Real-time Next Generation NDR

Packet CYBER

차세대 NDR에 대한 비밀과 거짓말

VISTA (주)씨큐비스타

NDR 경쟁 기술 비교

Packet CYBER

AI 기반 NDR 기술 특징

- 많은 경험 필요 (별도 전문가 필요)
- 수 주일간의 정상 트래픽 학습 필요
- 악성코드 탐지 기능 없음
- 별도 전문가 필요

제약 요소

- 실시간 탐지 불가 (※ 약 1 개월 사전 학습 필요)
- 이미 유입(감염)된 위협 환경 적용 불가 (※ 위협을 정상으로 학습)
- 이동 설치 불가 (※ 재 학습 필요)
- 악성코드 자체 탐지 불가 (※ 이상 탐지 위주)
- 의심스러운 트래픽은 쉽게 해석되지 않을 수 있음 (※ 이상 ≠ 위협)

Full Packet 수집 기반 NDR 기술 특징

- 벤더가 제공하는 위협 인텔 기반 악성코드 및 이상 징후 탐지 제한적 (외국보안벤더의 시그니처 및 TI 정보 기반)
- 하나의 사실을 확인하는 데 상당한 분석 시간 소요 (전체 패킷 확인)
- 별도 전문가 필요

제약 요소

- 이미 유입(감염)된 위협 환경 적용 시, 시그니처 및 TI 정보 의존 탐지
- 이동 설치 어렵고 분석 시간 요소 (※ 전체 패킷 캡쳐➔ Batch 처리 ➔ 메타데이터 추출 / 시그니처 매칭 ➔ 메타데이터 연계 분석)
- 제한적 탐지 (※ 시그니처 및 TI 의존적)
- 제한적 행위 기반 위협 탐지 (※ NDR 정의를 따르지 못함)

- ✓ "실시간" 악성코드 탐지 (?) / 위협 특정 (?)
- ✓ "실시간" 네트워크 이상행위 탐지 (?) / 위협 특정 (?)
- ✓ 탐지된 위협에 대한 대응 가이드북 (?)
- ✓ 사람의 개입 최소화 운영 (?)

I. 효율적인 위협 탐지 및 대응 불가!
II. 보안 팀의 운영 부담 가중!

PaketCYBER가 경쟁사 NDR 대비 우수한 이유는 무엇인가요?

PacketCYBER 고객은 침해 이후 공격을 9배 이상 빠르게 탐지합니다!

9X

누구도 PacketCYBER가 보는 것을 볼 수 없으며, 증명할 수 있습니다!

귀사의 기업 환경에서 14일 동안 PacketCYBER를 테스트하십시오.

타 NDR 벤더가 보지 못하는 위협을 발견하게 될 것입니다

Packet CYBER™	Others
MTTD 수초 이내. MTTR 수분 이내.	MTTD / MTTR: 9주일 이상

※ MTTD: Mean Time To Detect (평균 탐지 소요 시간)
※ MTTR: Mean Time To Response (평균 대응 소요 시간)

모든 패킷을 100% 저장하고 분석하기 때문에 모든 사이버 보안 위협을 탐지하고 대응할 수 있다?

➔ Really?

※ OO공사 실제 네트워크 테스트 결과 (기간: 1 개월)

	네트워크에 잠재된 위협		RSA Netwitness + AI 분석 모듈 + 전문 분석 인력 (4명)	PacketCYBER
01	위험한 파일 다운로드 (외부 → 내부)	HTTP기반 악성코드 / 추가 검증 VT (27/55)	☐	☑
02	자동 클릭 툴 다운로드 (외부 → 내부)	HTTPS기반 악성코드 / 추가 검증 VT (16/70)	☐	☑
03	출처 불분명 다운로더 다운로드 (외부 → 내부)	HTTPS기반 Office 2016 다운로더 / 추가 검증 VT (28/59)	☐	☑
04	보안 서비스 서버 접속 실패	다수의 내부 IP에서 webclinic.ahnlab.com로 접속 시도 / 12,969,530건의 접속 실패	☐	☑
05	중지된 서버 접속 시도1 (내부 → 외부)	내부 IP에서 내부 IP의 다수 포트로 접속 시도 / 접속 실패	☐	☑
06	중지된 서버 접속 시도2 (내부 → 외부)	내부 IP에서 홍콩 IP 80포트로 접속 시도 / 453,676건의 접속 실패	☐	☑

모든패킷을100%저장하여분석하는솔루션은 탐지및분석에많은시간과노력이수반되며, 위협탐지및분석이매우어렵습니다.

공격이발생했을때는 위협 탐지정확도와 탐지속도가생명입니다!

기존 보안으로 해결할 수 없었던 상황 위협 헌팅 사례 #1

Packet CYBER

폐쇄 망 임에도 네트워크 이상 징후가 발생하여, 원인 분석이 불가능한 상황 (글로벌 APT, NDR 실패)
➔ 감염된 폐쇄 망 내 이상 징후에 대한 원인 분석 및 알려지지 않은 위협에 대한 성공적인 헌팅

사례1 OO 시청

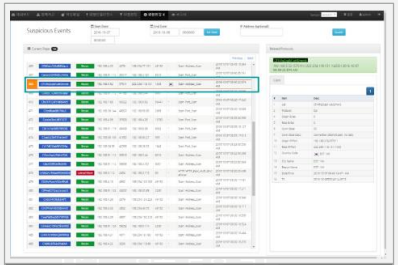
- 폐쇄망으로 운영되는 CCTV 네트워크에 이상 현상을 감지하였으나, 어떠한 보안 솔루션 및 네트워크 관리 솔루션으로도 원인 규명이 불가능한 상태
- 침해사고 대응에 필요한 위협 가시성 및 악의적인 행위를 찾을 수가 없음

	적용 솔루션	수행 내용	결과
1	업계 최고 외산 샌드박스	Call Back기반 탐지 시도	실패
2	ML기반 외산 네트워크 이상탐지	네트워크 이상 탐지 시도	학습 기간 필요로 실패
3	EDR	-	임베디드 디바이스 환경으로 적용 불가

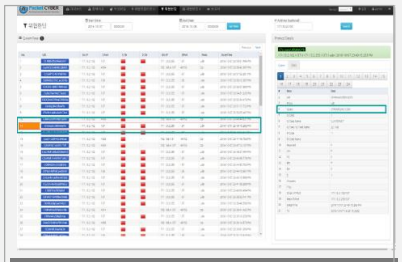
1. DB 공격 이상 징후
2. 드로퍼 공격 이상 징후
3. C&C 접속 이상 징후
4. 이상 접속 시도 1
5. 이상 접속 시도 2

해결책 : PacketCYBER

- 네트워크 이상에 대한 원인 규명 및 알려지지 않은 공격 요소 들을 찾아냄
- 보안 담당 주무관의 호평:
  "이미 감염되어 있는 Endpoint들을 찾을 수 있는 유일한 솔루션"

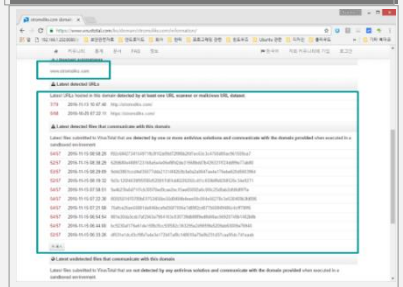


탐지 – 경고 발생 확인



이상 DNS 쿼리 탐지

다양한 IP의 1433포트(MS-SQL Port)로의 접속 시도 확인



드로퍼 악성코드 감염 확인

기존 보안으로 해결할 수 없었던 상황 위협 헌팅 사례 #2

Packet CYBER

최신 보안 솔루션들을 사용하고 있으나, 침해사고 발생. 네트워크가 안전한지 여부 분석 불가능 (글로벌 NDR 실패)
➔ 네트워크가 안전한지 여부 분석 및 알려지지 않은 위협에 대한 성공적인 헌팅

사례2 OO 시청

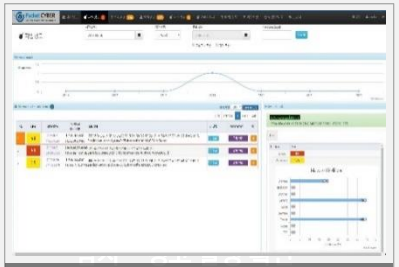
- 다양한 보안 솔루션 운영 중이나 네트워크가 안전한지 분석이 불가능한 상황
- 알려지지 않은 위협에 의한 악의적인 행위를 찾을 수 없음

	적용 솔루션
1	다수 보안 솔루션 및 악성코드 샌드박싱 운용
2	보안관제 팀 운영

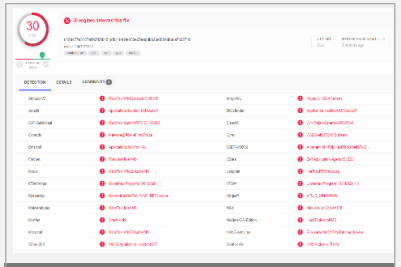
1. SMTP 메일에 악성 파일이 포함되어 외부로 전송
2. kSign 툴로 위장한 악성코드와 접속 기록이 있는 IP가 HTTP 프로토콜에 포함
3. ftp.aiub.unibe.ch로 FTP 접속을 계속 시도
4. 악성코드와 통신 기록이 있는 의심 IP가 HTTP 프로토콜에 포함
5. 스캐닝 탐지...

해결책 : PacketCYBER

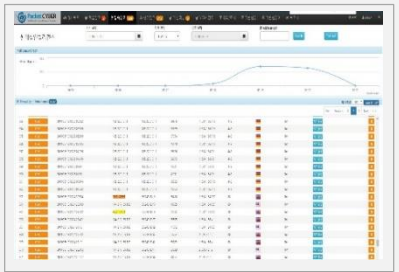
- **네트워크 이상에 대한 원인 규명 및 알려지지 않은 공격 요소들을 찾아냄**



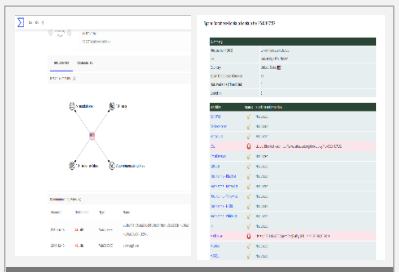
탐지 – 악성코드 유입 경고가 발생했음을 파일경고에서 확인함



위험 경고가 발생한 악성코드가 KMSpico (MS우회 인증 툴) 임을 확인함



위협 의심 IP(35.0.127.52)가 탐지되었음을 접속경고에서 탐지



위협 의심 IP 헌팅 – 6개의 Spam DB에 등록되어 있음을 확인함

기존 보안으로 해결할 수 없었던 상황 위협 헌팅 사례 #3

Packet CYBER

공공 Wi-Fi를 구축 및 시범 운영하고 있으나 위협 상황에 대한 어떤 해결책도 없음 (글로벌 NDR 실패)
➔ 공공 Wi-Fi 네트워크 위협에 대한 성공적인 위협 헌팅

사례3 OO 시청

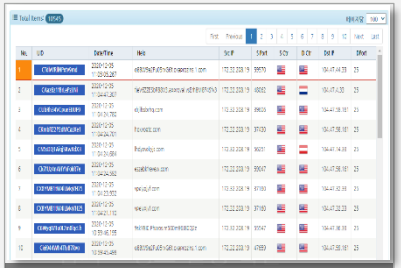
- 공공Wi-Fi를 구축하여 시범 운영하고 있으나 공공 Wi-Fi 네트워크 위협 상황이 궁금하나 해결책이 없음

적용 솔루션
적용 가능 솔루션 없음

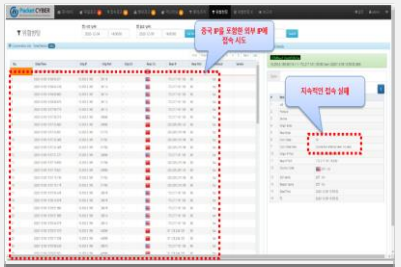
1. Wi-Fi라우터에 할당된 공인 IP를 이용하여 10,545건의 SPAM 메일 발송
2. 특정 사설 IP에서 외부에 있는 66개 IP의 80번 포트로 1,286회 접속 시도
3. 영리 사업자의 POS단말기가 Wi-Fi 서비스 사용
4. 중국 IP를 포함한 다수의 외부 IP에서 공인 IP의 22번 포트(SSH)로 접속 시도

해결책 : PacketCYBER

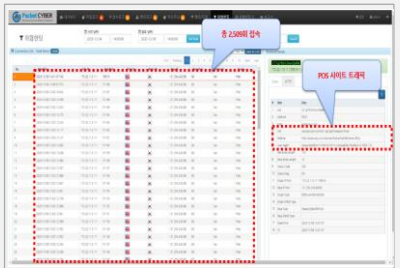
- 공공 Wi-Fi 네트워크 위협 상황 분석



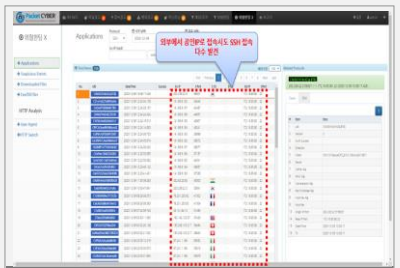
25 Perfect Gifts For Those You Love
25 Gadgets That Will Make 2020 A Lot Better
25 Best Gifts Under $60 In 2020 등
다양한 이메일 제목으로 10,545건 스팸 발송



내부 IP가 중국을 포함한 66개 외부 IP의 80번 포트로 지속적인 접속을 시도하나 실패함



영리 사업자의 POS 단말기가 공공 Wi-Fi망에 접속해 트래픽 사용



중국 포함 다수의 외부 IP에서 공인 IP의 22번 포트(SSH)로 접속 시도

네트워크상의 위협을 가시화 함으로써 공격자의 Dwell 타임을 줄이는 것이 핵심 !

Real-time DETECT, HUNT, RESPOND

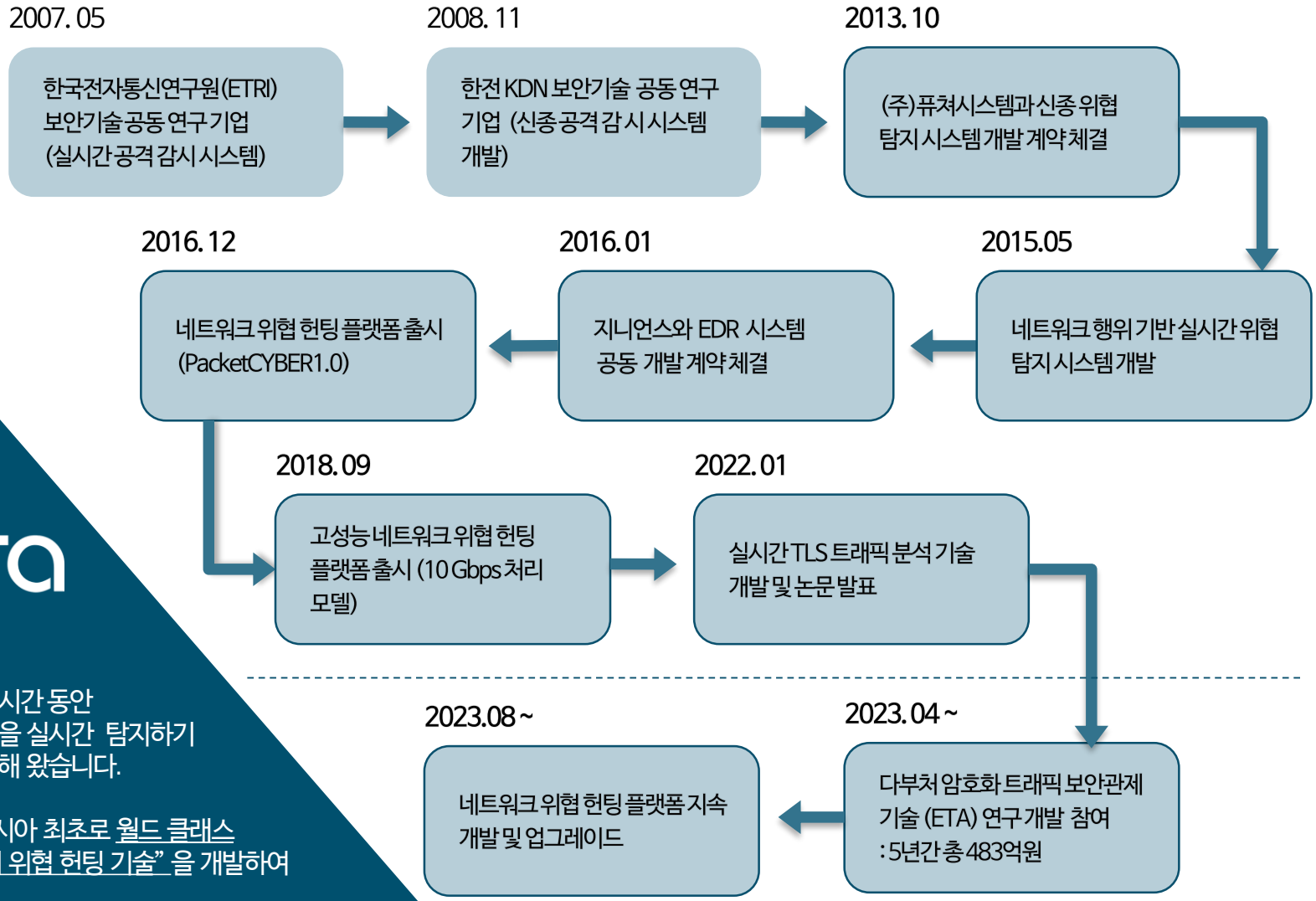
Reference Sites

Packet CYBER

금융 고객	OO 은행	OO 은행	OO 은행	
공공 고객	중앙부처 1	중앙부처 2	중앙부처 3	중앙부처 4
	광역단체 1	OO공사	공공기관 1	공공기관 2
기업 고객	중견기업 1	중견기업 2	중견 제조업체 1	
	대기업 1	일본 IDC		

씨큐비스타 주요 기술 개발 경험 및 능력

Packet CYBER



vista

씨큐비스타는 10 여년이 넘는 시간 동안
기존 보안 기술이 놓치는 위협을 실시간 탐지하기
위한 다양한 보안 기술을 개발해 왔습니다.

이러한 기술력을 바탕으로 아시아 최초로 월드 클래스
네트워크 기반 "실시간 사이버 위협 헌팅 기술" 을 개발하여
보급하고 있습니다.

(주)씨큐비스타

주소 : 경기도 성남시 분당구 판교로 255번길 9-22 (삼평동) 판교 우림 W-CITY 511호 (우 13486)

데모 및 제품 문의 : 02-565-0236 | sales@cqvista.com

Packet CYBER