진화하는 랜섬웨어와 의료정보 보호 방안

More security,
More freedom

안랩 솔루션컨설팅팀 **김승관 부장**

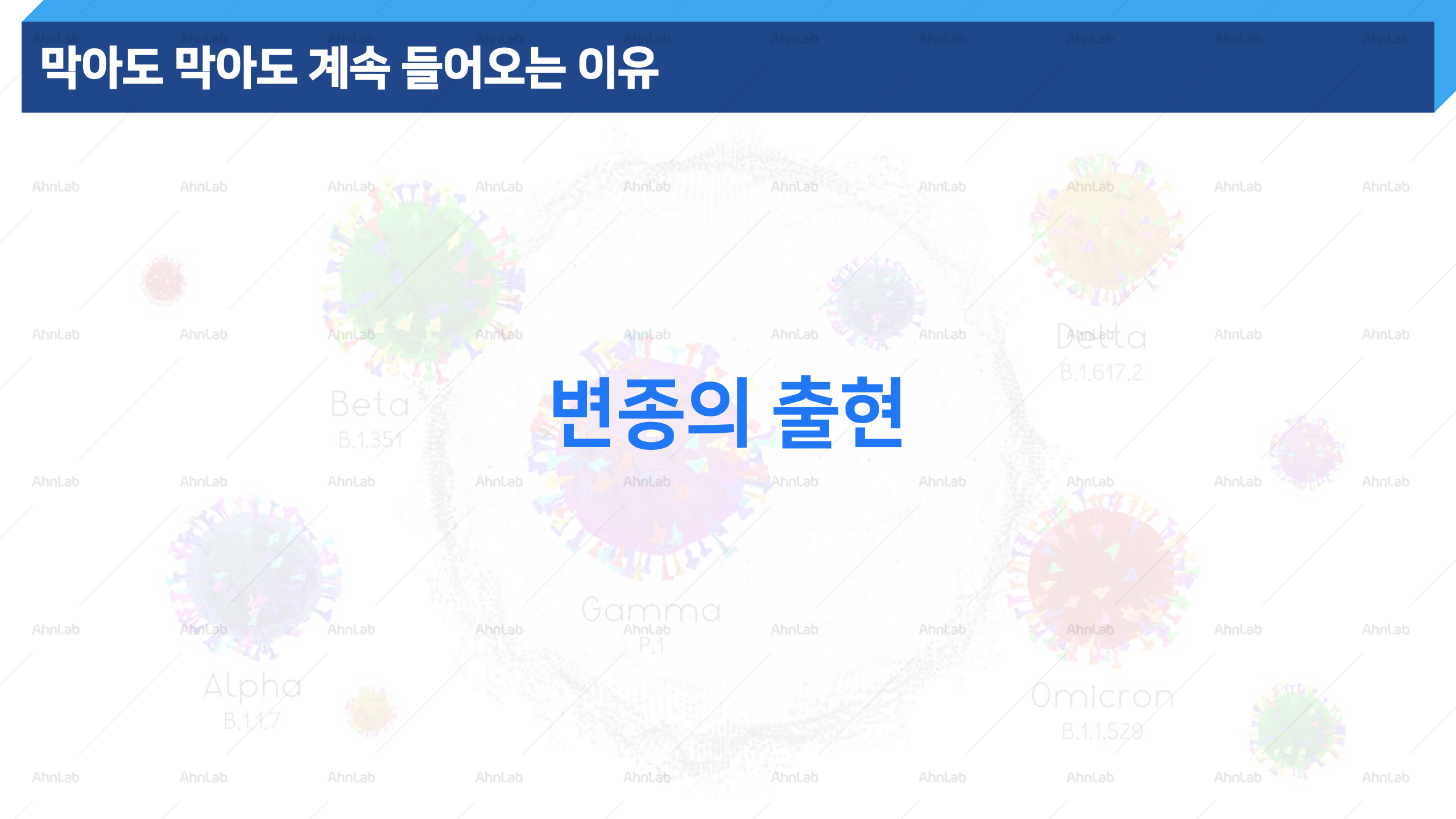
AhnLab

01.
신규 랜섬웨어 통계

AhnLab

막아도 막아도 계속 들어오는 이유

변종의 출현



02.
탐지 우회 기법 (defense evasion)

AhnLab

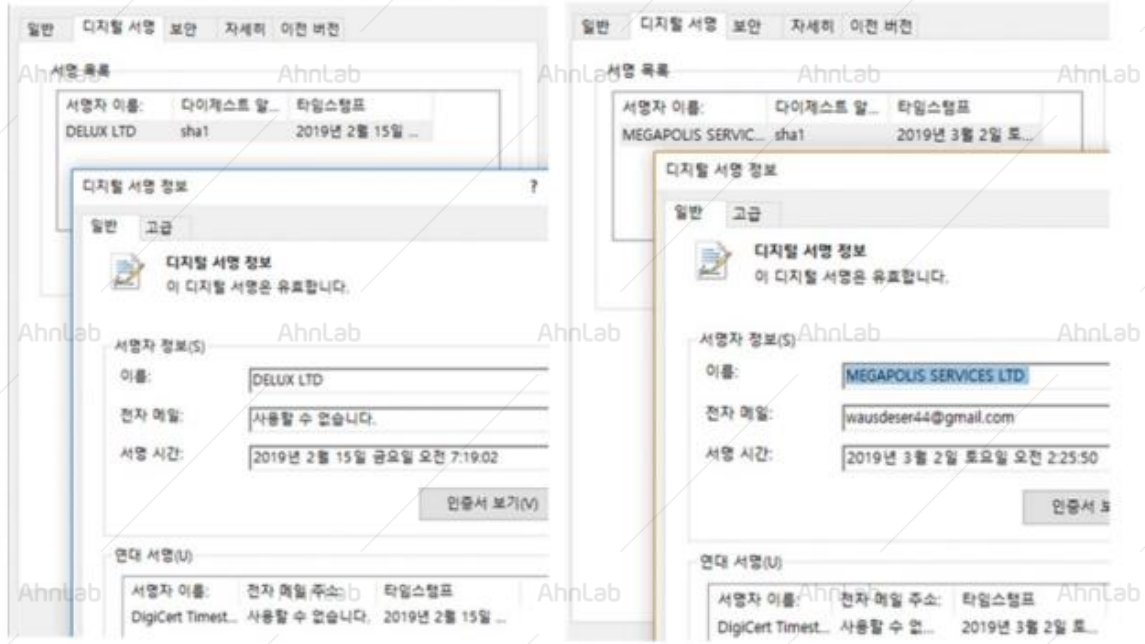
02. 탐지 우회 기법

정상 SW/ 정상 환경과 최대한 비슷하게

정상 파일명과/ 경로 유사 생성

유형	악성코드 명
정상 프로그램 위장	C:₩ProgramData₩Adobe₩wsus.dll C:₩ProgramData₩Adobe₩Setup₩wsus.exe C:₩Intel₩localserv.exe C:₩Intel₩logon.exe C:₩Intel₩wsus.exe C:₩hp₩sysinfo.exe C:₩hp₩slog.exe C:₩hp₩AdFind.exe C:₩hp₩sage.exe C:₩hp₩wsus.exe
윈도우 소프트웨어 위장	C:₩ProgramData₩Microsofts Help₩wsus.exe C:₩ProgramData₩Microsofts Help₩wsus.exe C:₩Windows₩localserv.exe C:₩Windows₩tasks₩wsusrv.exe
서비스명	IntelProtected

유효 인증서 사용



02. 탐지 우회 기법

시그니처 패턴을 우회하자

난독화 기법

인코딩 : 인코딩 알고리즘을 사용해 데이터를 모호하게 한다.
(ASCII Encoding, HEX Encoding, UNICODE Encoding …)

```
root@machine:/# echo "hello world" | base64
aGVsbG8gd29ybGQK
```

[Base64 Encoding 예시]

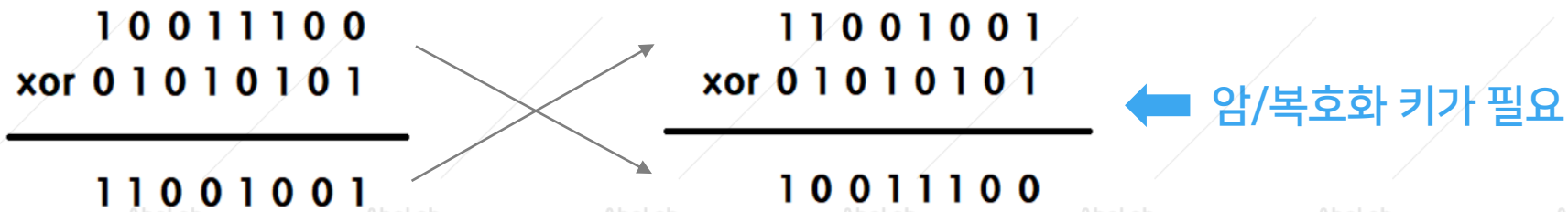
단순 Decode 명령을 이용하여 손쉽게 해제 할 수 있다.

Base64 –d "aGVsbG8gd29ybGQK"
>> hello world

02. 탐지 우회 기법

난독화 기법

암호화 : 복호화 함수와 암/복호화하는데 사용하는 키를 식별해야 한다
(대칭키, 비대칭키)



calc.exe

Offset	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F	ANSI ASCII
00000000	4D	5A	90	00	03	00	00	00	04	00	00	00	FF	FF	00	00	MZ ÿÿ
00000010	B8	00	00	00	00	00	00	00	40	00	00	00	00	00	00	00	¸ @
00000020	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	
00000030	00	00	00	00	00	00	00	00	00	00	00	00	F8	00	00	00	ø
00000040	0E	1F	BA	0E	00	B4	09	CD	21	B8	01	4C	CD	21	54	68	° ´ Í!¸ LÍ!Th
00000050	69	73	20	70	72	6F	67	72	61	6D	20	63	61	6E	6E	6F	is program canno
00000060	74	20	62	65	20	72	75	6E	20	69	6E	20	44	4F	53	20	t be run in DOS
00000070	6D	6F	64	65	2E	0D	0D	0A	24	00	00	00	00	00	00	00	mode. $

calc_xor.exe

Offset	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F	ANSI ASCII
00000000	6E	79	B3	23	20	23	23	23	27	23	23	23	DC	DC	23	23	ny³# ###'###ÜÜ##
00000010	9B	23	23	23	23	23	23	23	63	23	23	23	23	23	23	23	›#######c#######
00000020	23	23	23	23	23	23	23	23	23	23	23	23	23	23	23	23	################
00000030	23	23	23	23	23	23	23	23	23	23	23	23	DB	23	23	23	############Û###
00000040	2D	3C	99	2D	23	97	2A	EE	02	9B	22	6F	EE	02	77	4B	-<™-#—*î ›"oî wK
00000050	4A	50	03	53	51	4C	44	51	42	4E	03	40	42	4D	4D	4C	JP SQLDQBN @BMML
00000060	57	03	41	46	03	51	56	4D	03	4A	4D	03	67	6C	70	03	W AF QVM JM glp
00000070	4E	4C	47	46	0D	2E	2E	29	07	23	23	23	23	23	23	23	NLGF ..) #######

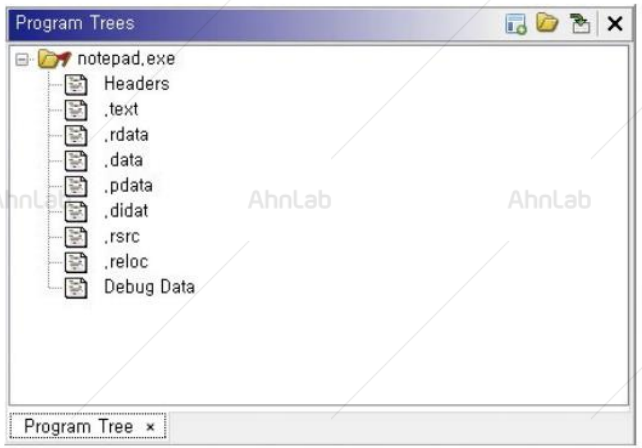
[XOR 암호화]

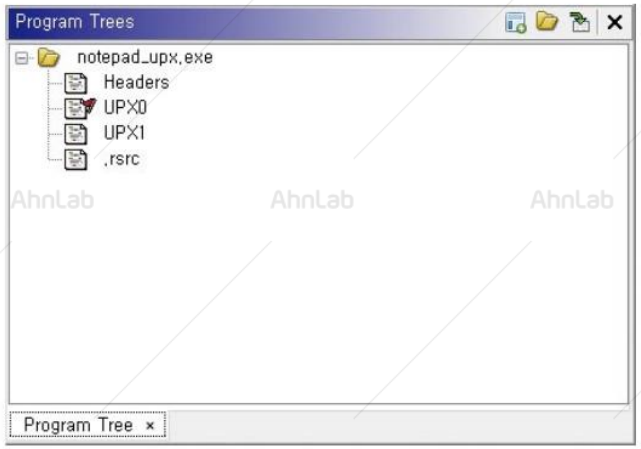
02. 탐지 우회 기법

난독화 기법

패킹 : 패킹은 정상 바이너리 파일을 패커를 통해 실행 압축시킨다.

(UPX, Upack, ASPack, Petite, FSG 1.33, nPack…)





[정상파일과 패킹파일UPX 비교]

03.
대응 전략

AhnLab

03. 대응 전략

컨셉별 보안 제품군

01

시그니처 기반

- 백신제품군 (엔드포인트)
- IDS / IPS 제품군 (네트워크)

- **알려진 위협** (Known Attack)
- **시그니처 기반 정적 분석**
- **실시간 감시 및 차단**

02

SandBox 기반

- APT 솔루션 (네트워크)
- APT 솔루션 (클라우드)

- **알려지지 않은 위협** (UnKnown Attack)
- **가상화 샌드박스 기반 동적 분석**
- **파일 실행 보류**

03

모니터링 기반

- EDR (엔드포인트)
- NDR (네트워크)

- **위협의 가능성이 있는 모든 행위** (Known, Unknown)
- **실제 시스템 기반 행위 및 이벤트 분석**
- **프로세스 종료, 파일 삭제, 네트워크 격리**

04.
APT 제품 컨셉

AhnLab

04. APT 제품 컨셉

AhnLab MDS

MDS, MDS Agent, MTA 통합 관리 **MDS Manager, MDS Analysis Manager**

미분석 파일 실행 보류 **MDS Agent**

메일 특화 대응 **MTA License**

알려지지 않은 위협 대응을 위한 선택 **AhnLab MDS**

파일 분석 솔루션

파일이 존재하는 모든 곳에 설치
다양한 파일 포맷 분석

샌드박스 솔루션

격리된 환경에서 파일 실행
악성 행위 탐지를 통한 위협 탐지

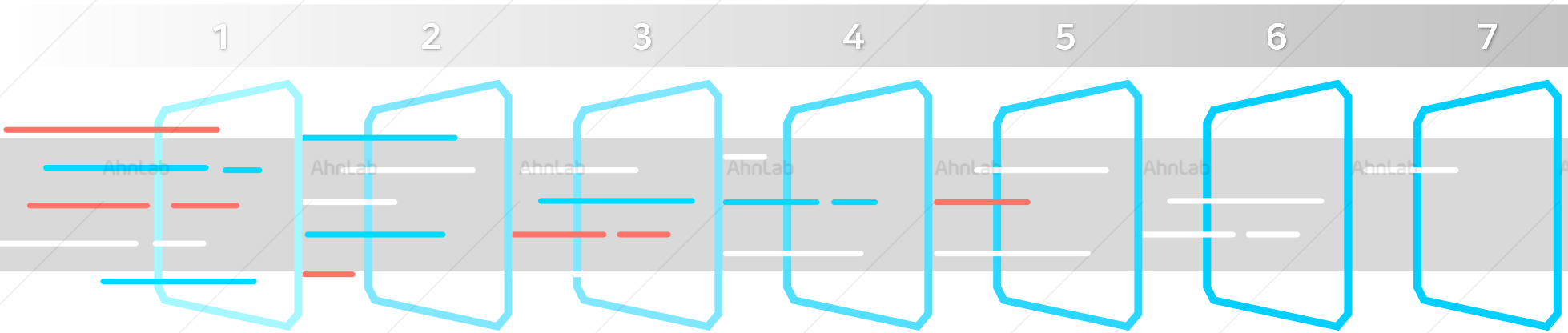
APT 대응 솔루션

APT 공격에 사용되는 기법 대응
예: 파일, C&C 통신, URL, 취약점

04. APT 제품 컨셉

MDS는 7단계 수집/분석/대응 프로세스를 가지고 있습니다.
다양한 기법으로 APT 공격을 대응합니다.

Zero-Day
랜섬웨어
네트워크 공격
APT 공격
Known 위협
Unknown 위협
취약점 공격



1.네트워크 검사
- C&C (Command & Control) 통신 탐지
- SNORT/YARA

2.파일 수집
- HTTP, HTTP v2, FTP, SMTP 등
- 실행파일 수집 (네트워크)
- 비실행 파일 (네트워크)
- 예: exe, docx, pdf, hwp 등

3.에이전트 탐지
- 실행 보류(Execution Hold)
- 비정상 행위 탐지
- 의심 파일 수집 (AI)

4.캐싱/예외
- 화이트리스트
- 블랙리스트
- 캐싱
- 인증서 검증

5.정적 검사
- 시그니처 기반 검사
- URL 검사
- 개인정보 (MTA)
- 피싱메일 (MTA)

6. 동적 검사
- 샌드박스 검사
- 실행/비실행 파일 전용 엔진
- Anti-VM 회피 기능

7. 에이전트 대응
- 파일 삭제
- 호스트 격리

04. APT 제품 컨셉

동적 검사 (Sandbox) – 실행 파일 (PE, Portable Executable)

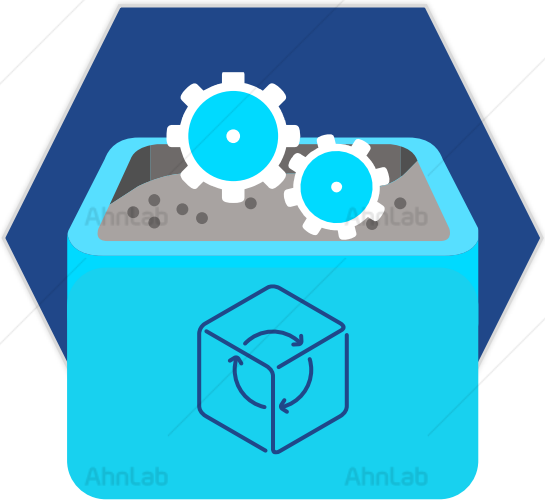
알려지지 않은 위협(Unknown), 파일을 실행하여 악성 행위를 포함하는지 분석합니다.

01
실제 PC 유사 환경 파일 실행
- WIN 7, 10, 11 지원
- MS Office, 한글 HWP 포함 (공식 라이선스)
- Edge, Chrome 브라우저
- 실제 파일 실행 스크린샷 제공

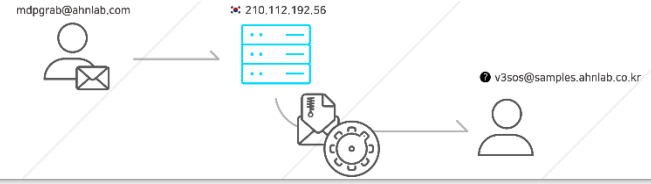
02
프로세스 행위 분석
- 행위 정보 (악성/일반)

파일, 프로세스, 레지스트리, 스레드, 디스크, 디렉터리, 디버깅, 후킹, 라이브러리, 메모리, 익스플로잇, 암호화 등
- 웜, 트로이목마
- 다운로더, 스파이웨어 등

03
네트워크 행위 분석
- API 호출 / C&C 서버 호출
- TCP/UDP/HTTP/HTTPS
- URL 분석 / 이상 트래픽 식별
- PACP 파일 다운로드 제공



04
Dropped 파일 분석
- 이벤트로 인해 생성된 파일 정보
- 특정 파일 핀포인트 분석 제공

05
공격 흐름도 분석


06
분석 요약 / 레포트 제공
- 위험도: High, Medium, Low, Grey 등
- 진단명, 감염 경로, 탐지 대상, 공격자
- 백신 진단 내역
- 탐지 원인 및 대응방안 제공

04. APT 제품 컨셉

동적 검사 (Sandbox) – 비실행형 (Non-PE)

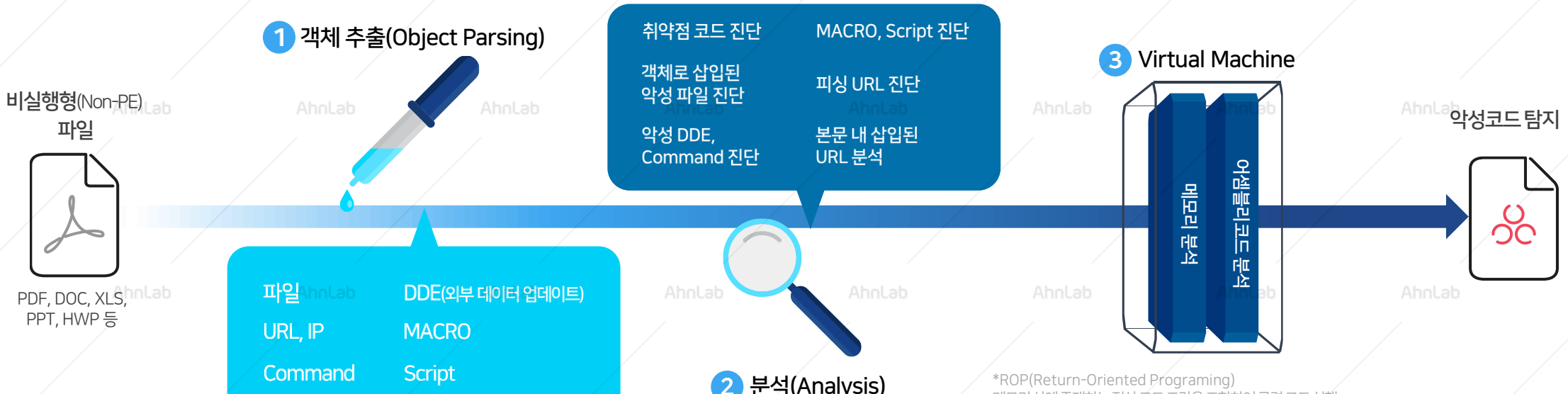
문서를 포함하는 비실행형 파일 분석, 실행 파일과 달라야 합니다. 실행 파일 분석과는 다른 엔진을 사용합니다.

정적 콘텐트 분석 COSMOS 엔진

- 파일 정적 분석을 통한 빠른 검사 진행 및 진단 포인트별 상세 분석 리포팅 제공
- 추출된 객체(Object)를 MDS 기존 분석 프로세스와 연계 분석하여 탐지율 개선
- 신변종 악성코드에 대응하기 위해, 단기간 개발 가능한 경량화된 모듈형 엔진 프레임워크 제공

동적 콘텐트 분석 DICA 엔진

- 애플리케이션 취약점 공격 단계에서 악성코드 탐지
- 제로데이(zero-day) 취약점을 이용한 신종 악성코드 탐지
- ROP 공격/ 힙 스프레이 공격



*ROP(Return-Oriented Programing)
메모리 상에 존재하는 정상 코드 조각을 조합하여 공격 코드 실행

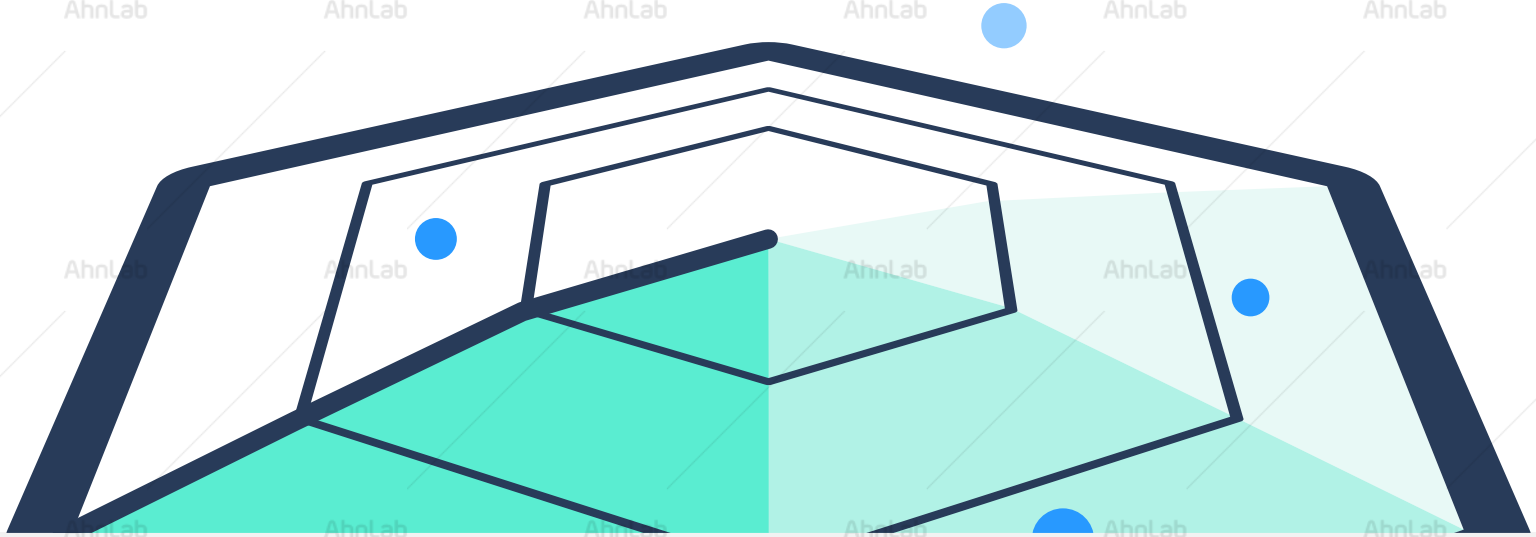
*힙 스프레이(Heap Spray)
데이터가 동적으로 할당되는 메모리 공간인 힙(Heap) 영역에 의미 없는 NOP 값을 채워 쉘코드 실행

04. APT 제품 컨셉

직접적인 대응 방안에 대해서 생각했다라고 한다면,

또 다른 관점의 대응 방안에 대해서 생각해 보도록 합시다.

원인 파악



05.
분석 제품 컨셉

AhnLab

05. 분석 제품 컨셉

일반적으로 사고가 발생하였을 경우 여러분들의 대처 형태는??

Worst Case

일단 원복

백업본 복구

재설치

Best Case

원인 파악을 위한 시도

네트워크 절체 후 보관

디스크 이미징

취약 환경(점)을 보완하지 않는다면,
이미 한번 학습한 공격자는 반드시 재이용 합니다.

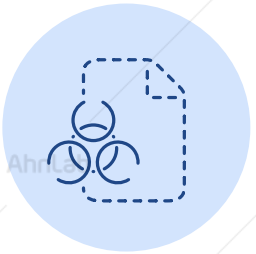
05. 분석 제품 컨셉

공격자 입장에서 생각해보자

Anti Forensic

로그 변조

시스템 파괴



파일 숨김

로그 삭제

루트킷

모니터링 도구를 이용해 중앙에서 관리한다면….

05. 분석 제품 컨셉

컨셉별 보안 제품군

01

시그니처 기반

- 백신제품군 (엔드포인트)
- IDS / IPS 제품군 (네트워크)

- **알려진 위협** (Known Attack)
- **시그니처 기반 정적 분석**
- **실시간 감시 및 차단**

02

SandBox 기반

- APT 솔루션 (네트워크)
- APT 솔루션 (클라우드)

- **알려지지 않은 위협** (UnKnown Attack)
- **가상화 샌드박스 기반 동적 분석**
- **파일 실행 보류**

03

모니터링 기반

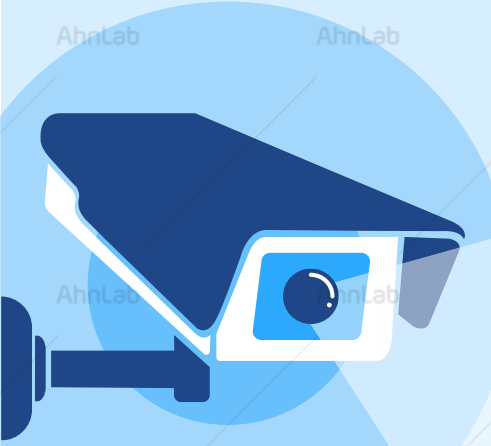
- EDR (엔드포인트)
- NDR (네트워크)

- **위협의 가능성이 있는 모든 행위** (Known, Unknown)
- **실제 시스템 기반 행위 및 이벤트 분석**
- **프로세스 종료, 파일 삭제, 네트워크 격리**

05. 분석 제품 컨셉

EDR을 실생활에 비유하면, CCTV와 같은 역할을 합니다.

- 능동적인 모니터링을 통해 위협을 선제적으로 식별하고, 장기적인 위협 대응 체계 수립에 기여



범죄 현장에 **CCTV를 설치하자**

Threat Hunting과 사고 분석에 활용

엔드포인트 **로깅 강화**

- 파일
- 네트워크
- 레지스트리
- 프로세스
- 시스템 설정
- 사용자 행위
- Who, When, Where, What, How

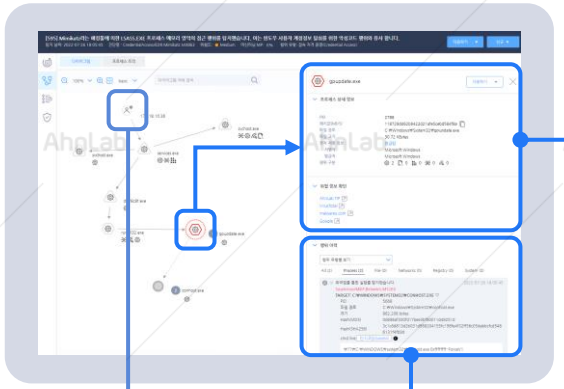
침해 조사에 필요한 정보를 **안정적으로 상시 수집**

별도 시스템에 **로그 백업**

05. 분석 제품 컨셉 - 다양한 분석 정보 제공

트리거 프로세스별 상세 정보(PID, MD5, Sha256, 경로, 크기, 전자서명, 타겟별 상세 정보)를 제공합니다.

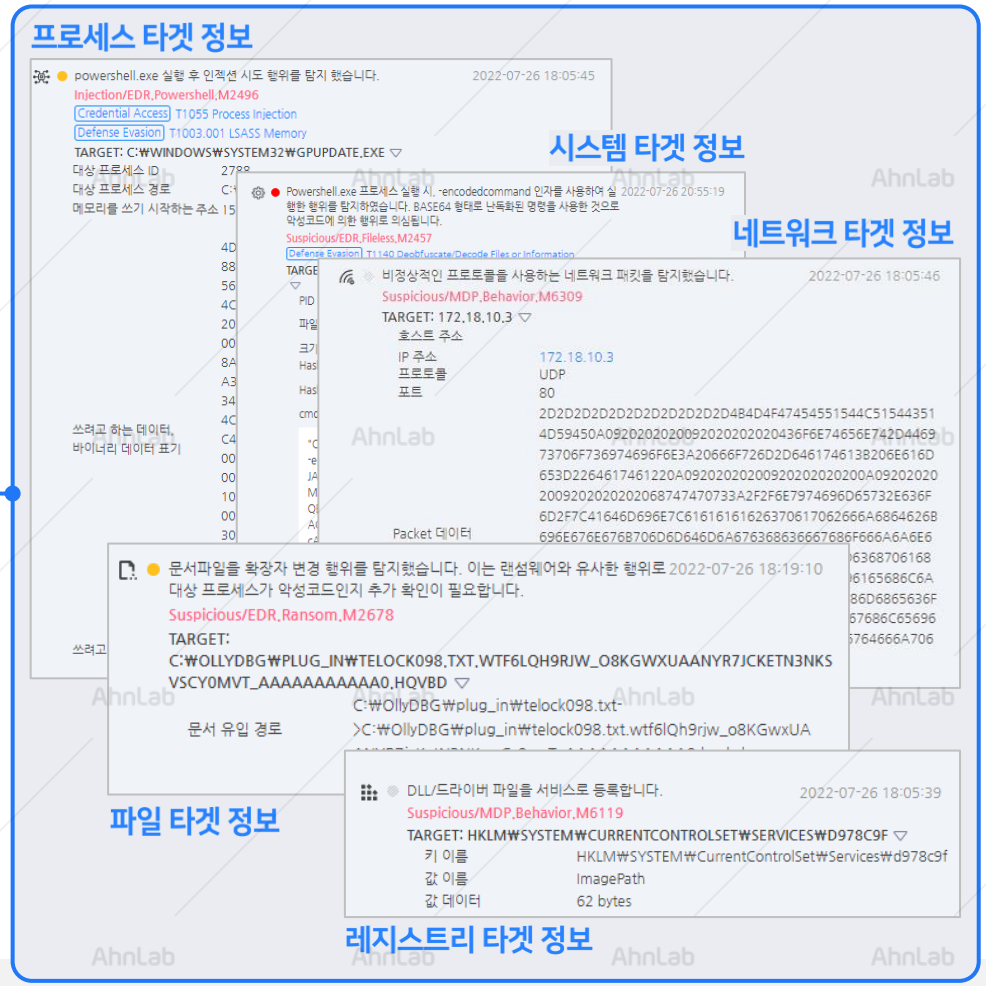
- 프로세스, 파일, 시스템, 레지스트리, 네트워크 타겟별 행위 및 상세 정보 제공 → 유형, 위험도 별 로그 종류 정렬
- 각 프로세스, 파일에 대한 실시간 대응 가능



선택한 프로세스 정보/대응 메뉴

프로세스 상세 팝업

내부 Client<->Client 통신 정보



05. 분석 제품 컨셉 – 타임라인 분석

탐지된 위협 분석 정보를 **'레벨링(leveling)' 하여 타임라인 별로 정보를 제공**합니다.

- 주요 행위별(객체 종류/위험도), 일반 행위별(객체 종류), Artifacts 정보를 기준으로 사전 분류
- 필요조건 조합으로 타임라인 확인 가능

05. 분석 제품 컨셉 - EDR 활용 시 어려운 점

EDR에서 탐지되는 이벤트가 많은데, 무엇이 이상한 것이지?

악성코드 탐지? 오탐 아냐?

우리는 악성코드 대응, 분석 가능한 전문 인력 없는데

백신처럼 자동으로 대응 해줄 수 없나?

위협 탐지, 대응, 모니터링을 위한 인프라 뿐만 아니라
의심스러운 행위에 대한 판단을 할 수 있는 분석 전문가가 필요

05. 분석 제품 컨셉 – MDR 서비스 제공

Without MDR 서비스

수많은 Alert 발생으로 사용 어려움

고급 보안 전문가 인력 확보 어려움

백신처럼 자동화된 분석 및 대응 필요

With MDR 서비스

효과 01

보안 위협에 대한 실시간 대응 체계 확보

전문인력에 의한 관제 및 대응 프로세스에 따라 보안성 강화

효과 02

보안 위협에 대한 가시성 확보

고객 환경에서 발생하는 방대한 위협 이벤트 중에서 분석 대상 분류
안랩 전문가에 의해 위협에 대한 정밀 분석 및 직접 대응 수행

효과 03

선제적인 위협 사냥을 통한 사고 방지

주요 보안 이슈에 대한 신규 탐지 정책 설정을 통한 이전 위협 행위 유무 조사

효과 04

보안 예방을 위하여 다양한 형태의 컨텐츠 제공

End Point 환경에서 발생된 위협 및 의심 행위에 대한 분석 보고서 제공
보안 위협과 이에 대응하는 최신 보안 기술 동향 리포트 제공
수시 분석된 신규 취약점 정보에 대한 정보 보고서 제공

비용 절감, 효율성 ↑

More security, More freedom

AhnLab