# APT대응 **보안솔루션**

## Zombie **ZERO** Inspector **N**

NPCORE

신변종 악성코드 탐지/차단

# CONTENT

## 1 보안현황


01 증가되는 사이버 공격

02 지능형 위협 공격


# 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<br>악성코드 디자인 | Ransomeware / Bootkit /<br>Backdoor 등 |
| 탐지율 | 샘플 발견시<br>99% 탐지룰 작성 | **샘플이 발견되어도<br>10% 탐지룰 작성<br>(변종이 다양함)** |

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

# CONTENT

## 2 좀비제로


01 제품 개요

02 주요 특징

- 체계적인 수집
- 수집 전용 가속보드
- 실시간 트래픽 차단
- 다차원 분석
- 가상머신 우회 방지
- ECSC 공식 연동
- MITRE ATT&CK 분류
- 악성코드 공격 형태 분석
- 글로벌 탐지 패턴

03 세부 기능 요약

04 기대 효과


NPCORE

# 01 제품 개요

## ZombieZERO Inspector N

네트워크로 침입하는 알려진/알려지지 않은 신/변종 악성코드 탐지/차단 시스템


**1 위치**
네트워크 구간 미러링 방식 설치

**2 수집**
네트워크 트래픽 안 파일 수집

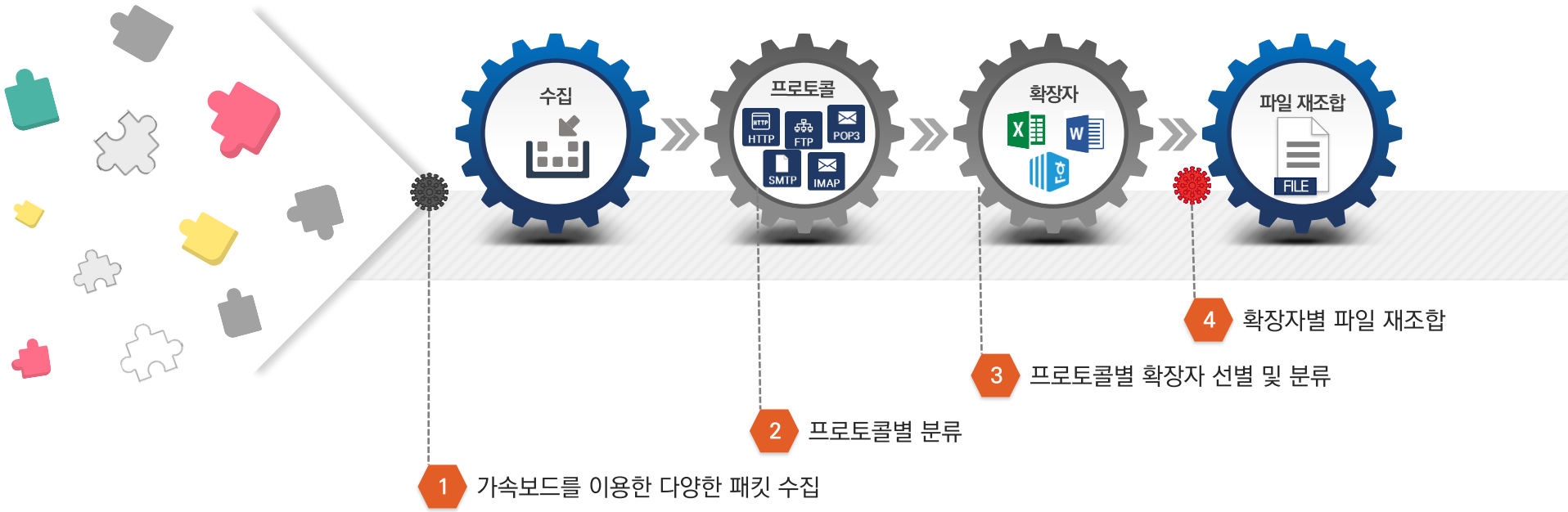
**3 분석 / 탐지**
수집된 파일에 대한 다차원 분석 및 탐지

**4 차단**
분석 결과를 토대로 악성 URL 접속 차단

**5 관리**
관리자 UI 및 분석 보고서 제공

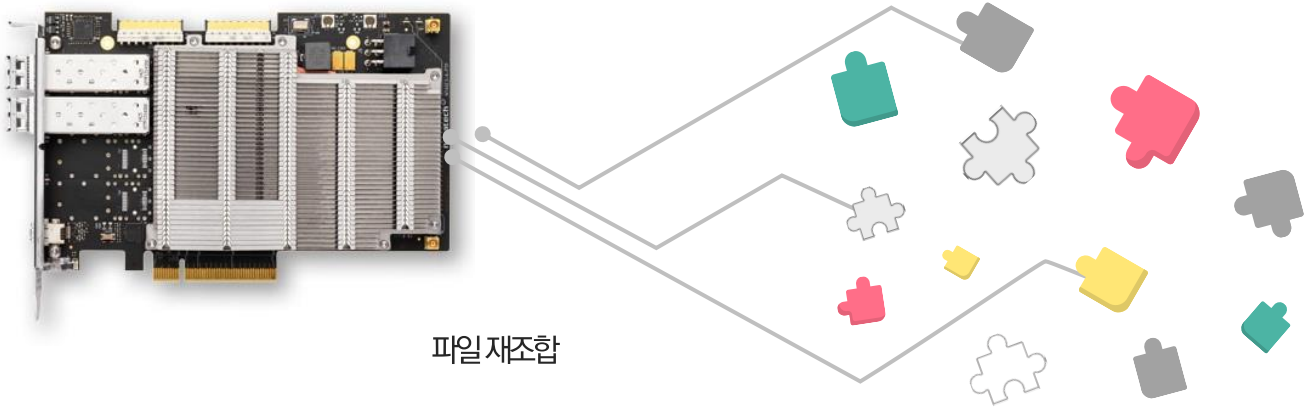
# 02 주요 특징 – 체계적인 수집

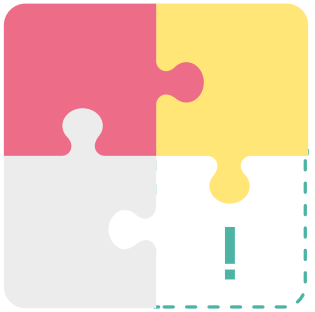
- 가속보드를 이용한 패킷 수집 및 파일 재조합



# 02 주요 특징 - 수집 전용 가속보드

- 수집 전용 가속보드를 사용하여 <u>유실 없는 네트워크 패킷 수집</u>



파일 조각 하나라도
수집 못할 경우
원본파일 조합 불가

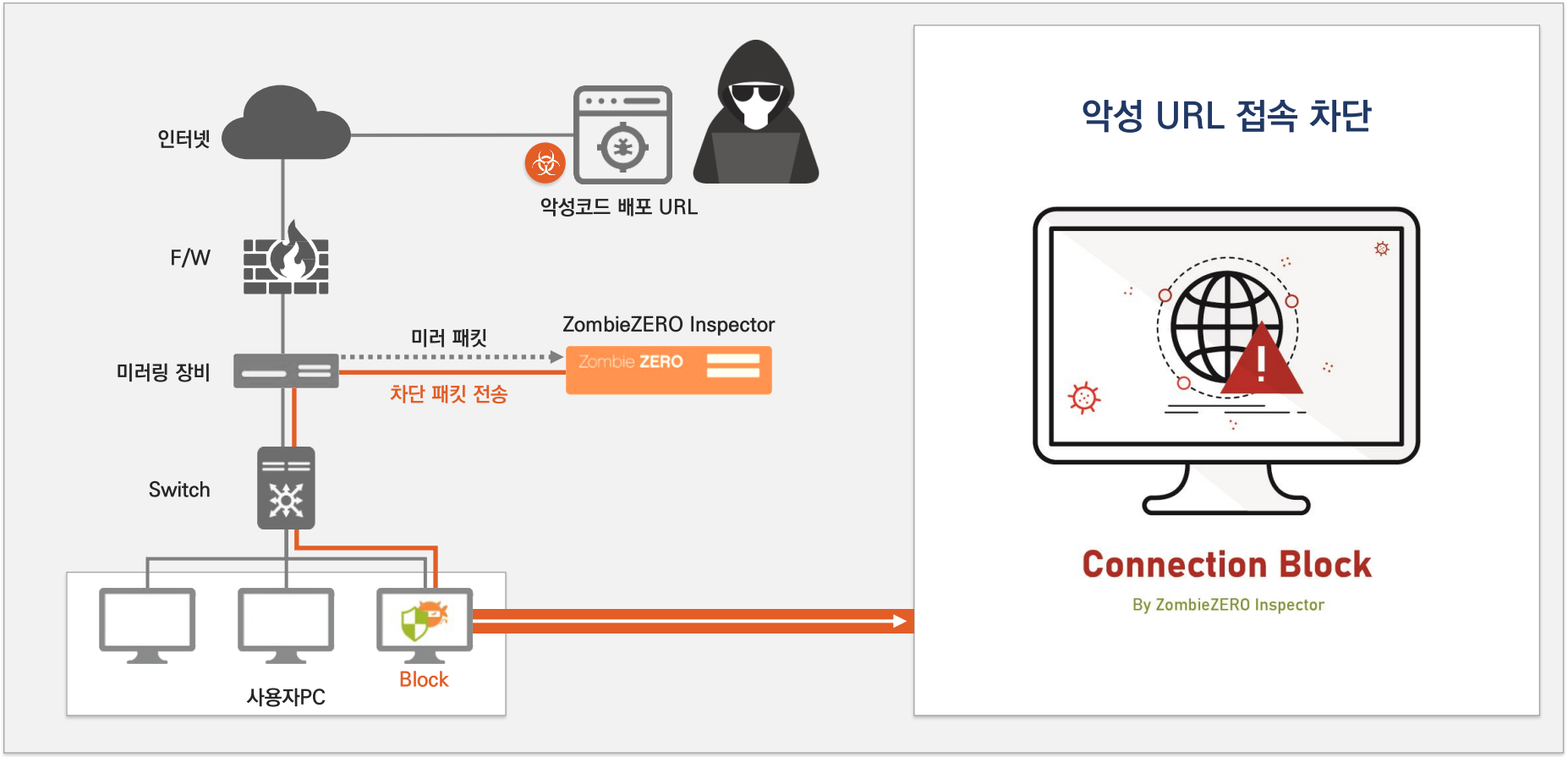
## 수집 가속 보드 장점

- 네트워크상 다중 지점에서 실시간 데이터를 수집, 하나의 분석 스트림으로 병합하여 분석 데이터의 상관 관계를 보다 쉽게 설정
- 나노초 정밀도로 모든 이더넷 프레임의 타임스탬핑
- 지능형 기능으로 CPU 부하가 극히 낮은 상태에서 애플리케이션 성능 가속

**지원 : 1GbE 4port / 10GbE 2port / 10GbE 4port**

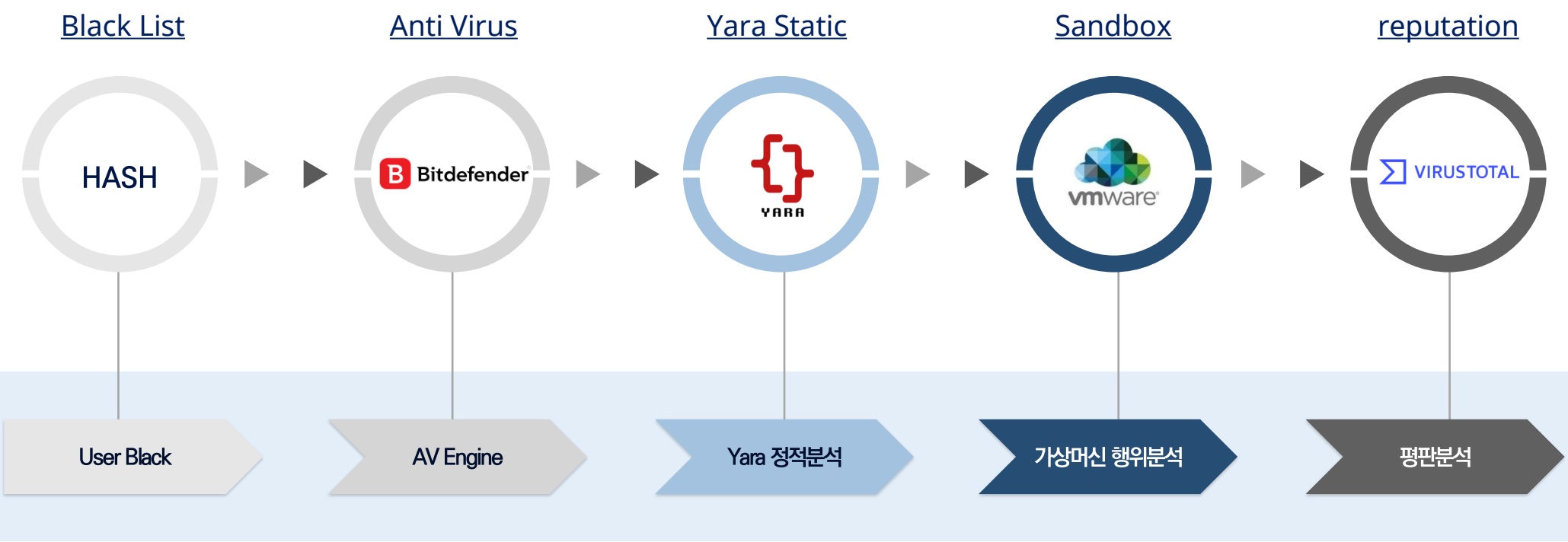
# 02 주요 특징 – 실시간 트래픽 차단

- C&C 서버 접속 및 악성코드 배포 사이트 URL 접속 차단 등 **실시간 차단**



# 02 주요 특징 – 다차원 분석

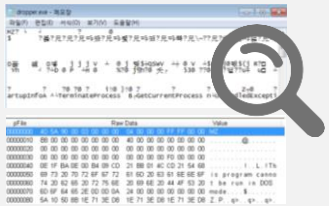
- 시그니처/정적/동적분석 등의 알려지지 않은 악성코드 다차원 분석



# 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

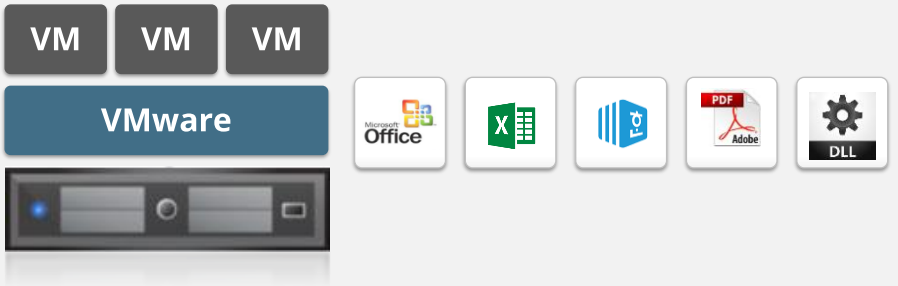
```
rule CEO_Fraud
{
    meta:
        author = "Natalie"
        date = "11/06/2018"
        description = "This is a basic YARA rule for CEO fraud."

    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**

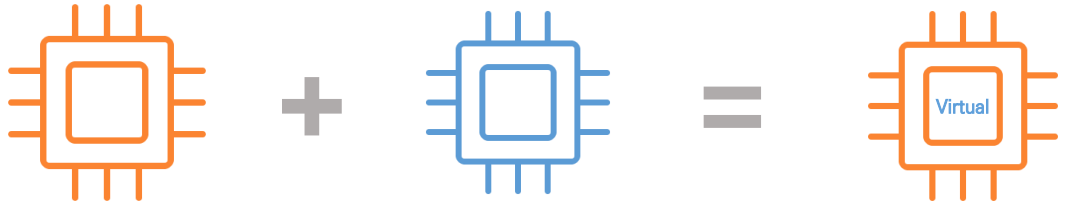
동적분석 : 악성 행위 분석



# 02 주요 특징 – 가상머신 우회 방지

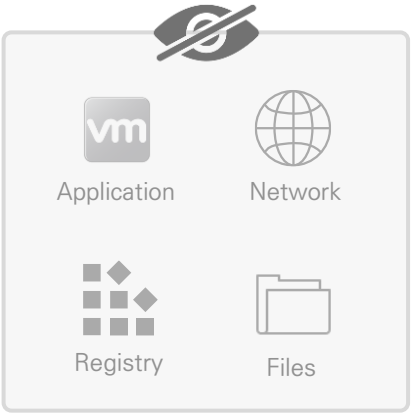
- 적은 비용의 가상머신 구성으로 리얼머신 구성과의 동일 효과 제공
- 가상머신을 우회하는 악성코드의 행위를 유도하여 동적 행위 탐지 분석

## 가상머신 우회 방지 기술




| Real Machine | Virtual | Fake Real Machine |
|---|---|---|
| BFEBFBFF000306C3<br>Physical CPUID | 0FABFBFF000306C3<br>Running Inside Hypervisor | BFEBFBFF000306C3<br>Running Inside Real Machine |

**리얼머신의 CPUID 정보로 변경**
**(EAX/EBX/ECX/EDX)**




**가상머신 고유정보 숨기기**

- 가상머신의 CPUID 정보를 **리얼머신의 CPUID 정보로 변경, 가상머신 고유정보 숨기기** 등의 우회 방지 기술
- 가상머신 우회 방지 기술을 통하여 악성코드는 **가상머신을 리얼머신으로 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

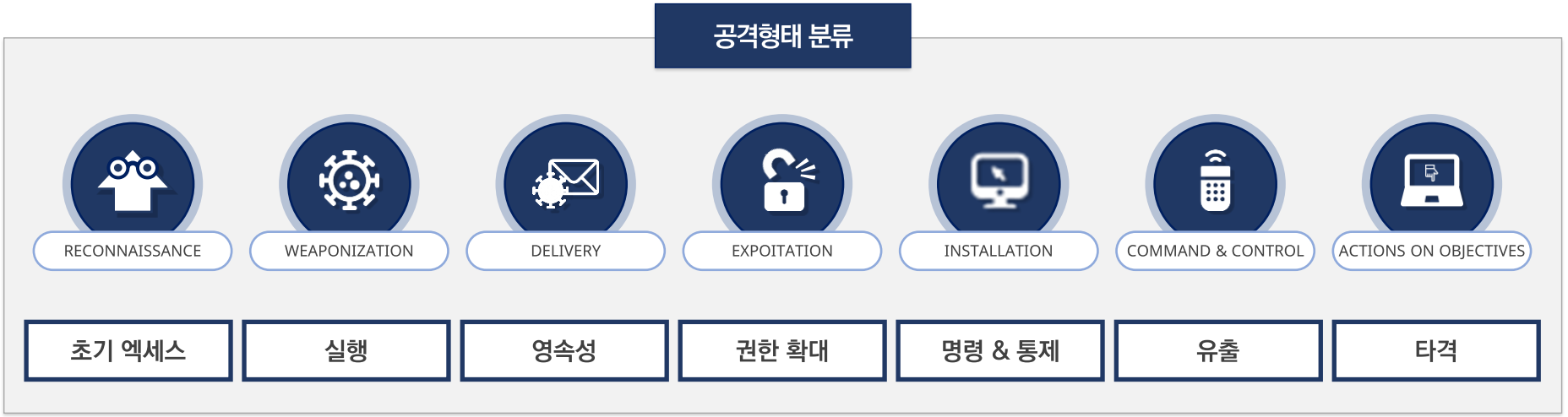
- 표준화된 MITRE ATT&CK 분류에 맞는 악성 코드의 카테고리화 적용
- 악성코드의 공격 방법(전술)에 대해 확인 가능

MITRE

ATT&CK™

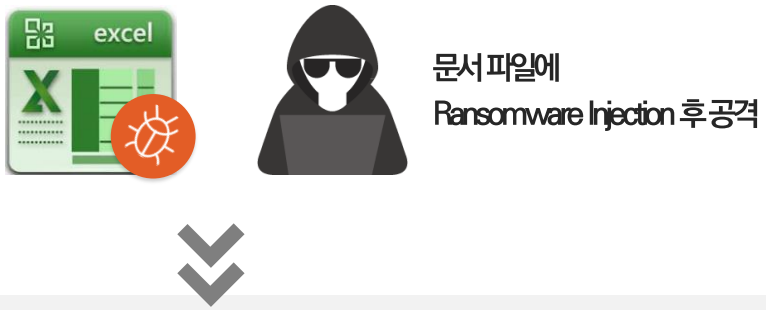
Adversarial Tactics, Techniques & Common Knowledge

**공격의 결과가 아닌**
**진행중 공격에 대한 기술 및 방법의 형태 모니터링**

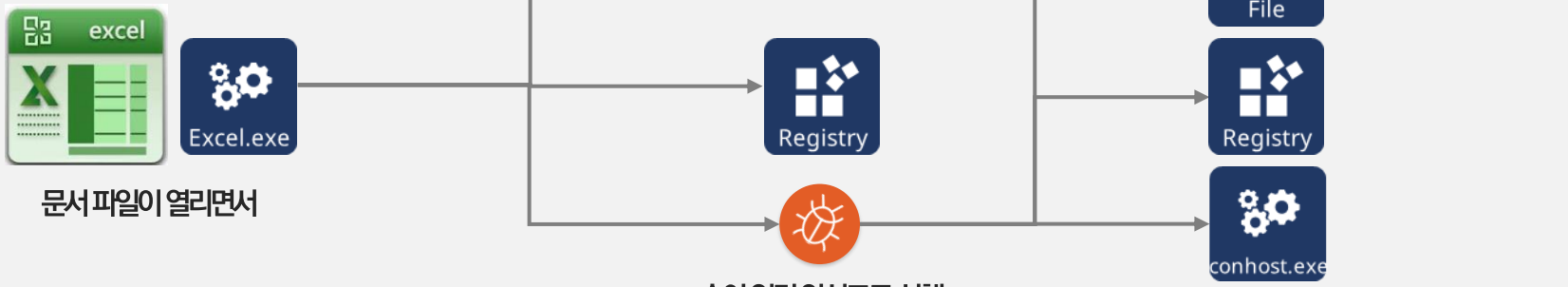


# 02 주요 특징 – 악성코드 공격 형태 분석

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





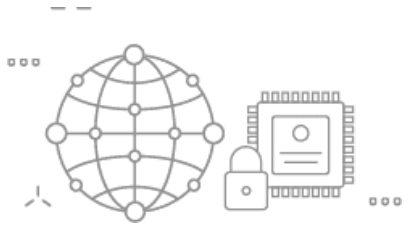


# 02 주요 특징 – 글로벌 탐지 패턴

- 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 | **네트워크 수집을 통한 악성코드 탐지 및 CnC 악성 URL 접속 차단**<br>· 수집전용 가속보드를 이용한 트래픽 수집과 다차원 분석<br>· HTTP, FTP, POP3, IMAP, SMTP 프로토콜 파일 수집<br>· Web 기반 Exploit을 통하여 유입되는 악성코드 탐지<br>· 문서 (MS-office, HWP, PDF) / 압축 / 실행 파일을 통한 악성코드 탐지 |
| VM Sandbox 운영 | **가상머신 샌드박스 동적 분석시스템**<br>· 가상머신 샌드박스 동적분석 시스템을 통해 폐쇄 네트워크 환경에서 분석기능 제공<br>· 인터넷 차단 환경에서 수동 업데이트 기능 지원 및 의심파일 수동분석 기능 지원<br>· 가상머신 우회방지 기능을 통한 리얼머신 구성과 동일한 동적 행위 분석 제공<br>· 다양한 Windows OS 버전의 샌드박스 생성 지원 및 최대 40개 샌드박스 생성 가능 |
| 연동 API 활용 | **연동 API를 통한 탐지율 확보**<br>· 내장 AV엔진(Bit-defender)을 통한 알려진 악성코드에 대한 빠른 탐지/차단 기능<br>· 교육부 사이버안전센터 ECSC 공식 YARA Rule 연동<br>· 국내 및 글로벌 패턴 연동을 통한 평판 분석과 바이러스 토탈을 이용한 추가 검색 기능 |
| 편의성 | **통합 관리를 통한 편의성 제공**<br>· 분석 보고서 제공 (Doc, Excel, PDF)<br>· 대시보드를 통해 관리 대상 보안 수준, 악성 파일 분석 현황, 주요 이벤트, 현황 정보 파악 가능<br>· 주요 보안 이벤트 발생 시 알림(E-mail, SMS 등) 제공<br>· Syslog 를 이용한 관제 솔루션과의 연동 기능 제공 |
| 확장성 | **장비 증가에 대한 유연한 확장성**<br>· 가상 분석 이미지를 추가하거나 장비를 병렬로 구성하여 증가하는 분석 파일에 대하여 확장 운영 가능<br>· 파일 수집 장비(Detector)와 파일분석장비(Analyzer)의 분리로 향후 시스템 확장 시 파일 분석 장비만 추가하여 시스템 운영 가능<br>· 장비 별 최대 20Gbps 트래픽까지 처리하며 최대 4개의 10GbE 인터페이스 구성 가능 |

# 04 기대 효과

## Security
다차원 탐지/분석
AV+동적+정적+평판

## Profit
경쟁사 대비
합리적비용

## Flexibility
교육부 사이버안전센터
ECSC 공식 연동

## Safety
악성코드 행위분석
가상머신 우회방지

## Innovation
MITRE ATT&CK 분류
악성 흐름도 제공

### 정확한 분석·빈틈없는 차단
다차원의 탐지/분석 기술력
가상머신을 이용한 행위 분석
가상머신 우회방지 기능

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

### 전문성 및 가시성 향상
수집전용 가속보드 사용
MITRE ATT&CK 분류
악성 행위 흐름도 제공

# CONTENT

## 3 엔피코어


01 인증 및 특허

02 레퍼런스

03 글로벌 영업현황

# 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