
- MALICIOUS CODE DEACTIVATING APPARATUS AND METHOD OF OPERATING THE SAME
- 악성 코드 차단 장치 및 이의 동작 방법

02 레퍼런스

국내외 150여개 이상의 공공기관, 기업, 대학, 금융기관 레퍼런스 보유

국세청 ational Tax Service
경찰청 KOREAN NATIONAL POLICE AGENCY
검찰 PROSECUTION SERVICE
대한민국 국방부 Ministry of National Defense
우정사업본부 KOREA POST
Your Best Credit Partner SGI서울보증
서민금융진흥원
The K 한국교직원공제회
한국광해관리공단 Mine Reclamation Corp.
서울특별시
경상남도 GYEONGNAM
경상북도 GYEONGSANGBUK-DO
서울특별시교육청 SEOUL METROPOLITAN OFFICE OF EDUCATION
부산광역시교육청 BUSAN METROPOLITAN CITY OFFICE OF EDUCATION
인천광역시교육청 INCHEON METROPOLITAN CITY OFFICE OF EDUCATION
경상북도교육청 Gyeongsangbuk-do Office of Education
전라남도교육청
대구광역시교육청 DAEGU METROPOLITAN OFFICE OF EDUCATION
푸른등대 한국장학재단
KGU 경기대학교
동덕여자대학교
OSB 저축은행
BNK 경남은행
금융위원회
유한양행
jtbc
LS 엠트론
보훈공단 중앙보훈병원
서울케어 서울특별시 서울의료원
제주대학교병원 JEJU NATIONAL UNIVERSITY HOSPITAL
indosat ooredoo
Kamisu City Hall, Japan
Royal Malaysia Police
VNPT Vietnam Posts and Telecom Group
Vietnam Cryptography University
Spry

03 글로벌 영업현황

엔피코어는 우수한 파트너들과 함께 **글로벌 정보보안 전문기업**으로 도약하고 있습니다.

제4회 '수출 첫 걸음상' 수상 및 수출 유망 중소기업 지정

3년 연속 100만불 이상 수출

총판영업

큐오텍, 아이티윈, 파이오링크 등 우수한 총판과 협업을 통하여 공공, 기업, 금융권 등에 판매

조달시장

국제 CC인증 획득 및 우수한 파트너 계약을 통하여 해외 판매를 위한 요구사항 충족 및 기회발굴

해외영업

베트남에 지사를 두고, 말레이시아, 인도네시아, 미국, 베트남 등 해외 총판사와 계약 체결. 정보보호 시장의 기존 고객을 보유하고 있는 총판사들을 통하여 현지의 영업 및 기술지원 확보를 통한 제품 판매 및 영업 강화

THANK YOU

HEAD QUATER
ISBiz Tower 1001, 26, Yangpyeong-ro 21-gil, Yeongdeungpo-gu, Seoul, R.Korea
Tel : +82-2-1544-5317 Fax: +82-2-413-5317 Email : ceos@npcore.com

SUBSIDIARY
1801 Research Blvd Suite 570 Rockville, MD 20850

BRANCH
3rd floor, number 138 Hoang Ngan street, Trung Hoa ward, Cau Giay district, Ha Noi city
Tel: +84-4-3837-8554 Fax: +84-4-3837-8556