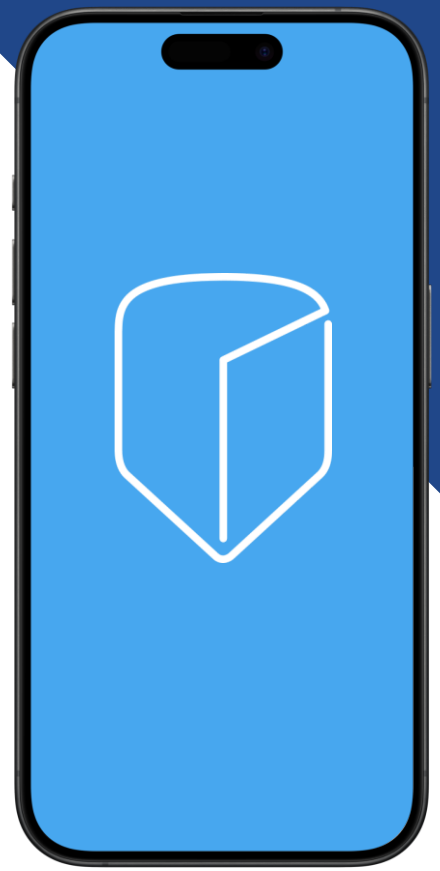
AhnLab

Mobile Engine Suite for iOS

More security,
More freedom



표준제안서

AhnLab

Table of Contents

AhnLab

1. 모바일 위협 동향

1-1. 모바일 악성코드 증가 추이

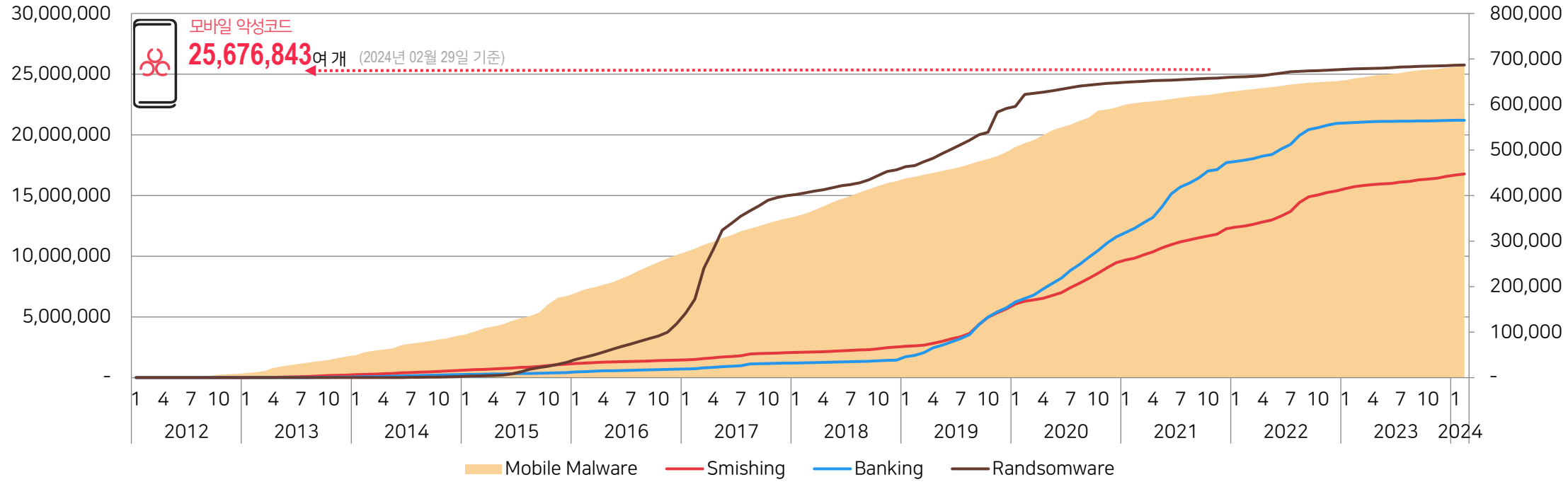
모바일 금융 거래 환경을 직·간접적으로 위협하는 악성코드, 스미싱, 보이스피싱 등의 공격은 증가하고 다각화 되고 있습니다.
ex) 문자 메시지를 통해 악성 앱을 설치하는 스미싱 공격, 금융 서비스와 유사하게 제작된 뱅킹 사칭 앱 등

모바일 악성코드
2,567만여 개

스미싱 악성코드	447,647여개	(2019년 상반기부터 증가 추세)
Banking 사칭 악성코드	565,314여개	(2019년 하반기부터 증가 추세)
모바일 랜섬웨어	686,928여개	(2016년 하반기부터 증가 추세)

~ 2024.02.29 누적

모바일 악성코드 증가 추이



1-2. 모바일 거래(Transaction) 구간 보호 필요성

모바일 시대에 도래하면서 다양한 유형의 위협이 발견되었고, 이를 통해 사용자들의 디바이스를 노리는 모바일 보안 위협 행위도 빈번하게 늘어나고 있습니다.
안전한 스마트폰 거래(Transaction)에 대한 개인의 불안과 기업의 리스크가 증가하고 있으며, 이와 관련한 법·사회적 요구사항 또한 고도화되고 있습니다.

“안전한 모바일 거래(Transaction) 방안의 필요성”

사용자가 입력한 개인정보 및 거래 비밀번호 화면이 그대로 외부에 송출된다면?	사용자 디바이스에 스파이웨어가 심어져 있다면?	디바이스가 탈옥된 상태로, 취약한 상태라면?
위변조 되지 않은 공식 애플리케이션으로 정상 접속한 사용자인가?	사용자가 실제와 유사한 피싱 사이트에서 거래를 한다면?	사용자가 모바일 디바이스에서 안심하고 이용할 수 있는 서비스일까?

1-3. 모바일 특화 위협 대응 필요성

스마트폰 대중화 및 모바일 디바이스 다변화에 따라 모바일 위협은 나날이 증가하고 있지만, 기존 PC 환경에 특화된 보안 대응 역량만으로는 복합적으로 진화하는 모바일 위협 대응에 한계가 있습니다.

스마트폰 보급과 사용자 세대 교체	국내 스마트폰 회선 수 56,16만대 (MSIT, 2024.02) 양분화된 OS플랫폼과 낮아지는 iOS 사용자의 연령대(2024.02) - 18~29세: iOS(65%) > Android(35%)) - 30대: Android(59%) > iOS(41%) - 40대~70대: Android(75%) > iOS(25%) - Total: Android(71%) > iOS(29%)	전 연령대 타겟의 입체적 보안 필요
모바일 뱅킹 사용자 증가	모바일 뱅킹, 조회, 가계부 등의 애플리케이션 보급 확대 인터넷 뱅킹 이용실적 중 모바일 뱅킹 건수 85.2% 차지 모바일 뱅킹 등록 고객 수 2억 704만명 (한국은행, 2023.03)	정보 거래에 대한 집중적인 대응 필요
스미싱, 앱 위•변조 및 악성코드 증가	사용자 정보를 노리는 악성코드의 위협, 꾸준히 증가 (2024년 2월 기준, 악성코드 수 2,567만 여 개) 공식 마켓(Google/Apple) 외 3rd Party 마켓 내 악성 앱 활동 악성 위·변조 앱을 통한 정보 유출, 금융 피해 등 2차 피해	유연한 대응 역량 필요

1-4. iOS에서의 보안 안전성에 대한 의문

보안뉴스
애플의 인기 높은 자동화 앱에서 발견된 취약점, 긴급 패치 요망
2024-02-23 13:02 국제부 문가용 기자

ZDNET Korea
아이메시지로 사용자 몰래 아이폰 감염시킨다
2023/12/28 10:06 남혁우 기자

매일경제
"해킹 취약지점 발견"…아이폰15 출시 앞둔 애플 '날벼락'
2023-09-08 13:29:29 김인오 기자

보안뉴스
아이폰에 스파이웨어 심는 '트라이앵귤레이션 작전', 정교한 사슬처럼 엮인 공격
2024-01-02 18:35 국제부 문가용 기자

보안뉴스
아이폰의 차단 모드, 모든 위협을 차단하는 건 아니다
2023-12-06 12:28 국제부 문가용 기자

VOA
"북한 해킹조직, '애플 운영체제' 악용 암호화폐 탈취…정권 자금 마련"
2023.11.30 조상진

iOS는 정말 안전할까요?

1-5. iOS에서 발견된 취약점

CVE체계(Common Vulnerabilities and Exposure)는 소프트웨어의 보안 취약점을 가리키는 표기법으로, iOS도 예외는 아닙니다.
매년 지속적으로 iOS의 취약점은 늘어나고 있으며, Apple 에서도 이를 보완하여 패치를 진행하지만 사용자가 최신 소프트웨어를 유지해야 보완이 가능한 구조입니다.

애플 | 여러 제품

CVE-2022-48618

Apple 여러 제품 메모리 손상 취약점

Apple iOS, iPadOS, macOS, tvOS 및 watchOS에는 읽기 및 쓰기 기능이 있는 공격자가 포인터 인증을 우회할 수 있는 TOCTOU(검사 시간/사용 시간) 메모리 손상 취약점이 포함되어 있습니다.

- **조치:** 공급업체 지침에 따라 완화 조치를 적용하거나 완화 조치를 사용할 수 없는 경우 제품 사용을 중단하십시오.
- **랜섬웨어 캠페인에 사용되는 것으로 알려져 있습니까?:** 알 수 없음
- **추가된 날짜:** 2024-01-31
- **마감일:** 2024-02-21

애플 | iOS와 아이패드OS

CVE-2024-23296

Apple 여러 제품 메모리 손상 취약점

Apple iOS, iPadOS, macOS, tvOS 및 watchOS RTKit에는 임의 커널 읽기 및 쓰기 기능을 가진 공격자가 커널 메모리 보호를 우회할 수 있는 메모리 손상 취약점이 포함되어 있습니다.

- **조치:** 공급업체 지침에 따라 완화 조치를 적용하거나 완화 조치를 사용할 수 없는 경우 제품 사용을 중단하십시오.
- **랜섬웨어 캠페인에 사용되는 것으로 알려져 있습니까?:** 알 수 없음
- **추가된 날짜:** 2024-03-06
- **마감일:** 2024-03-27

애플 | iOS와 아이패드OS

CVE-2024-23225

Apple 여러 제품 메모리 손상 취약점

Apple iOS, iPadOS, macOS, tvOS, watchOS 및 VisionOS 커널에는 임의 커널 읽기 및 쓰기 기능을 가진 공격자가 커널 메모리 보호를 우회할 수 있는 메모리 손상 취약점이 포함되어 있습니다.

- **조치:** 공급업체 지침에 따라 완화 조치를 적용하거나 완화 조치를 사용할 수 없는 경우 제품 사용을 중단하십시오.
- **랜섬웨어 캠페인에 사용되는 것으로 알려져 있습니까?:** 알 수 없음
- **추가된 날짜:** 2024-03-06
- **마감일:** 2024-03-27

애플 | 여러 제품

CVE-2024-23222

Apple 여러 제품 유형 혼동 취약성

Apple iOS, iPadOS, macOS, tvOS 및 Safari WebKit에는 악의적으로 제작된 웹 콘텐츠를 처리할 때 코드 실행으로 이어지는 유형 혼동 취약점이 포함되어 있습니다.

- **조치:** 공급업체 지침에 따라 완화 조치를 적용하거나 완화 조치를 사용할 수 없는 경우 제품 사용을 중단하십시오.
- **랜섬웨어 캠페인에 사용되는 것으로 알려져 있습니까?:** 알 수 없음
- **추가된 날짜:** 2024-01-23
- **마감일:** 2024-02-13

1-6. iOS를 향한 다양한 모바일 보안 위협

iOS 환경에서는 플랫폼을 취약하게 하는 탈옥, 탈옥 탐지를 우회하는 후킹 공격, 사용자의 주요 정보를 유출하도록 원격제어 공격 등
iOS 환경에서도 보안 위협으로부터 사용자의 안전한 모바일 이용 환경을 확보할 수 있는 방안이 필요합니다.

- 탈옥 기기는 Apple 정책 상 최신 OS 업데이트 불가
- 사용중인 OS에서 취약점 발생해도 탈옥 시 OS 업데이트 등의 조치 불가
- 취약점 및 탈옥 툴을 활용한 악성 공격에 **멀웨어 감염 및 개인정보 유출 위험 증가**

- 후킹 공격은 일반적인 앱에서 특정 API를 호출한 경우 해당 API를 공격자의 API로 변경
- 공격자가 고객사 앱의 API 자체를 후킹하는 경우 **탈옥 탐지를 우회하는 위험 발생**

- 사용자 기기에 원격제어 앱을 설치하도록 유도하여 기기를 원격으로 조종하는 금융 사기 증가
- 공격자는 사용자의 화면에 표시되는 정보 탈취 및 직접 기기를 제어하여 **개인정보 및 금융정보 유출**

2. Mobile Engine Suite(iOS) 소개

2-1. 제품 개요

Mobile Engine Suite for iOS는 탈옥 탐지, 후킹 탐지, 원격제어 탐지 등 다양한 보안 기능을 제공하는 iOS 전용 보안 제품입니다.
앱 연동 방식이 아닌 SDK 방식으로 제공되며 고객사의 앱 내부에 탑재되어 고객사의 자체 운용이 가능합니다.

AhnLab
Mobile Engine Suite (iOS)

제공 방식

- 앱 연동 방식이 아닌 고객사 앱에 Mobile Engine SDK for iOS를 적용
- 제공하는 SDK를 **고객사 앱에 직접 적용하여 자체 운용하는 방식**

주요 기능

- 탈옥 탐지: iOS 기기의 탈옥 여부 탐지, FlyJB 우회 방지
- 후킹 탐지: Frida와 같은 후킹 툴을 이용한 후킹 여부 탐지
- 후킹 차단: MSHook, FishHook 등 후킹 탐지를 우회하는 후킹 우회 툴 탐지 및 차단
- 원격제어 탐지: 원격제어 앱 동작 여부 탐지
- 앱 위변조 검사: 앱의 다양한 정보를 조합 및 검증하여 앱 위변조 여부 탐지
- 디버거 검사: 악의적인 앱 분석을 차단하기 위해 디버거 탐지 및 방지 수행
- VM 검사: 고객사 앱 구동 환경이 VM인지 VM 여부 검사

기대 효과

- 디바이스 별 정보 제공을 통해 **고객 디바이스 별 위협**을 세부적으로 관리하여 **보이스피싱 예방** 효과 확대
- 탈옥, 후킹 등 취약해진 플랫폼 환경에서 발생할 수 있는 **보안 사고를 사전 방지**
- 고객사의 **능동적인 검사 및 탐지를 통해 효과적인 보안 환경 마련 가능**

2-2. 제품 특장점

AhnLab Mobile Engine Suite for iOS 적용을 통해 iOS 환경의 서비스 이용자에게 안전한 이용 환경을 제공할 수 있습니다.

01

확장된 탐지 방식

탈옥 툴 존재 여부, 프로세스 검사 등 다양한 방식을 활용하여 복합적으로 탈옥 여부를 탐지

02

고객사 환경 지원

고객사 환경에 따라 로컬 기반 앱 위변조 탐지 또는 서버 기반 앱 위변조 탐지 도입 가능

03

iOS 전용 통합 보안

탈옥, 후킹, 원격제어, 앱 위변조, 디버거, VM 탐지 및 검사를 제공하는 iOS 전용 통합 보안 제공

2-3. 컴플라이언스 대응 효과

금융감독위원회의 '모바일 거래 시 디바이스 보안' 대책 마련 요구 및 전자금융거래법 개정안 등 모바일 거래와 관련된 주요 컴플라이언스에 대응할 수 있습니다.

※ 전자금융거래법 개정 법률 제 17354호 "전자금융거래법" 타법개정 (2020.06.09) 및 시행(2020.12.10)
금융회사 또는 전자금융업자 및 전자금융보조업자(이후 "금융회사 등"이라 한다)는 전자금융거래법 제9조 1항에 해당하는 사고로 이용자에게 손해가 발생한 경우 손해 배상 책임 법제화(제9조 1항)
금융회사 등은 접근매체의 위조나 변조로 발생한 경우, 손해 배상 책임이 있음(제9조 1항 1호)
계약체결 또는 거래지시의 전자적 전송이나 처리 과정에서 발생한 사고에 대해 금융회사 등이 이용자에게 손해를 배상하도록 함(제9조 1항 2호)
전자금융거래를 위한 전자적 장치 또는 정보통신망 등에 침입하여 거짓이나 그 밖의 부정한 방법으로 획득한 접근매체의 이용으로 발생한 사고에 대해 금융회사 등이 이용자에게 손해를 배상하도록 함(제9조 1항 3호)
금융회사 등은 전자금융거래가 안전하게 처리될 수 있도록 선량한 관리자로서의 주의를 다하여야 함(제21조 1항 1호)
금융회사 및 전자금융업자는 전자적 침해행위로 인하여 전자금융기반시설이 교란 · 마비되는 등의 사고(이하 "침해사고"라 한다)가 발생한 때에는 금융위원회에 지체 없이 이를 알려야 할 의무가 있음(제21조의5 1항)
금융회사 및 전자금융업자는 침해사고가 발생하면 그 원인을 분석하고 피해의 확산을 방지하기 위하여 필요한 조치를 해야함(제21조의5 2항)
금융회사 등은 접근매체의 사용 및 관리함에 있어 범죄에 이용할 목적으로 또는 범죄에 이용될 것을 알면서 접근매체 대여 또는 보관 · 전달 · 유통하는 행위에 관여하면 안됨(제6조3항3호)
금융회사 등은 계좌정보를 사용 및 관리함에 있어서 범죄에 이용할 목적으로 또는 범죄에 이용될 것을 알면서 계좌와 관련된 정보를 제공받거나 제공하는 행위 또는 보관 · 전달 · 유통하는 행위를 하면 안됨(제6조의3)

개정 전

1. 접근매체의 위/변조로 발생한 사고
2. 계약체결 또는 거래지시의 전자적 전송이나 처리 과정에서 발생한 사고

개정 후

1-3. 현행법과 동일

3. 해킹 및 침해 사고에 대한 책임 명문화
4. 계좌정보 관련 정보를 제공받거나 제공하는 행위에 대한 책임 명문화

2-4. 사용 환경

구분	상세 내용
지원 OS	iOS 11.0 이상
제공 형태	Software Development Kit (고객사 앱 내부 탑재)
실행 방식	개발 가이드 문서 및 예제 코드 샘플 제공
검사 대상	• iOS 운영체제 검사 • 후킹 여부 • 원격제어 여부 • 앱 위변조 여부 • 디버거 • VM
업데이트	최신 룰 라이브러리 제공 (고객사 앱 재배포 필요)
제공 및 동작 방식	• 고객사 애플리케이션 빌드 시 Mobile Engine Suite for iOS 라이브러리 파일을 포함하여 빌드 • 고객사 애플리케이션에서 기능 동작을 위한 함수를 호출 • 탐지 및 검사 결과에 따른 조치(서비스 종료 또는 알림 등)는 고객사 앱에서 자체적으로 결정

3. What is NEXT ?

Mobile Engine Suite(iOS) 탐지된 데이터를 Transaction Security Center를 통해 가시성 있는 자료로 확인해보세요!

Mobile Engine Suite 연동

- 탈옥/디버거 등 iOS 맞춤형 탐지 결과 제공

※ 별첨 – Jail-Break Scanner 와의 비교

구분	Mobile Engine SDK for iOS	Jail-Break Scanner (단종)
지원 OS	iOS 11.0 이상	iOS 9.0 이상
제공 형태	Software Development Kit (고객사 앱 내부 탑재)	
실행 방식	개발 가이드 문서 및 예제 코드 샘플 제공	
검사 대상	• iOS (운영체제 검사) • 후킹 여부 • 원격제어 여부 • 앱 위변조 여부 • 디버거 • VM	• iOS (운영체제 검사)
업데이트	최신 룰 라이브러리 제공 (고객사 앱 재배포 필요) * 자체 업데이트 지원	최신 룰 라이브러리 제공 (고객사 앱 재배포 필요)
제공 및 동작 방식	• 고객사 애플리케이션 빌드 시 Mobile Engine Suite for iOS 라이브러리 파일을 포함하여 빌드 • 고객사 애플리케이션에서 기능 동작을 위한 함수를 호출 • 탐지 및 검사 결과에 따른 조치(서비스 종료 또는 알림 등)는 고객사 앱에서 자체적으로 결정	

※ 별첨 – 성능

안랩은 AV-TEST, AV-Comparatives 등 공신력 있는 글로벌 인증 기관의 테스트에서 뛰어난 평가 결과로 검증된 강력한 모바일 엔진을 보유하고 있습니다.

AV-Test Nov 2023

100%
Protection

11년 연속 **66회** 인증 획득
(국내 유일)

AV-TEST av-test.org CERTIFIED ANDROID

All tested manufacturers

AhnLab, 阿里钱盾, ANTIY, ARMOR FOR ANDROID, avast, NoxSecurity, NQmobile, NSHC, MAX, panda, PLAY CASTLE, AVG, Avira, Baidu, Bitdefender, BullGuard, cheetahmobile, TOTAL AV, PSafe, 360, Quick Heal, secucloud, SECURION, COMODO, Dr. Web, eset, F-Secure, G DATA, Google, SK telecom, SOPHOS, 腾讯手机管家, ThreatTrack, TREND MICRO, WEBROOT, HAURI, Hi Security, IKARUS, NETCOP, Juniper, kaspersky, WhiteArmor, ZEMANA, Zoner AntiVirus, lookout, Malwarebytes, McAfee, eScan Enterprise Security, NAVER Cloud, NortonLifeLock

https://www.av-test.org/en/antivirus/mobile-devices/

※ 별첨 – 대응 프로세스

안랩 시큐리티 대응 센터(ASEC)의 4단계 대응 프로세스를 기반으로 강력한 악성코드 및 해킹 억제 역량을 제공합니다.

ASEC

AhnLab Security Emergency response Center

1단계 : **접수**	2단계 : **분석**	3단계 : **1차 대응**	4단계 : **2차 대응**
신·변종 바이러스, 해킹 사고 접수	**상황 분석** 1. 국내·외 피해 조사 및 예측 2. 프로그램 용도 3. 바이러스·해킹 발생 시점 및 행동 분석	**엔진 대응** 1. 바이러스·해킹 툴 대응 엔진 제작 2. 엔진 업데이트	**모듈 변경** 1. 변종 바이러스 엔진 추가 등록 2. 해킹 툴 방지 모듈 개발 3. 제품 업데이트
바이러스·해킹 툴 수집	**샘플 분석** 1. 샘플 입수·분석 2. 분석 리포트 제출 3. 대응 방식 결정 4. 대응 일정 확정	**추가 공격 대응 준비** 1. 변종 바이러스·해킹 툴 모니터링 2. 고객 응대 확대	

※ ASEC(AhnLab Security Emergency response Center)은 안랩에서 운영하는 비상 대응 조직으로, 바이러스 및 보안 위협의 24시간 감시, 신속한 대응 및 지속적인 연구를 수행하여 고객사의 중요 정보 자산 및 비즈니스 연속성을 보호하여 고객사의 대외 신뢰도 강화에 기여합니다.

More security, More freedom

AhnLab