당신의 안티바이러스는 과연 안전한가?

: PC/모바일 안티바이러스 성능 및 랜섬웨어 탐지 분석 연구

Analyze antivirus performance and ransomware detection for PC and mobile

KAIST Cyber Security Research Center
Kangsik Shin, Researcher

2025. 03.

KAIST CSRC Cyber Security Research Center

연구 목적

- 기존 상용 소프트웨어 평가 항목 및 정보보호 제품 성능평가 항목의 모호함
- 최적의 시험 환경 구축 및 테스트 시나리오 수집 및 연구 필요
- 보안 언론 매체를 통한 투명한 연구결과 공개 및 신뢰성 확보
- 제조사와 정부 공공기관 및 기업 보안 담당자와의 공감대 형성/커뮤니티 구축
- **정보보호 솔루션의 신뢰성 검증을 통한 기술적 가치 및 인지도 상승**

[별표 2]

상용소프트웨어 평가항목 및 배점한도(제3조제2항 관련)

평가부문	평가항목	평가기준
기능성	기능구현 완전성	제안요청서에서 요구하는 기능이 모두 구현되어 있는지 여부를 평가한다.
	기능구현 정확성	구현된 모든 기능들이 정상적으로 동작하는지 여부를 평가한다.
	상호 운용성	제안요청서에서 요구하는 다른 프로그램 또는 시스템과의 연동(데이터 교환, 인터페이스 요구 충족 등) 가능 여부를 평가한다.
	보안성	권가되지 않은 사람이나 시스템의 접근을 방지하여 정보 및 데이터를 보호하는지 여부를 평가한다.
	표준 준수성	제안요청서에서 요구하는 규제 또는 표준을 준수하여 개발되었는지 여부를 평가한다.

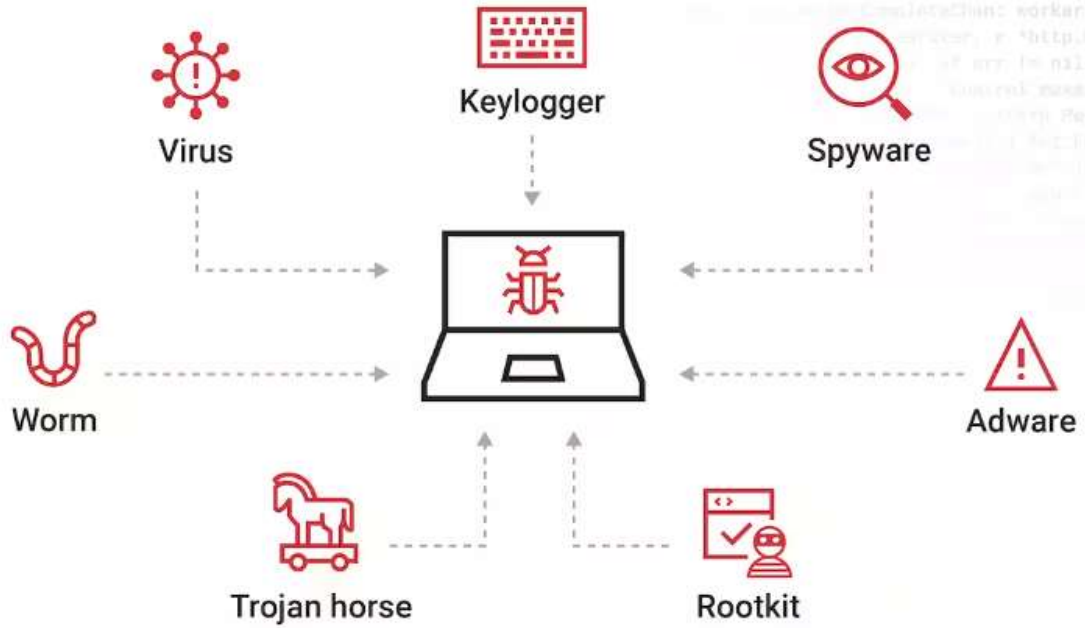
History

- `22년 10월 SCA(Software Composition Analysis) 도구의 오픈소스 취약점 탐지 정확도 및 기능 평가
- `23년 1월 화이트박스 테스팅 자동화 도구 평가를 통해 라인 및 브랜치 커버리지 평가
- `23년 3월 안티바이러스(Anti-Virus) 소프트웨어 평가를 통해 기존 평가 방법과 다른 악성코드 탐지 평가
- `23년 12월 모바일 안티바이러스(Mobile Anti-Virus) 제품 성능 평가
- `24년 2월 생성형 AI 활용한 PC 안티바이러스(Anti-Virus)에 대한 성능 평가 완료
- **`25년 2월 유/무료 PC 안티바이러스 평가 및 랜섬웨어 성능 평가 완료(with Mobile)**
- 기존 국내 소프트웨어 테스트 평가 항목으로 평가 하기 어려운 상용 소프트웨어에 대한 평가 기준 수립

>> KAIST 사이버보안연구센터 블로그게시

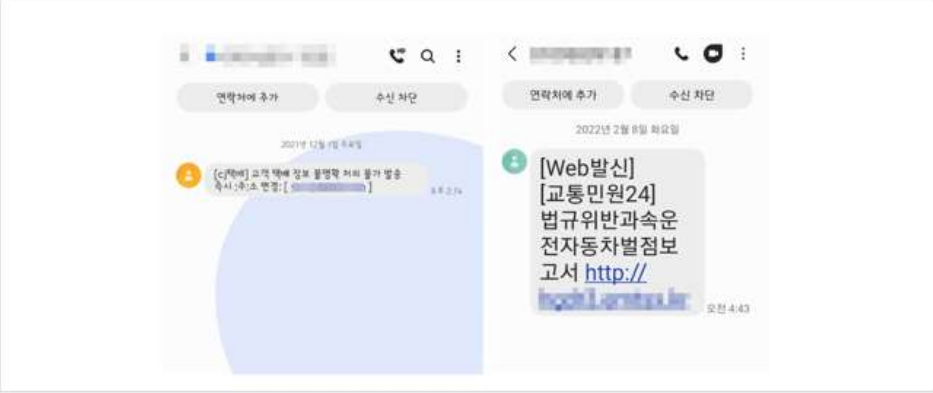
악성코드(Malware)란?

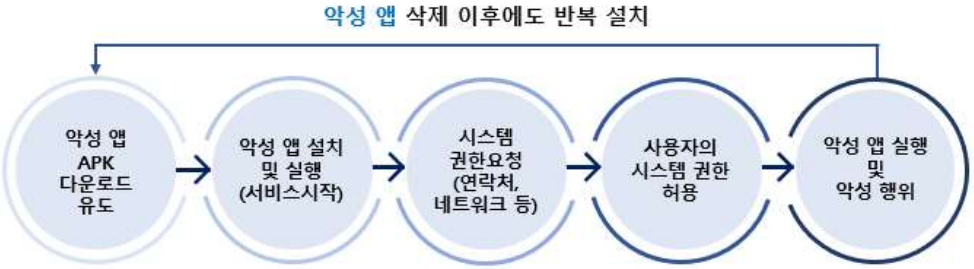
- 악성 소프트웨어라고도 하며 컴퓨터, 서버, 네트워크 등에 악영향을 끼치는 모든 소프트웨어
- (**초기**) 감염 시 컴퓨터의 성능이 느려지고, 오작동을 일으키는 단순 컴퓨터 바이러스
- (**현재**) 디지털 환경 변화로 지능화되고 기능이 복잡해져, 다양한 악성 행위를 하는 악성 소프트웨어 통칭



모바일 악성코드(Malware)는 무엇인가?

- 모바일 기기를 제어하거나 모바일 기기 내 정보를 획득하기 위해 만든 악의적인 소프트웨어
- 외부 링크를 통해 설치를 유도하거나, 다운로더 앱을 통해 은닉하여 악성 앱을 설치
- 2015년 기점 이후, PC 보다 **모바일기기 사용률 증가로** 모바일 악성 앱 또한 활동이 **증가함**
  - 페이크앱, 크립토재킹, 스미싱, 보이스피싱, 가짜뱅킹 앱 등

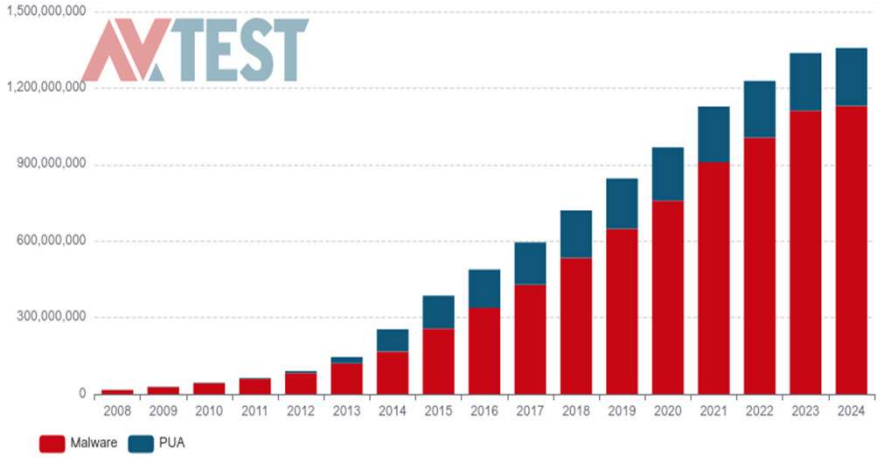




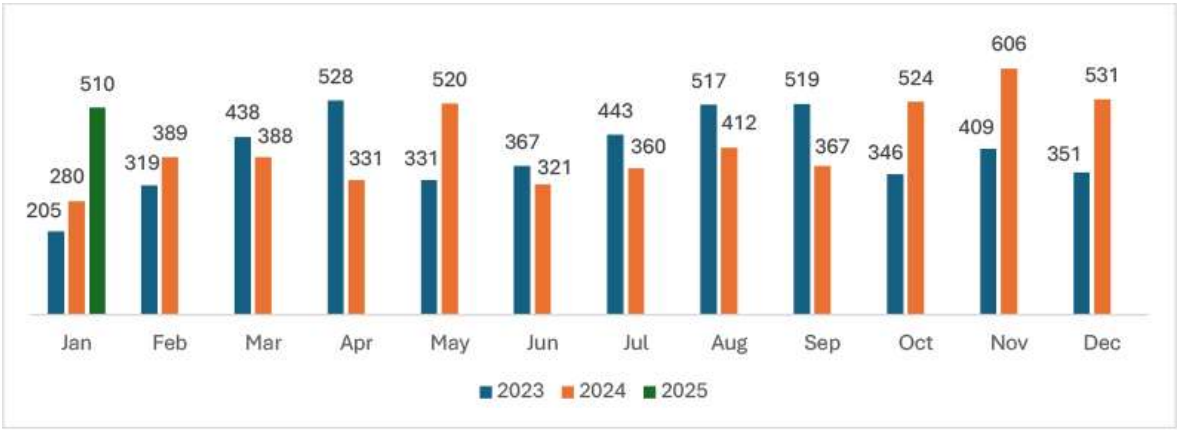
출처: 금융보안원, 김준형 형사 블로그

전 세계 악성코드 현황

- 디지털 전환에 맞게 생성형 AI 기술과 다양한 서비스가 생겨나면서 악성코드 또한 폭발적으로 증가
- 독일 통계 기업인 STATISTA 조사에 따르면 하루평균 약 56만개의 악성코드가 탐지되고 있음
- 또한, 랜섬웨어의 경우 전체 악성코드에서 발생 빈도가 점차 증가하고 있음
- 전세계 기업의 약 60%가 랜섬웨어 피해를 경험할 정도로 기업을 대상으로 지속적인 공격 발생



악성코드 발생 현황(2024년 기준)



월별 랜섬웨어 공격 발생 빈도(2025)

* PUA(Potentially Unwanted Program) : 광고 팝업, 성능 저하와 같은 보안 위험 유발

출처 : statista, AV-TEST, Cyfirma

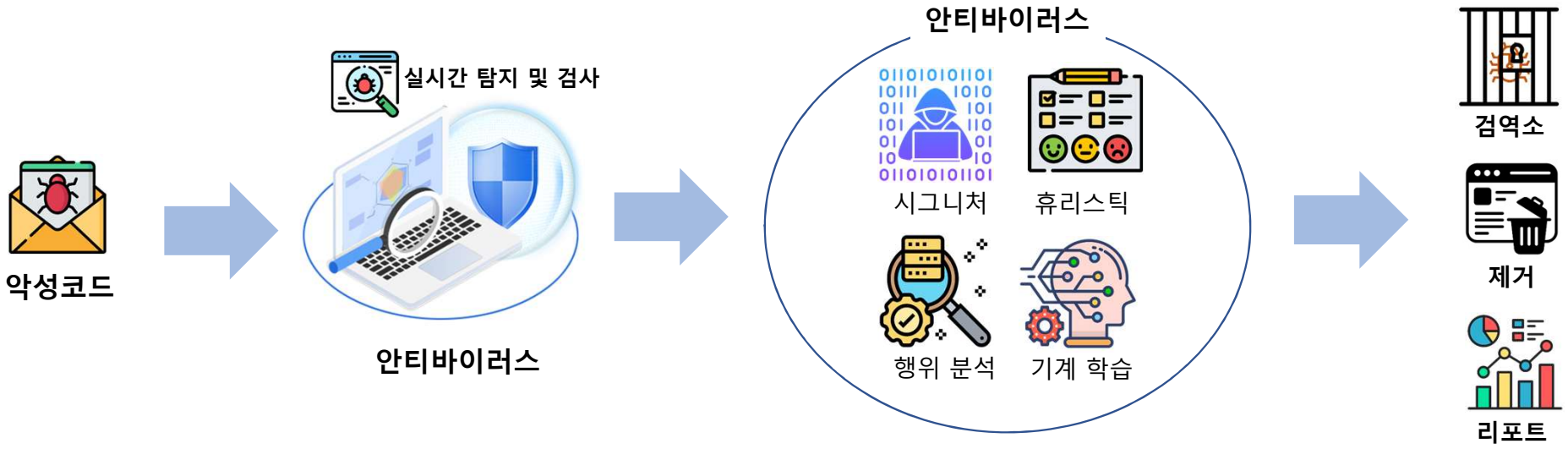
안티바이러스(Anti-Virus) 란?

- 악성 소프트웨어를 찾아내서 제거하는 기능을 갖춘 컴퓨터 프로그램
- **"바이러스 검사 소프트웨어"**라고도 하며, 국내에선 "**컴퓨터 백신**"으로 알려짐
- 컴퓨터 시스템 및 드라이브 검사를 통해 바이러스 정보(시그니처)와 일치하는 바이러스 식별
- (**과거**) 바이러스, 스파이웨어, 애드웨어 등 **악성코드 유형(특성)에 따라 특화된 제품 출시**
- (**최근**) 악성코드의 지능화/정교화와 다양한 악성행위 통합 수행에 따른 특화 제품 무의미
  - 악성코드 유형에 **특화된 제품 쇠퇴** → 통합된 안티바이러스 제품 주목

PC 악성코드 검사 및 결과

안티바이러스(Anti-Virus) 탐지 기술

- **시그니처 기반 –** 알려진 공격의 패턴 저장하고 비교해 악성코드를 탐지
- **휴리스틱 기반 –** 악성코드의 특징을 분석해 프로파일링 한 정보를 바탕으로 유사도 기반 탐지
- **행위 분석 기반 –** 시스템 변화 유무에 따라 판단, 시스템 모니터링을 통해 공격 패턴을 탐지
- **기계 학습 기반 –** 악성코드에서 수집 및 분석한 Feature 정보를 바탕으로 학습된 모델을 이용한 탐지



안티바이러스(Anti-Virus)의 한계점

- 안티바이러스의 가장 큰 문제는 신규 악성코드의 **생성 속도를 따라잡기 힘듦**
- **안티바이러스를 우회**하기 위해 지능화 및 정교화를 통한 **지속적 진화**
- 안티바이러스에 탐지 되지 않으면 시그니처를 생성 하기 전 감염자 및 피해 발생(피해 확산 가능)
- 파일 압축 및 보호 기술 계층에 대한 탐지 오류
- 잘못된 악성코드 시그니처 패턴 정보로 인한 한계
- 모호한 시그니처로 인해 **정상 프로그램이 악성코드로 오진**
- 시그니처 데이터베이스가 업데이트되지 않으면 신규 악성코드 탐지 제한

기존실험 에서는 한계점에 대한 테스트 진행

PC/모바일 안티바이러스는 무엇이 중요할까?

1	UI/UX 중심의 설계	• 직관적이고 효율적인 인터페이스 제공 • 사용자 경험(User Experience) 중심의 인터페이스 설계
2	플랫폼 및 기기 호환성	• 다양한 디바이스 및 플랫폼에서 호환성을 고려한 안정적 동작 필요 - 하드웨어(CPU 칩셋 등), 운영체제 등 이기종 기기 지원
3	하드웨어 리소스 최적화	• 사용자 작업에 영향이 없는 성능 최적화 필요 - 사용자 PC/모바일 기기 내 하드웨어 자원을 최적화하여 사용
4	악성코드 탐지 성능	• 악성코드, 피싱앱 등 신속한 악성 여부탐지 필요 - 중요 정보가 많은 PC/모바일 기기의 안전을 위한 탐지 성능 중요
5	**신속한 업데이트 & 유지보수**	• 새로운 악성 앱 및 보안 취약점 대응 위해 업데이트 및 유지보수 필요

체계적인 실 환경 기반의 테스트 환경 구현
3개월 간격으로 수집 된 악성코드를 분기마다 테스트 진행(총 3분기)
의견을 통한 다양한 테스트 수행

이전 안티바이러스 성능 평가와의 차이점

AS IS

"안티바이러스 탐지율 위주 및 악성코드의 생애주기 고려하지 않은 시나리오 기반 테스트"

- 대량 악성코드에 대한 탐지율 비교
- 악성코드 확장자별 탐지율 테스트
- 5년 이상 수집된 악성코드 샘플 사용
- 탐지율 위주의 테스트 시나리오 및 샘플

TO BE

"사용자의 궁금증과 안티바이러스 목적에 맞는 테스트 시나리오 기반의 성능 평가"

- 안티바이러스의 최신 악성코드 탐지율 평가
- 사용자들의 요구하는 테스트 항목 수행
- 매 분기 별 테스트를 통한 객관적 성능 평가
- 랜섬웨어 탐지율 및 차단 성능 테스트

안티바이러스의 어떤 점이 궁금할까? – 개인 사용자

주기적인 검사기능이 필요한가요? 실시간 탐지만 켜놓으면 되는거 아닌가요?

확장자별 악성코드 안티바이러스의 성능이 궁금해요

랜섬웨어에 대한 탐지율이 궁금해요

국산제품보다 외산 제품이 더 좋은거 아닌가요?

안티바이러스를 두 개 설치하면 누가 먼저 잡는지 비교해주세요

어떤 안티바이러스가 가장 좋은지 알려주세요

2개이상의 악성코드가 실행되면, 둘다 잡을수 있나요?

무료 안티바이러스와 유료는 성능 차이가 정말 있나요?

안티바이러스의 어떤 점이 궁금할까? –기업 또는 기관

안티바이러스
제품을 추천해주세요

테스트에 사용한
샘플을 제공해주세요

기업 및 공공기관 등

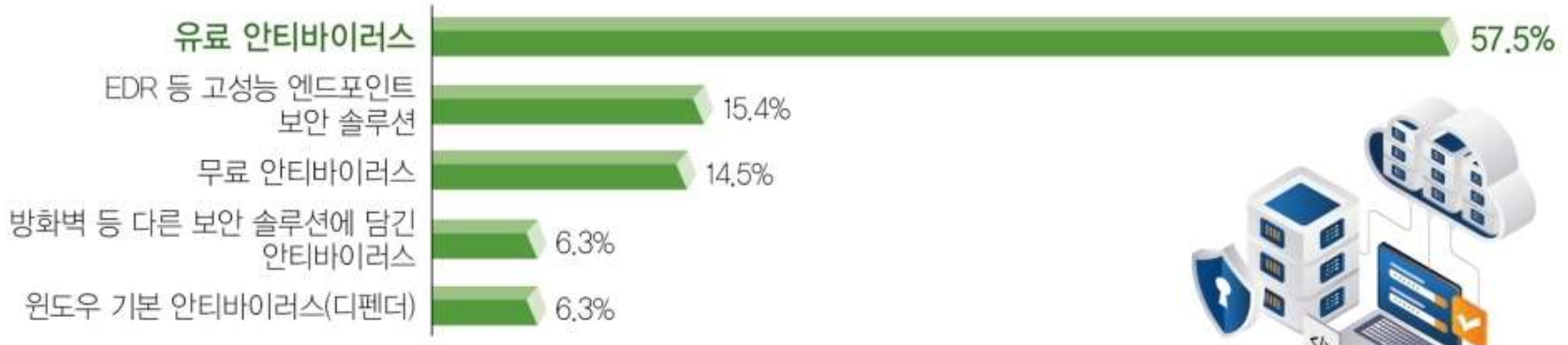
안티바이러스 성능
테스트 방법과 노하우를
알고싶어요

기업(기관)에서 사용하고
있는 안티바이러스 제품
성능이 궁금합니다

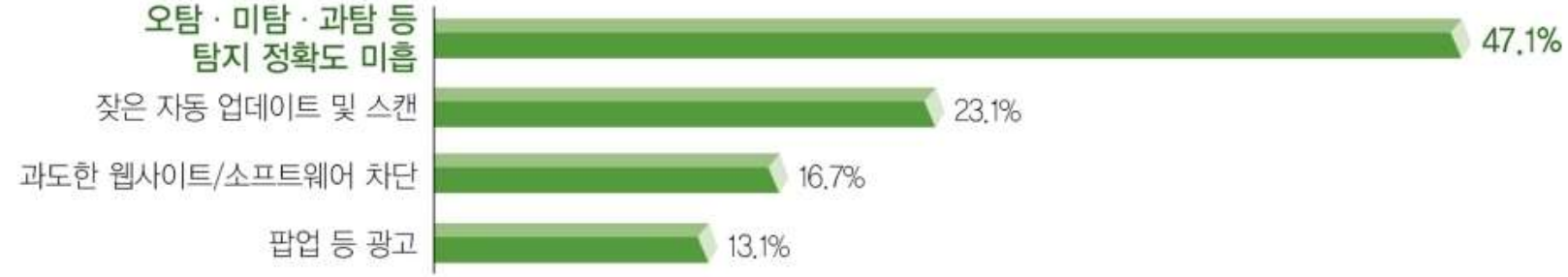
보안뉴스 사전 설문조사

응답자: 약 2300명

Q 귀사는 어떤 종류의 안티바이러스를 사용하고 있나요?



Q 안티바이러스를 사용하면서 가장 불편한 점은 무엇인가요?

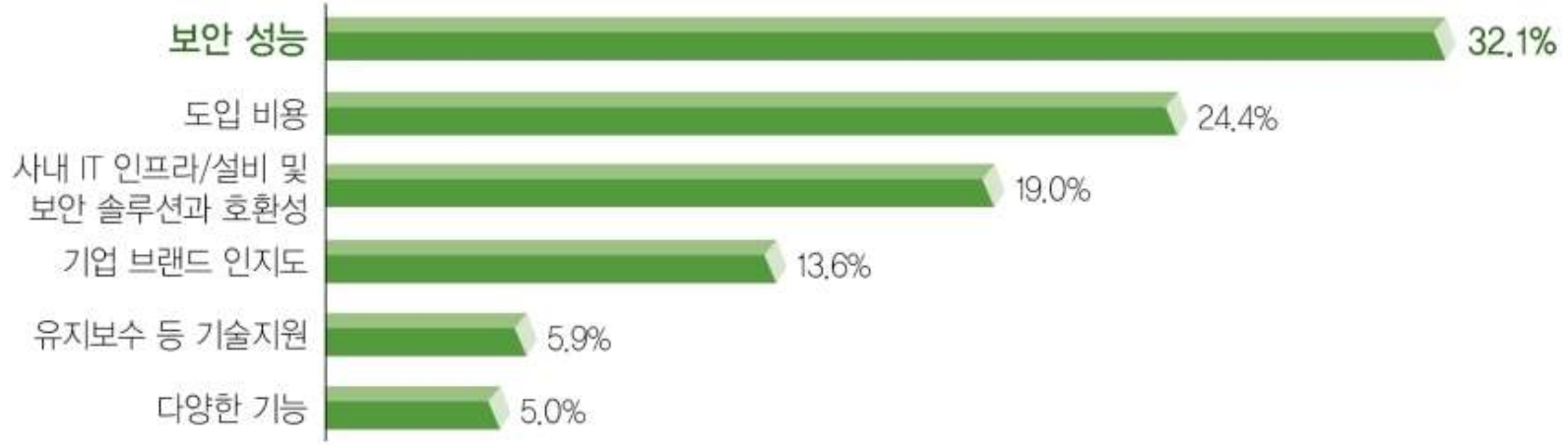


출처: 보안뉴스, [2025 안티바이러스 리포트] 기초가 튼튼해야 보안도 '탄탄'

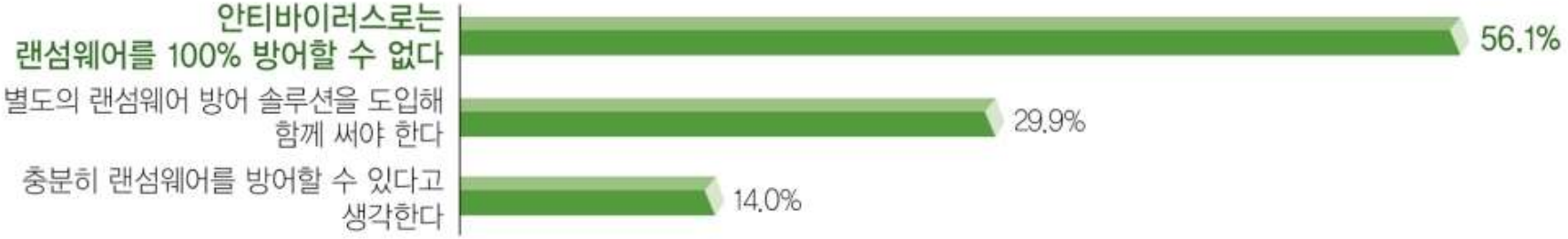
보안뉴스 사전 설문조사

응답자: 약 2300명

Q 귀사의 안티바이러스 선택 기준은 무엇인가요?



Q 대부분의 안티바이러스가 랜섬웨어 방어도 가능하다고 말하고 있습니다. 이에 대해 어떻게 생각하시나요?



출처: 보안뉴스, [2025 안티바이러스 리포트] 기초가 튼튼해야 보안도 '탄탄'

모바일 및 PC 안티바이러스 테스트 백신 및 악성코드 샘플 선정

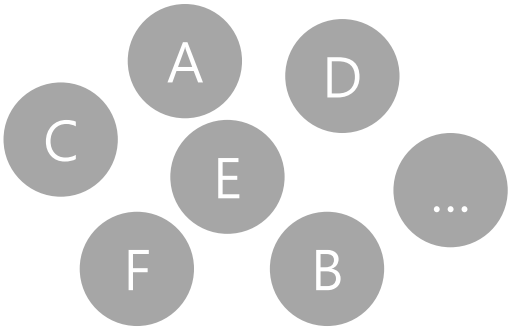
평가 대상 및 선정 방법

- (모바일 기준1) 다운로드 횟수 및 상위 별점 제품
- (모바일 기준2) Android 운영체제 및 태블릿 설치가 가능한 제품
- (모바일 기준3) VirusTotal 내 엔진 제공 및 미제공 각 3개씩

➡ **11개의 후보 제품에서 6개를 선정하여 테스트 진행**

- (PC 기준1) 유료/무료 버전이 있는 안티바이러스 제품 ~~5~~ -> 4개
- (PC 기준2) 국내 및 국외 시장 점유율이 높고 Windows 설치 가능 제품

➡ **약 20개의 후보 제품에서 ~~10~~ -> 9개를 선정하여 테스트 진행**

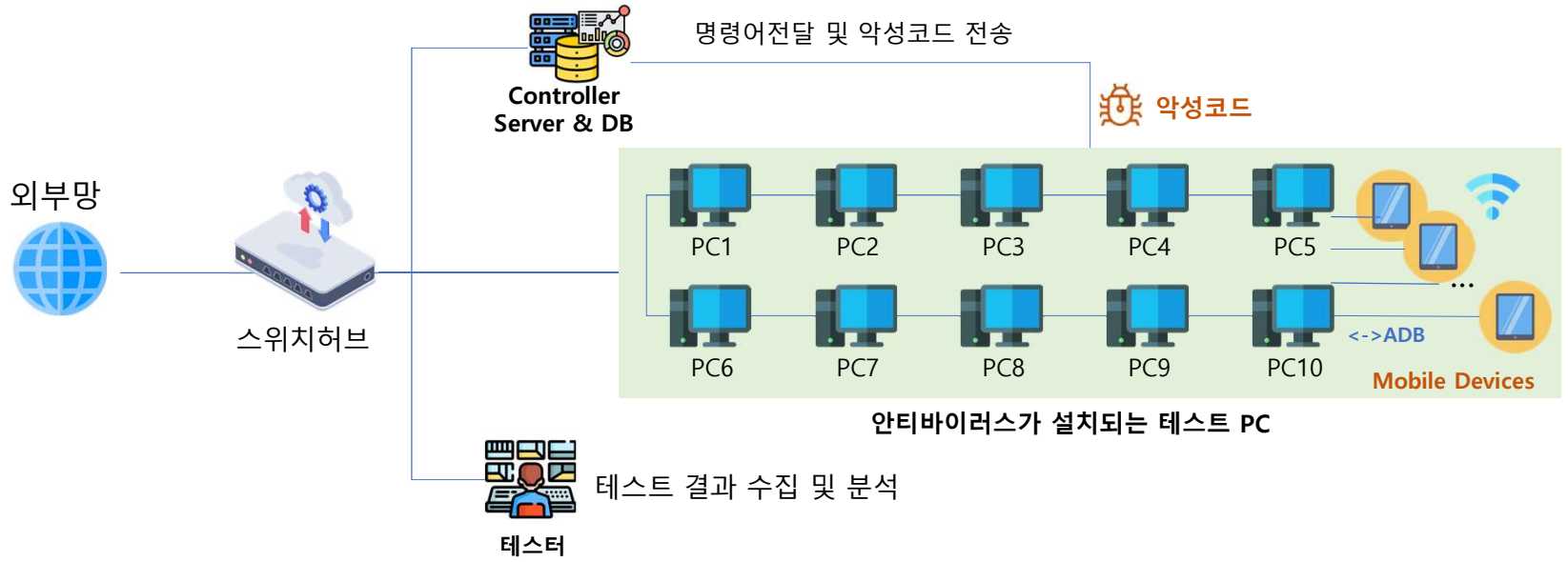


자체 크롤링 및 악성코드 DB 사이트에서 샘플 수집

- (샘플 기준1) 130만개 샘플 중 최근 3개월간 발생된 악성코드
- (샘플 기준2) EXE, DOC, Ransomware 유형별 악성코드
- (샘플 기준3) VirusTotal 내 질의를 통한 정상/비정상 데이터 검증

PC/모바일 안티바이러스 성능 테스트 환경

- 테스터 PC의 Controller 소프트웨어를 통해 Target PC <-> Mobile Devices 기기 제어
- 테스트 단말기 내 APK 파일 설치 및 삭제를 위한 *ADB(USB Cable) 연결을 통한 디바이스 제어
  - 악성 앱 전달/실행/삭제/재부팅 등 사람 개입 최소화, 정확도 및 신뢰성 향상
- 테스트 단말기기는 WiFi를 연결하여 모바일 안티바이러스가 온라인 상태가 되도록 설정



* ADB : Android Debug Bridge

PC/모바일 테스트 소프트웨어 소개

(1) 대상 PC(Mobile) 기기 선택

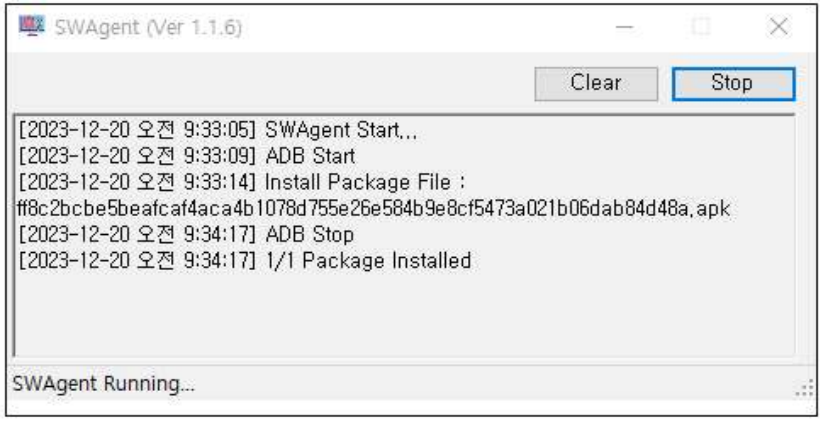
(2) 악성코드/악성앱 파일은 데이터베이스를 통해 관리

(3) 다운로드(전송)/ 설치(실행)/삭제/재부팅 등 명령어 전달

(4) Package Type(Tag) 설정을 통해 테스트 대상 선정

(5) SWAgent는 테스트 PC에 각각 설치되며, 각 명령 및 수행에 대한 로그 표시

Controller(테스터 PC)



Agent(모바일 기기가 연결된 각 PC에 설치)

PC/모바일 성능 테스트 시나리오

PC

- 분기 별(3개월) 신규 악성코드 실시간 및 탐지 정확도
- 유료/무료 버전 안티바이러스 테스트(단일 분기)
- (분기) 실행파일(EXE), 문서파일(doc,ppt,xls,pdf 등), **랜섬웨어 탐지 성능 비교**

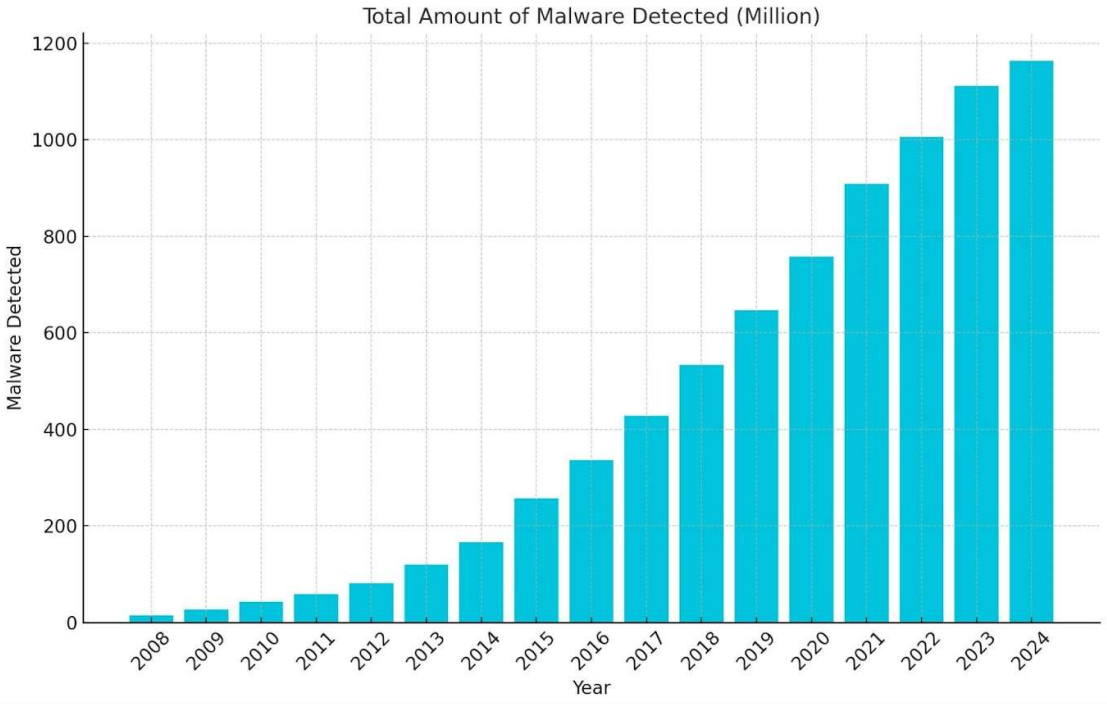
Mobile

- 1년간 수집된 악성 앱에 대한 실시간 및 정밀검사 테스트
- 메이저/마이너 모바일 안티바이러스 테스트(VirusTotal 엔진 제공 기준)

이미지출처 : TechM, ESET

첫번째, 안티바이러스의 신속한 업데이트 및 유지 보수 평가

- 사이버위협 관련 따르면 매일 56만 개의 새로운 악성코드 탐지, 약 10억개의 악성코드 존재
- 전 세계 인터넷 환경에서 매일 약 2,244건의 공격이 발생, 39초 마다 새로운 공격이 발생
- 스마트기기 확산으로 기업과 개인의 디지털 의존도가 높아지고 기술의 발전으로 사이버 공격에 노출



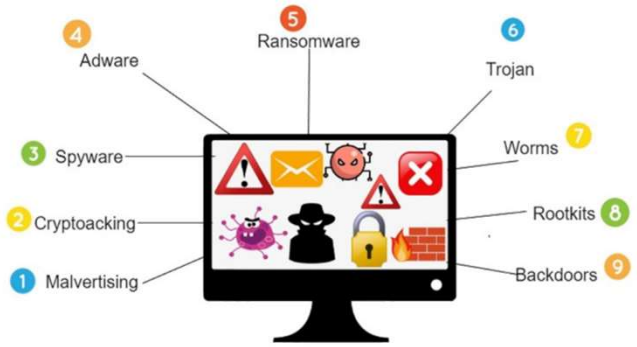
출처 : onecloud, next7it

PC 테스트 시나리오 1

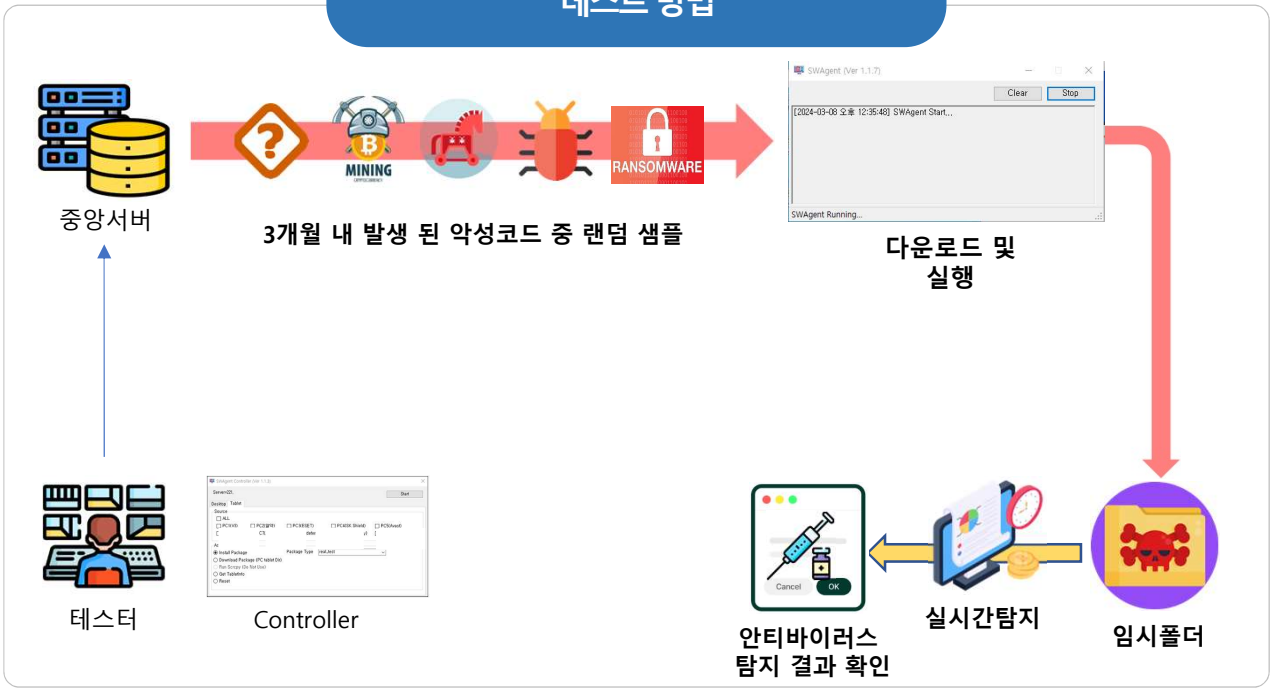
- 최근 3개월간 수집된 악성코드 분기별(3회, 2~4분기) 탐지율 비교
- SWAgent를 이용한 안티바이러스의 다운로드 및 실시간 테스트 수행

테스트 목적

안티바이러스의 신속성 및
유지보수에 따른 탐지율 비교



테스트 방법



PC 테스트 시나리오 1 결과 (2분기 – 실행파일)

비공개

PC 테스트 시나리오 1 결과 (2분기 – 문서형파일)

비공개

PC 테스트 시나리오 1 결과 (2분기 – 랜섬웨어)

비공개

PC 테스트 시나리오 1 결과 (3분기 – 실행파일)

비공개

PC 테스트 시나리오 1 결과 (3분기 – 문서형)

비공개

PC 테스트 시나리오 1 결과 (3분기 – 랜섬웨어)

비공개

PC 테스트 시나리오 1 결과 (4분기 – 실행파일)

비공개

PC 테스트 시나리오 1 결과 (4분기 – 문서형)

비공개

PC 테스트 시나리오 1 결과 (4분기 – 랜섬웨어)

비공개

두번째, 안티바이러스는 구매하여 사용해야 할까?

- 개인마다 다른 관점으로 인해 유/무료 안티바이러스 사용 여부가 다르다
- 소프트웨어 불법 다운로드로 인해 무료 인식이 강하며, 자신은 바이러스에 걸리지 않는다라는 자신감
- 안티바이러스를 설치하면 느려지는거 같고, 오히려 악영향을 끼치는 거 같다
- 유료 안티바이러스 제품 구매에 대한 부담감
- 대부분 기본 Windows Defender 또는 무료로도 충분히 내 PC가 안전할 것이라고 생각함

VS

무료 안티바이러스 vs 유료 안티바이러스

- 개인 또는 비영리 사용자에게 무료로 안티바이러스를 이용할 수 있도록 제공
- 같은 버전이라고 할지라도 영리기업에게는 유료로 판매하며, 별도의 차별화된 서비스 제공
- 무료 안티바이러스 배포로 인해 일반인들의 인지도는 높아졌지만 업계에선 안 좋은 선례를 남김
- 대표적인 무료 안티바이러스로는 Windows 운영체제에 기본 탑재된 Windows Defender가 있음
- 유료 안티바이러스는 운영체제에 상관없이 1년 기준으로 금액 마다 1~3 PC 지원가능(₩8,000 ~ ₩60,000↑)

안티바이러스 소프트웨어	
[펼치기 · 접기]	
엔진	백신 목록
V3	V3 · V3 Lite
비트디펜더	비트디펜더 · 바이러스체이서 · 알약 · 터보백신 · nProtect · 바이로봇 · EMSISOFT
Avira	아비라 · 엑소스피어
ClamAV	ClamAV · ClamWin
어베스트	AVG · Avast 어베스트 · norton 노턴 시큐리티
자체 엔진	트렌드마이크로 · Comodo · ESET · herdprotect · IKARUS · McAfee · kaspersky 카스퍼스키 · Malwarebytes 멀웨어바이트 · Panda Cloud Antivirus · Microsoft Defender · 키콤백신 · AppCheck 앱체크 · 네이버 백신

이미지 출처 : "안티바이러스" 나무위키

안티바이러스 유/무료 비교

- 잠재 고객 확보 및 데이터 수집 목적의 무료 안티바이러스 제공
- 무료와 유료 안티바이러스의 가장 특징 중 하나는 부가기능 및 업데이트 빈도 여부

특성	무료 안티바이러스	유료 안티바이러스
비용	무료	유료 (구독 또는 일회성 구매)
기본 악성코드 탐지/제거	지원	지원
실시간 스캔	제한적	지원
고급 위협 탐지	제한적	지원
랜섬웨어 보호	대부분 없음	지원
방화벽	대부분 없음	지원
이메일 보호	대부분 없음	지원
업데이트	낮음 or 수동	자동 업데이트
기술 지원	일부 미지원	지원
다중 기기 보호	대부분 단일 기기	다중 기기 지원(1~5↑)
광고	있음	없음
시스템 성능 영향	제품마다 다름	최적화
기타: VPN, 비밀번호 관리자 등	대부분 없음	일부 지원

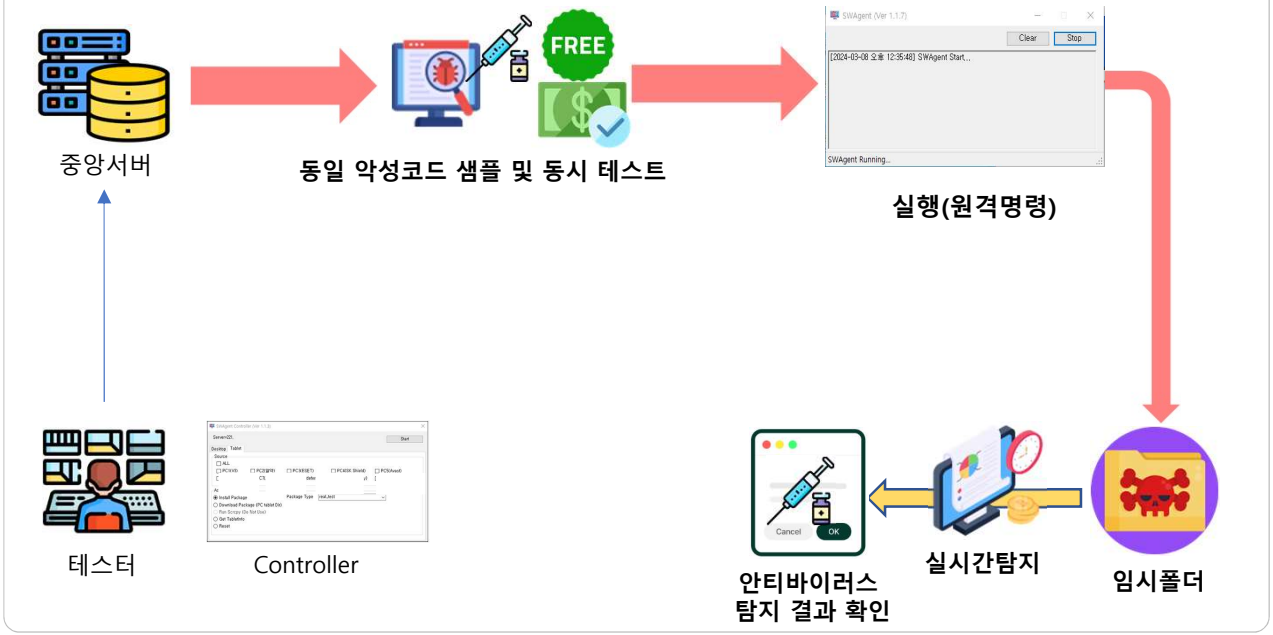
PC 테스트 시나리오 2

- 안티바이러스 제품 중 무료 5개와 동일한 제품의 유료버전 5개 제품에 대한 탐지 성능 비교 수행
- SWAgent를 이용한 유/무료 안티바이러스의 실시간 테스트 수행 및 탐지 결과 비교

테스트 목적

안티바이러스의
유/무료 탐지율 비교

테스트 방법



PC 테스트 시나리오 2 결과

비공개

PC 테스트 시나리오 2 결과

비공개

세번째, 랜섬웨어(Ransomware)를 안티바이러스가 탐지할 수 있을까?

- 랜섬웨어는 이용자의 데이터(문서, 이미지, 중요 시스템파일 등)을 암호화하고 금전을 요구하는 악성코드

Ransom(몸값) + Software(소프트웨어) 의 합성어

시스템을 잠그거나 데이터를 암호화하여 이를 인질로 삼아 금전을 요구하는 악성코드

구분	일반 악성코드	랜섬웨어
유포	웹사이트, 이메일, 취약점 등 유포방식 동일	
감염	소프트웨어 취약점 또는 직접 실행으로 악성코드 감염	
동작	정보 및 파일 유출, DDoS 공격 등	문서, 사진, MBR 등 중요데이터 암호화
대응	유포지 및 *C&C 서버 차단	유포지 및 C&C 서버 차단 ※ 복호화 키가 저장된 서버와의 경로는 X
치료	안티바이러스를 통해 치료	안티바이러스를 통해 치료 ※ 단, 암호화된 파일은 복구가 어려움
피해	개인, 금융 정보 유출 등 2차 공격 피해	암호화된 파일에 대한 복구를 빌미로 금전 요구

**C&C(Command & Control) 서버 : 악성코드 감염 시 해당 서버에 연결되어 해커의 명령을 수행*

출처 : KISA, 랜섬웨어 대응 가이드라인(2023)

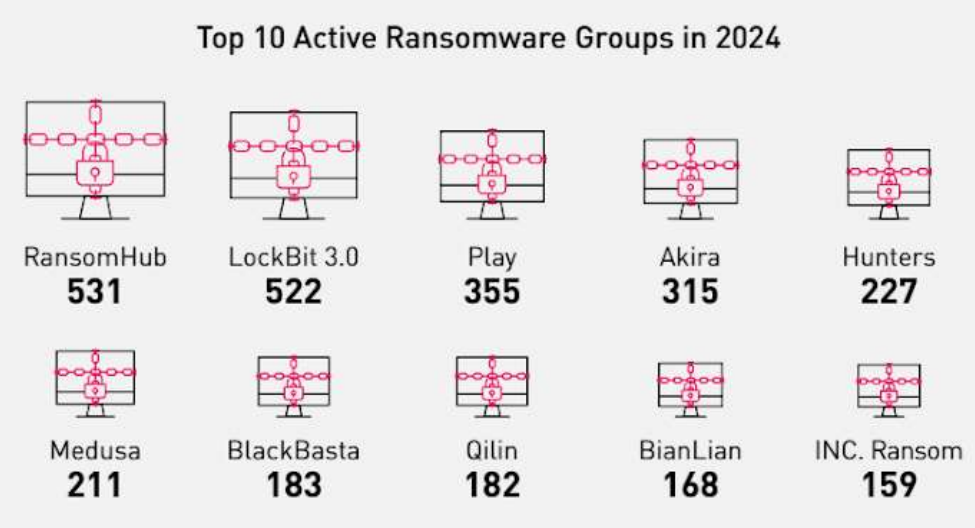
랜섬웨어(Ransomware) 공격 절차

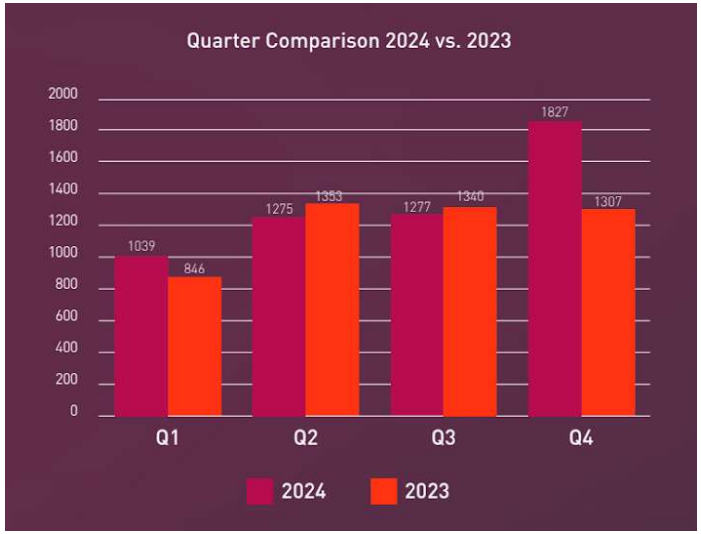
- 랜섬웨어는 실행(감염) 후 공유 폴더 등 클라우드 서버, USB, 외장하드로 확산을 시도
- 케르베르(Cerber), 락키(Locky), 워너크라이(WannaCry), 클롭(Clop), 콘티(Conti) 등 해커그룹마다 특징 존재

출처 : KISA, 랜섬웨어 대응 가이드라인(2023)

주요 랜섬웨어 트랜드 및 공격 동향

- LockBit, BlackCat(ALPHV) 등 조직적인 랜섬웨어 공격 활동을 통한 전 세계 기업 피해 확산 -> FBI 검거
- RansomHub, Fog, BlackSuit 등 새로운 조직 그룹 등장으로 인한 피해 지속 -> 46개의 새로운 그룹 등장
- 무차별 공격이 아닌 계획적인 목표를 통한 전략적 랜섬웨어 공격 집중
  - 랜섬웨어 공격 시 타격이 큰 제조, 의료, 교육, 에너지(인프라) 위주의 공격
  - 생성형 AI(음성, 이메일 등)을 이용한 정교하고 체계적인 공격이 지속적으로 증가 예상





출처 : cyberint, thehackernews, zscaler

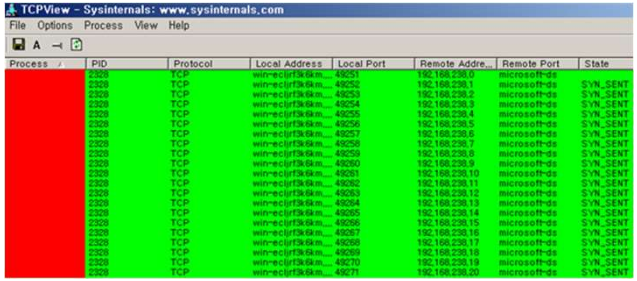
랜섬웨어(Ransomware)의 진화

- 가상화폐의 익명성 보장이라는 특성으로 인해 몸값(데이터 복구) 지불하는 수단으로 활동 및 공격성 증가
- 초창기 파일을 압축하고 암호화하는 단순 형태에서 시스템 복원 드라이브 제거, MBR 훼손 등 지능화됨

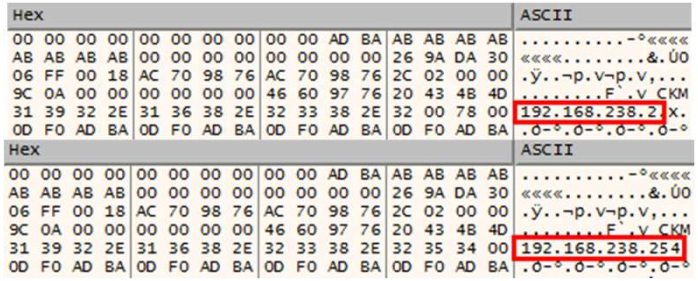
출처 : 랜섬웨어의 동향과 서비스형 Conti 동작 원리 살펴보기(2021)

현재의 랜섬웨어(Ransomware)는?

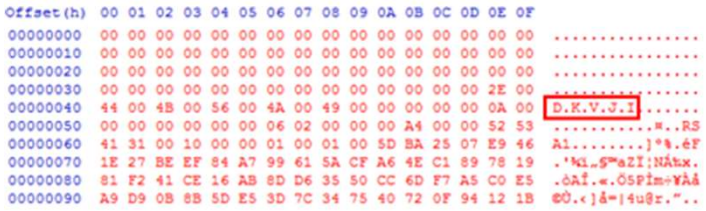
- 서비스형 랜섬웨어(Ransomware-as-a-Service, RaaS)를 통해 특정 타겟을 노린 사이버 위협 증가
- SMB 취약점처럼 같은 네트워크 대역의 PC에 랜섬웨어를 전파하여 피해를 확산 시킴
- 대표적인 서비스형 랜섬웨어 Conti 동작 원리
  - 개인이 아닌 기관이나 기업을 특정하여 공격하며, 파일 복호화 뿐만 아니라 민감정보를 빌미로 몸값 요구



<SMB 포트 스캔>



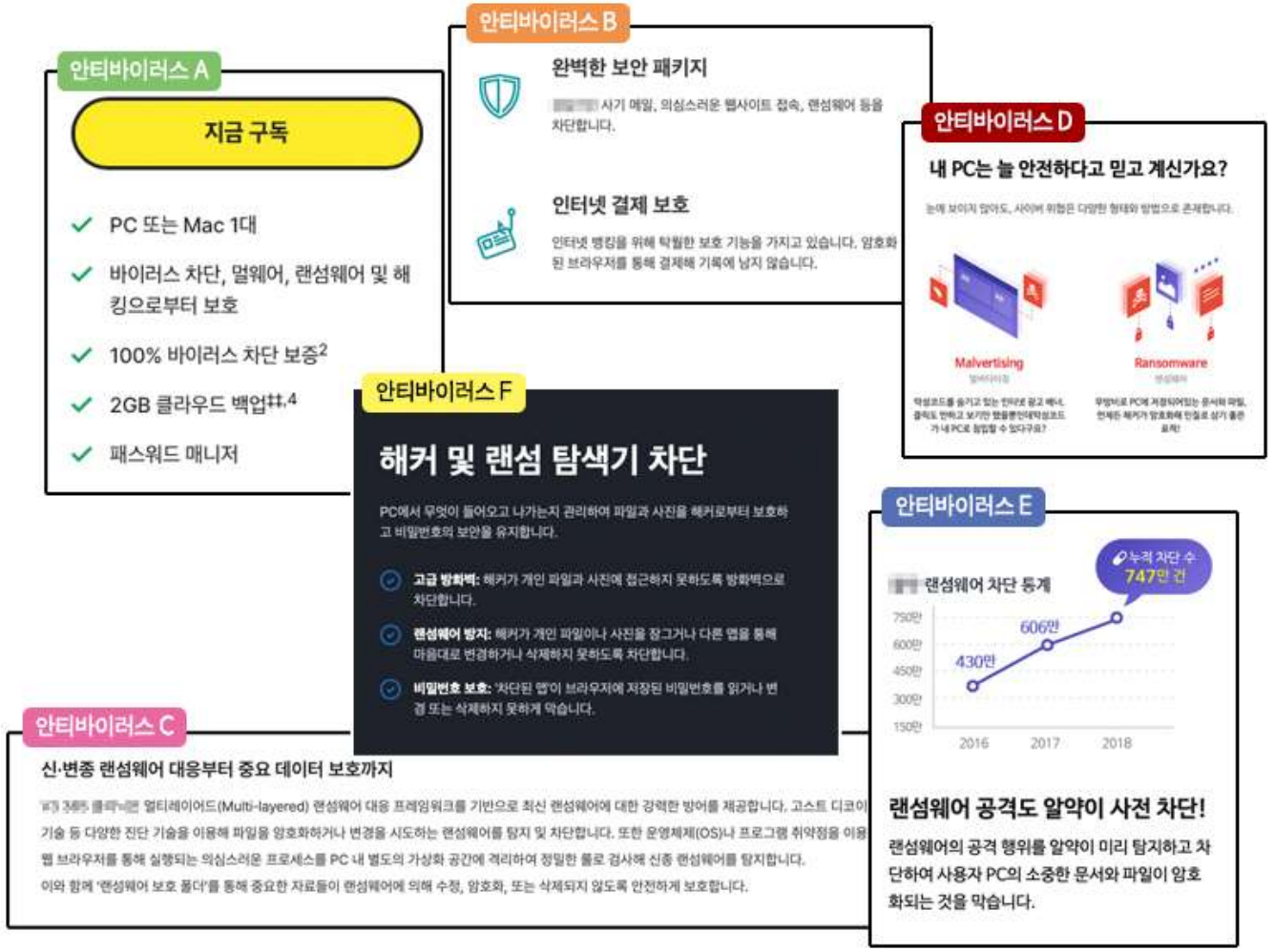
<네트워크 스캔 주소>



<DKVJI 시그니처 삽입>

<랜섬노트>

안티바이러스의 랜섬웨어 탐지 기능



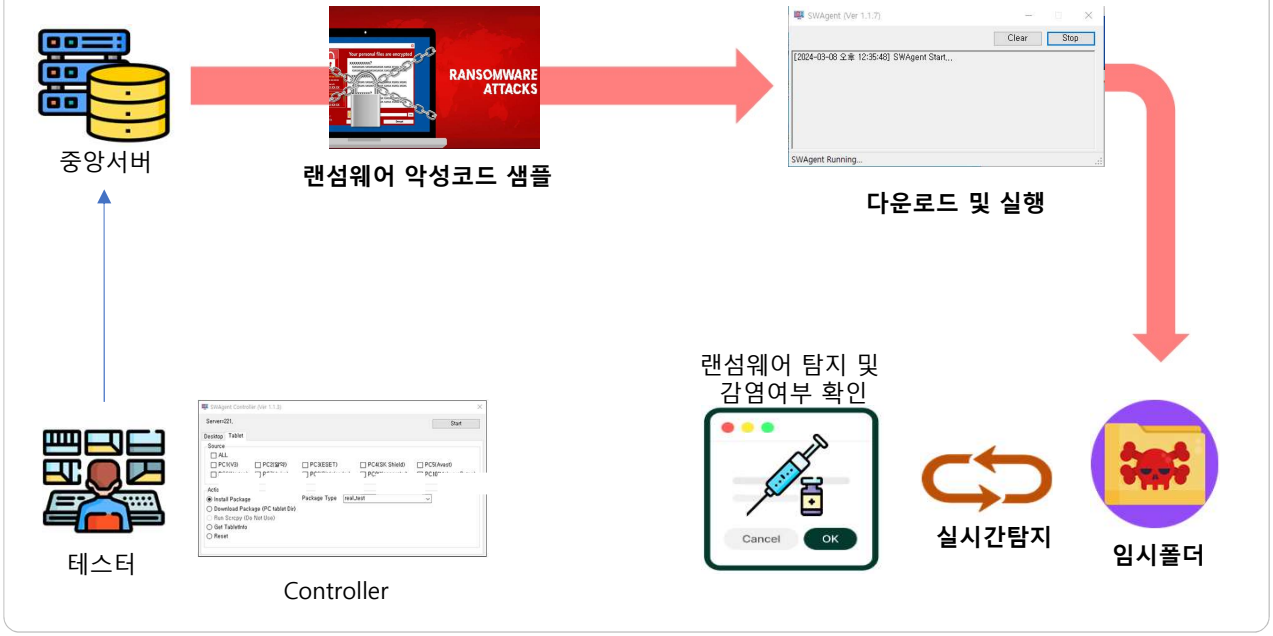
PC 테스트 시나리오 3

- 최근 3개월간 수집된 랜섬웨어에 대한 분기별 탐지율 비교
- 동작마다 약 5분~10분 정도 랜섬웨어 동작 탐지 또는 암호화가 될때까지 기다림

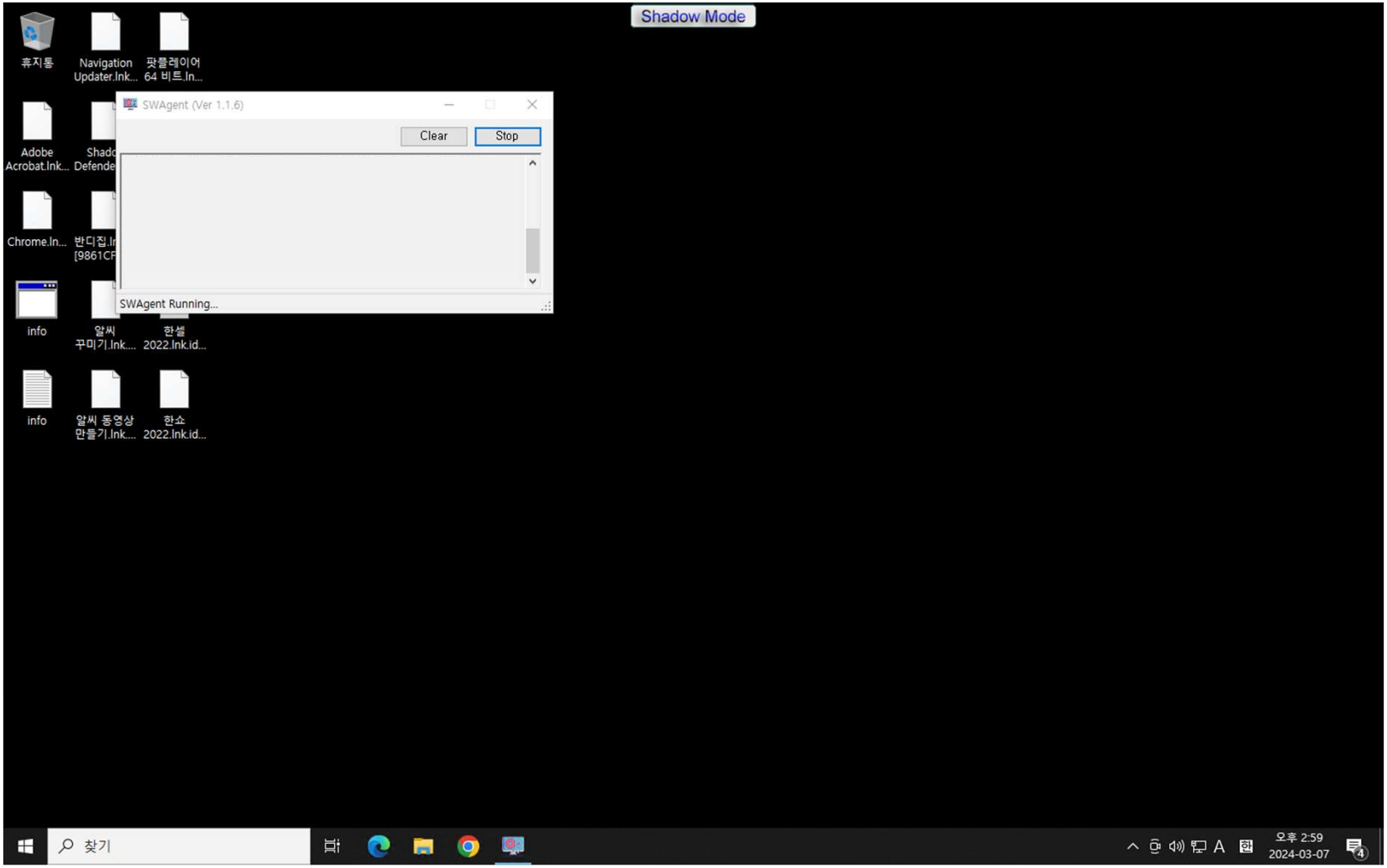
테스트 목적

안티바이러스 별
랜섬웨어의 실시간 및
다운로드 테스트 비교

테스트 방법



PC 테스트 시나리오 3 결과



PC 테스트 시나리오 3 결과

비공개

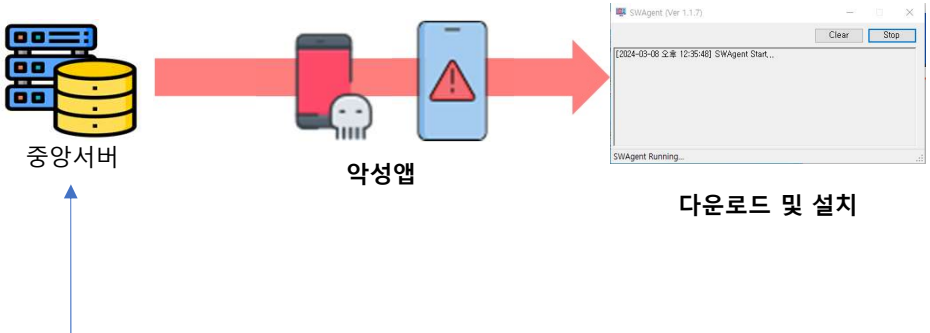
모바일 테스트 시나리오 1

- 2024년 한해 동안 수집된 악성코드들 중 랜덤 샘플링한 악성 앱(APK)에 대한 실시간 및 정밀검사 테스트
- 메이저/마이너 모바일 안티바이러스 비교(VirusTotal 엔진 제공 기준)

테스트 목적

한해 수집된 악성 앱을 통한
모바일 안티바이러스
성능 비교

테스트 방법



- 악성코드 샘플 중 무작위로 샘플링 된 악성앱
- 탐지율이 높은 100개 앱 설치

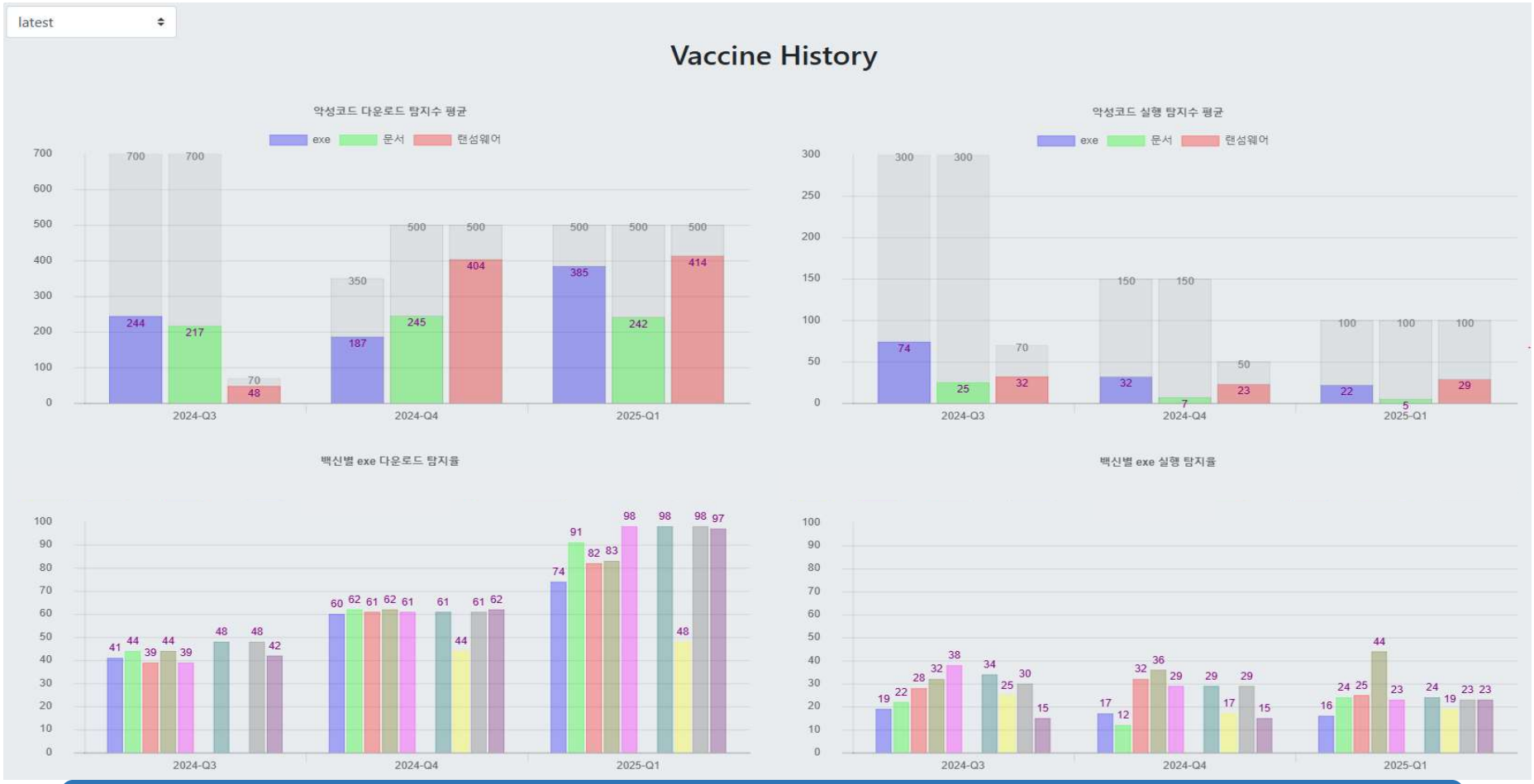
모바일 안티바이러스 검사 및
실시간 탐지

모바일 테스트 시나리오 1 결과(정밀검사)

비공개

모바일 테스트 시나리오 1 결과 (실시간탐지)

비공개



공개용 안티바이러스 탐지 테스트 결과 서비스 준비 중

결론

기술적 측면

- 탐지 규칙과 표준화 된 기준이 없어 악성코드 별 탐지율 통계가 어려움
- 랜섬웨어 탐지는 되었지만, 암호화 되는 것은 막지 못하는 안티바이러스가 있음
- 제조사마다 차이는 있지만, 유료(메이저) 안티바이러스에 성능 차이 있음

사용자 측면

- 알 수 없는 출처의 SMS 및 타인이 제공하는 URL 접근 금지
- 주기적인 안티바이러스 정밀 검사 수행 및 최신 업데이트 유지

보완사항

- 다양한 랜섬웨어 그룹 및 타입을 통한 랜섬웨어 탐지 및 차단 테스트
- C&C 서버 차단 및 활동하지 않는 악성코드에 대한 악성 유무
- *PUA 및 GameHack 등 탐지명 및 탐지 규칙에 대한 표준화 필요

*PUA (Potentially Unwanted Application) : 잠재적으로 원하지 않는 프로그램

THANK YOU

ksshin90@kaist.ac.kr