



효과적인 랜섬웨어 통제 방법

NGAV+ PC 가상화

A close-up, slightly blurred photograph of a hand in a dark blue sleeve moving a small, light-colored wooden piece (an abacus) across a light-colored wooden board. The board has a grid of lines, and several other similar wooden pieces are scattered across it. The background is a plain, light-colored surface.

소만사의 27년

시장 1위 데이터보호 전문기업 소만사

DLP 개인정보 유출 통제 분야 15년 1위, [Privacy-i](#), [Mail-i](#)

Secure Web Gateway 분야 20년 1위, [WebKeeper](#)

PC 가상화 (VDI) 누적 5만유저, [VD-i](#)

2019~2024	2023 VB 100 A+등급 획득 2021 PC 가상화 (클라우드 PC) VD-i 출시 2019 Privacy-i EDR 버전 출시 Endpoint 싱글에이전트 완성
2011~2018	Webkeeper SWG(Secure Web Gateway) HTTPS 가시성 확보, 외산 어플라이언스 대비 30% 성능, DLP일체, 누적 고객사 1,000 곳
2010	Endpoint DLP Privacy-i 출시
1998~2009	2008 DB-i 출시 1998 유해사이트 차단솔루션 Webkeeper 개발 1998 Network DLP 솔루션 mail-i 개발
1997	03.25 <㈜소프트웨어를 만드는 사람들> 설립

재무안정성 상위 1%

중소기업 **재무안정성 상위 1%(A+)**, 유일한 무차입 기업으로 20년 간 흑자를 기록
신용평가등급 A+, 현금흐름등급 CR-1로 중소기업 상위 1%의 재무적 안정성

Korea Rating & Data

I. 기업신용등급

회사명 : (주)소만사 대표자명 : 김대환 사업자번호 : 214-86-14882

기업개요

기업명	(주)소만사
대표자	김대환
법인(주)등록번호	110111-1394115
사업자번호	214-86-14882
본사주소	((07228) 서울 영등포구 영신로 220 (영등포동8가))
업종	(J58222) 응용 소프트웨어 개발 및 공급업
주요제품명	개인정보보호, 내부정보유출방지 인터넷필터링 및 악성코드차단 솔루션
종업원수	338명 (전국소속 117명 포함)
기업규모	중기업 (중소기업확인서 (중소벤처기업부))

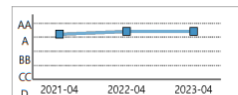
경영규모 (단위:백만원)	재무기준일	총자산	납입자본금	자본	매출액	순이익
	2022-12-31	84729	543			

신용등급이력

평가기준일	재무기준일	신용등급	변동
2023-04-14	2022-12-31	A+	-
2022-04-15	2021-12-31	A+	
2021-04-19	2020-12-31	A	

신용등급

기업신용평가등급	현금흐름 등급
A+	CR-1
평가기준일	2023년 04월 14일
재무기준일	2022년 12월 31일

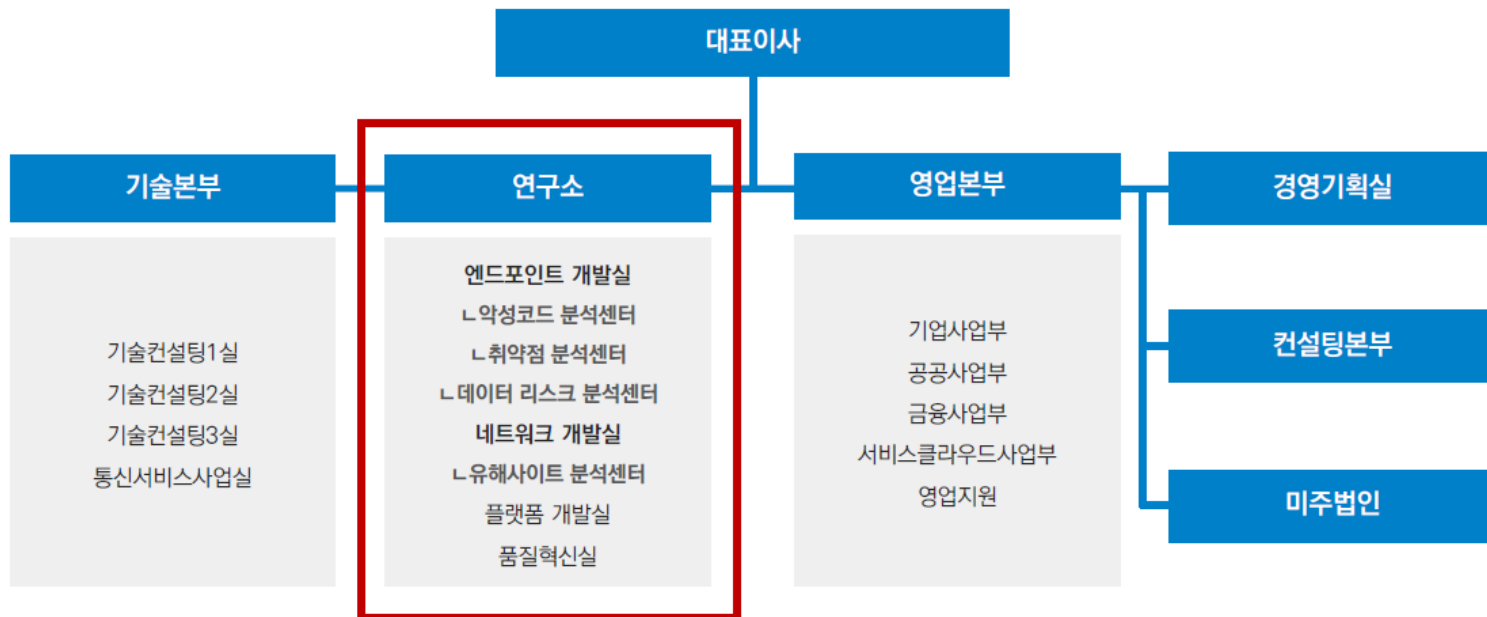


구 분	2021년	2022년	2023년
매출액	443	535	577
영업이익	82	83	115
당기 순이익	82	88	135
차입금	0	0	0
총자산	784	847	1,024

(단위: 억원)

악성코드, 취약점 분석 인력

- 악성코드 분석센터 (악성코드/랜섬웨어 분석), 취약점 분석센터 (엔드포인트 보안 플랫폼 개발, 취약점 분석), 데이터 리스크 분석센터 (개인정보/기밀정보 유출차단), 유해사이트 분석센터 (악성코드/유해사이트 분석) 운영
- 컨설팅 본부 (50여개 주요기반 시설 취약점 점검 프로젝트 수행)



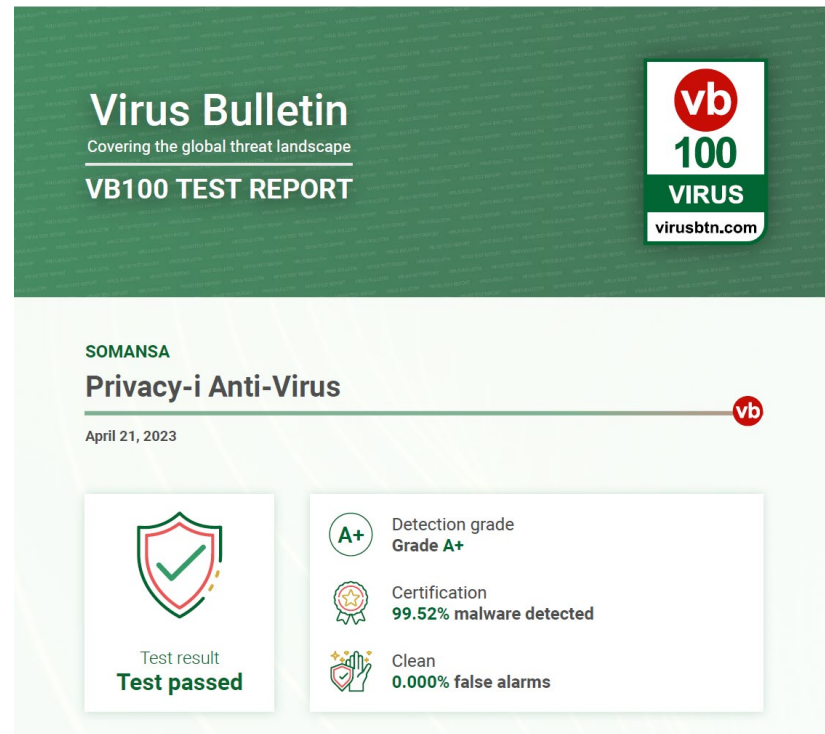
악성코드 대응 체계, Endpoint, Network, Server : XDR



영국 바이러스 연구기관

바이러스 불러틴 'VB 100' A+ 인증 획득

바이러스 불러틴 VB100 탐지 결과	항목	차단율
	오탐율	0%
	탐지율	99.52%



악성코드, 랜섬웨어 분석 리포트 월간 발행 및 배포

2024.02

친팔레스타인 단체 개발한 인프라 파괴
목적 BiBi 와이파이 악성코드

2023.10

Chinotto, RokRAT 정보탈취형 3종
북한발 LNK 악성코드분석

2024.01

CVSS위험도 최고점 10점 중 7.8점 평가
WinRAR 원격코드 실행 취약점

2023.06

코로나19 백신 연구데이터 1.4TB 탈취,
RA 그룹 랜섬웨어

2024.01

친팔레스타인 단체 개발한 인프라 파괴 목적 악성코드

이שראל 공격 목적으로 친 팔레스타인 단체에서 개발한 인프라 파괴 목적의 BiBi 와이파이 악성코드

요약

1. 이스라엘-팔레스타인 간 사이버 공격 목적으로 친 팔레스타인 세력이 개발한 신종 **BiBi 와이파이 악성코드** 이스라엘 보안기업인 차크 가릴가갈 네트워크 조사 중 발견.
2. 알려진 랜섬웨어는 데이터피해를 통한 파괴와 비록(비록)을 목적으로 함. **BiBi 와이파이 악성코드**는 랜섬웨어처럼 파일변경명령을 수행하나, 전산 인원과 파괴에 목적이 있어 국가 간 사이버 테러에서 주로 포착됨.
3. 감염 대상의 네트워크를 통해 시스템에 침투, PC 내 파일을 무작위 데이터로 덮어쓰는 방식으로 손상시킴. 데이터의 운영 체제 복구 요구 불가함.

대응 방안

1. Privacy-EDR과 같은 EDR 제품을 통해 취약점 실행을 탐지 기반으로 차단
2. 주요 데이터는 주기적인 백업을 통해 시스템 파손 시에도 복구가 가능하도록 대비
3. 논리적 암호화를 적용하여 악성코드 PC 유입을 통한 차단
4. AV(백신)기반방지 + EDR(행위)기반방지 솔루션
5. PC 취약점을 주기적으로 점검, 보완
6. 신변을 수 있는 메일의 첨부파일 실행 금지
7. 비 업무 사이트 및 신뢰할 수 없는 웹사이트와 연결 차단
8. OS나 애플리케이션은 최신 항상 유지

SOMANSA

2023.10

북한발 LNK 악성코드 3종 분석

2023년 10월 현재도 피해사례 지속적으로 발생 중 북한발 LNK 악성코드 3종 분석

요약

1. 사전에 발파된 정보를 바탕으로 정교한 랜섬 코드 제작하여 타겟 가남 : 세균계산사, 세균계수로서, 백신 위장 문서 등
2. 일회성 공격이 아닌 타겟에 정확하게 실행된 지속적 공격 : 10개월간 지속한 한미연합군을 노린 김수자 사이버 공격
3. 새로운 LNK 파일형식 활용 공격 수법 : 파일명(전자정보) 표시되지 않음 타겟을 쉽게 속일 수 있음 : 2023년 8월에만 6,600건이 발견, 현재 진행 중
4. LNK 파일 3종 : 1) Chinotto 악성코드 유포 : 가장 많이 발견한 사례 2) RokRAT 악성코드 유포 : 신뢰 가능한 서비스, OneDrive 통해 악성코드 유포 3) 정보탈취형 악성코드 유포 : 사용자 PC 온전 유지 파일 열람, 운영 IP, 프로세스 목록 등 탈취 : 사용자 PC 온전 유지 파일 열람, 운영 IP, 프로세스 목록 등 탈취

대응 방안

1. 논리적 암호화를 적용하여 악성코드 PC 유입을 통한 차단
2. AV(백신)기반방지 + EDR(행위)기반방지 솔루션을 최신 항상으로 유지
3. PC 취약점을 주기적으로 점검, 보완
4. 신변을 수 없는 메일의 첨부파일은 실행을 금지
5. 비 업무 사이트 및 신뢰할 수 없는 웹사이트와 연결 차단
6. OS나 애플리케이션은 최신 항상 유지

SOMANSA

2024.01

WinRAR 원격코드 실행 취약점

전 세계 약 5억 명이 사용하는 압축 프로그램에서 취약점 발견 CVSS(공통 취약점 등급 시스템) 위험도 최고점 10점 중 7.8점 평가 WinRAR 원격코드 실행 취약점

요약

1. WinRAR는 전세계 사용자 약 5억명을 확보한 압축 프로그램으로 1996년 출시 이후 꾸준히 버전업 지원 중
2. 사용자가 압고 공격 제인이 쉬운 탓에 2022년 9월 처음 발견했으나 지속적으로 악용될 가능성이 있음
3. CVSS 위험도 7.8점은 고위험군에 속하는 중수이며 해당 취약점의 악용될 경우 큰 피해가 발생할 수 있음
4. WinRAR는 취약점 발견 즉시 업데이트를 출시했으나 모든 사용자에게 적용되기까지 상당 시간 소요되어 피해발생이 지속될 것으로 예상
5. WinRAR 원격코드 실행 과정 : 1) 조직은 압축파일을 타겟에게 유동 2) 취약한 버전의 WinRAR를 파일을 실행하여 "리모콘" 원격 시 악성코드 실행

대응 방안

1. WinRAR 사용자는 프로그램을 최신 항상으로 유지
2. 논리적 암호화를 적용하여 악성코드 PC 유입을 통한 차단
3. AV(백신)기반방지 + EDR(행위)기반방지 솔루션을 최신 항상으로 유지
4. PC 취약점을 주기적으로 점검, 보완
5. 신변을 수 없는 메일의 첨부파일 실행 금지
6. 비 업무 사이트 및 신뢰할 수 없는 웹사이트와 연결 차단
7. OS나 애플리케이션은 최신 항상 유지

SOMANSA

2023.06

RA 그룹 랜섬웨어

코로나19 백신 연구데이터 1.4TB 탈취, RA 그룹 랜섬웨어

요약

1. 2023년 4월 사용자 용량한 RA 그룹 : - 23년 4월에 활동 시작하여 빠르게 활동 규모를 넓히는 중 - 한국군 특작대(보안사, 자산 관리사, 보철사, 제막사) 주둔 요격 한계지라는 한국군 한군, 그리고 대한 기업 등 공격 - 목적 달성을 위해 초기에는 탈취한 데이터의 일부를 공개하여 피해자 협박, 시간이 지남에 따라 더 많은 요구 공개하는 진행형인 백신 사용
2. Babuk 랜섬웨어와 RA 그룹 : - 소스 코드가 유출된 Babuk 랜섬웨어를 제조하여 RA 그룹이 랜섬웨어 공격 수법 - RA 그룹은 '이름' 기반 랜섬을 사용한다는 점에서 기존 랜섬웨어 그룹들과 공통점이 있음. - 랜섬웨어에 단 5일간의 기간을 주지 않음 랜섬 공격에 관여하는 것이 특징 - 랜섬 유출을 할지 여부와 피해 조치의 여부에 관계없이 공격하도 하짐 - 해당 사이트에서 직접 피해 조치의 데이터를 직접 판매하기도 함

대응 방안

1. 논리적 암호화를 적용하여 악성코드 PC 유입을 통한 차단한다.
2. AV(백신)기반방지 + EDR(행위)기반방지 솔루션을 최신 항상으로 유지한다.
3. PC 취약점을 주기적으로 점검, 보완한다.
4. 신변을 수 없는 메일의 첨부파일은 실행을 금지한다.
5. 비 업무 사이트 및 신뢰할 수 없는 웹사이트와 연결 차단한다.
6. OS나 애플리케이션은 최신 항상을 유지한다.

SOMANSA

Privacy-i 공공 레퍼런스

중앙부처, 공기업 및 공공기관

 고용노동부	 법무부	 문화체육관광부	 국민안전처	 인사혁신처	 대한민국 국방부 Ministry of National Defense
 특허청	 국세청 National Tax Service	 병무청	 경찰청 KOREAN NATIONAL POLICE AGENCY	 검찰 PROSECUTION SERVICE	 문화재청
 우정사업본부 KOREA POST	 한국수력원자력주 KOREA HYDRO & NUCLEAR POWER CO., LTD.	 한국동서발전주	 한국서부발전주	 KOMIPO 한국중부발전	 한국전력기술
 h-well 국민건강보험공단	 NPS 국민연금공단	 KDIC 예금보험공사	 NOC 한국석유공사 KOREA NATIONAL OIL CORPORATION	 파국가스공사	 ex 한국도로공사
 KOMSCO 한국조폐공사	 한국관광공사	 HUG 주택도시보증공사	 TP 사학연금 TEACHERS' PENSION	 근로복지공단	 건강보험심사평가원 HEALTH INSURANCE REVIEW & ASSOCIATION SERVICE

PC 7~10개 보안 에이전트



싱글 에이전트의 “압도적” 장점

항목	싱글에이전트	10개
부팅시간	빠름	지연
PC 성능	최적화	프로세스, MEM, CPU 과점 발생
후킹 횟수	하나의 프로세스에 의해서 한번만 수행	DLP, Anti 바이러스, DRM, 매체제어, 출력물 에이전트에 의해서 다수 후킹 발생
에이전트간 충돌회피	해당없음	보안에이전트간 충돌회피 작업 필수
개인정보 패턴 일관성	유지	동일 파일 USB 파일 복사 시 주민등록번호 150개, 출력 시 주민등록번호 145개 인터넷 전송 시 주민등록번호 152개
OS업그레이드시 대응	프로젝트 1회 수행	Win** OS 업그레이드시 모든 에이전트 업그레이드 프로젝트 개별적 수행

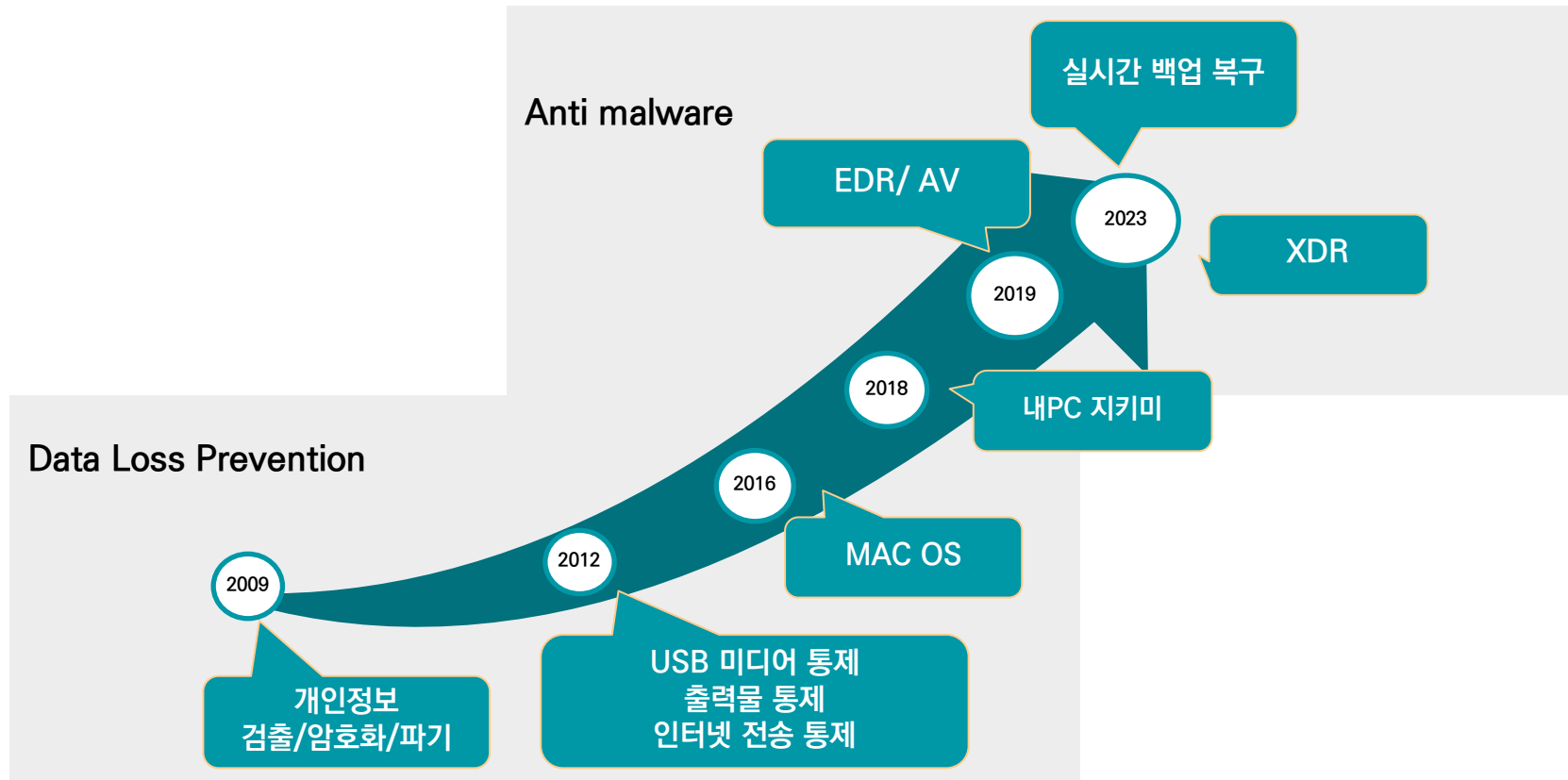
One more thing – It's way cheaper

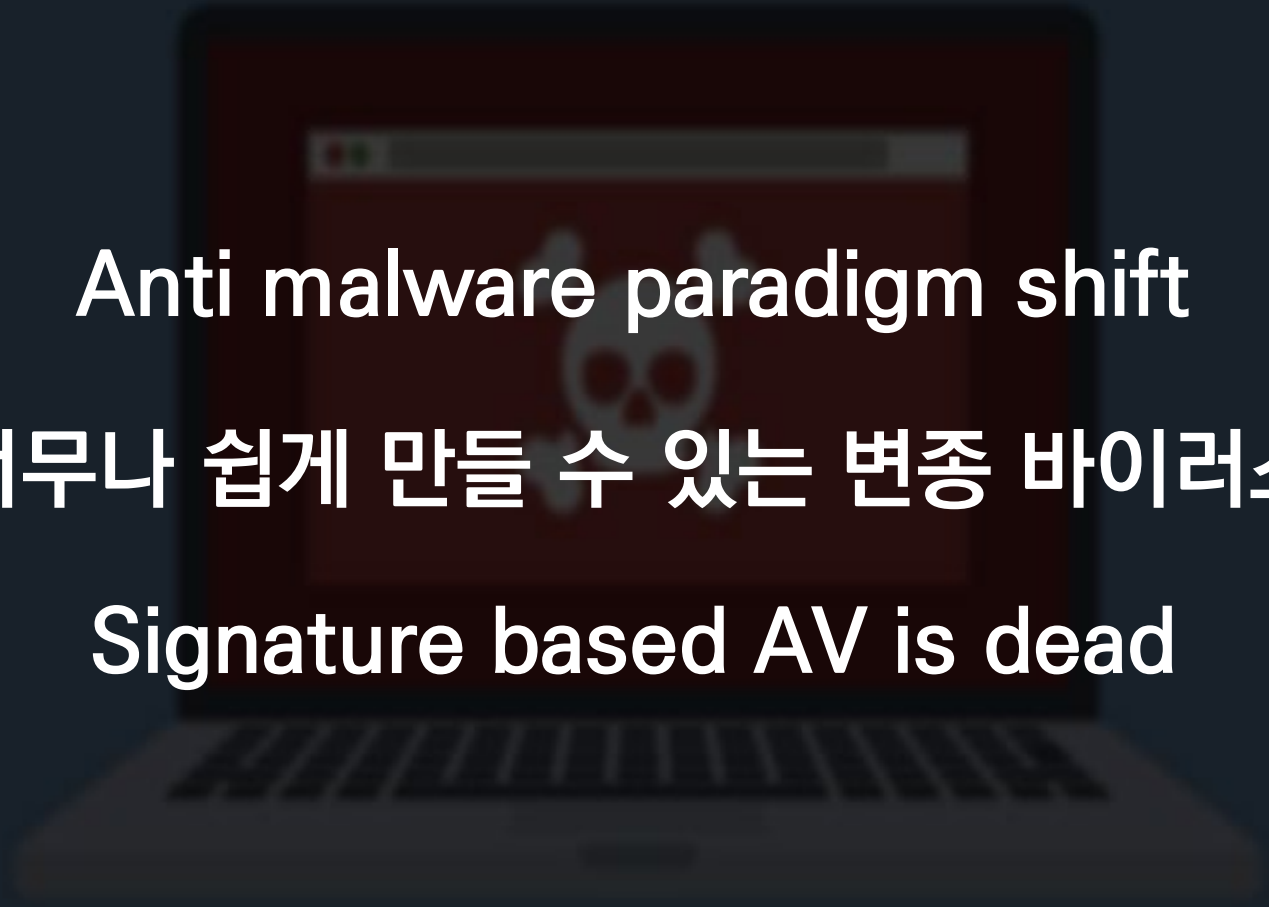


단 하나의 엔드포인트 싱글에이전트로
악성코드차단, 엔드포인트 위협탐지 대응 뿐만 아니라
개인정보보호, 개인정보 유출차단, 취약점 점검까지 수행

국내 싱글에이전트 솔루션 개발기업은 안랩과 소만사 단 두 곳

소만사 싱글에이전트 마지막 퍼즐 :NGAV



A dark, blurred background image of a laptop. On the laptop screen, there is a faint, light-colored skull icon with a cross through its center, set against a dark red background.

Anti malware paradigm shift

너무나 쉽게 만들 수 있는 변종 바이러스

Signature based AV is dead

전통 AV 한계점과 행위기반 악성코드 차단

항목	안티 바이러스 엔진	비고
악성코드 식별	파일 내 패턴(시그니처) 기반	
변종 악성코드 대응	변종 악성코드의 파일 내 패턴식별 후 대응	패턴 추출에 Hour to Days 변종 악성코드는 하루에도 수만 여개 발생
제로데이 공격 대응	취약점 분석 후 패턴 업데이트	취약점 분석에 수 일 ~ 수 주가 소요될 수 있음 그 사이 감염 PC가 기하급수적으로 확산될 수 있음
신규 악성코드 발생시 대응	악성코드 샘플 수집 → (수작업) 패턴 추출 → 패턴 업데이트	악성코드 샘플수집, 분석, 배포의 자동화 측면에서 한계
오탐 가능성	패턴기반으로 차단 오탐 가능성 상대적으로 낮음	

Response 강화

조직 내에서 사용하는
PC등의 정보처리 단말에서

감지된 내용을 토대로
신속하게 대응하는 것

Endpoint Detection and Response

위협으로 간주할 수 있는
“행위”를 감지하고

사후 분석 + 악성코드 사전 차단

A close-up, slightly blurred photograph of a hand in a blue sleeve knocking over a row of wooden dominoes. The dominoes are falling in a chain reaction, creating a sense of motion and inevitability. The background is a plain, light-colored surface.

EDR is Dead

사후분석 무용론

EDR 사후분석(Investigation) 한계

Endpoint의 Event를 한 곳으로 모아서, 사후에 분석한다.

항목	이슈	비고
누가 분석을 할 것인가	일반 보안전문가가 아닌 악성코드 분석 전문가가 필요	대기업 이외에는 그런 전문가가 내부에 없으며 채용을 하는 것도 불가능
기존 보안관제 인력이 EDR로 그 분석이 가능한가	관제 전문가는 악성코드 분석 불가	
그런 사람을 유지하는데 얼마나 많은 비용이 소요되는가	2~3인팀으로 운영되어야 하며 인건비만 연간 3~5억 소요	운영 인력비용이 솔루션 도입 TCO를 압도 대기업 이외는 불가능
이러한 사후분석이 어떤 의미가 있는가	사고를 막지 못하고 로그만 남으면 CISO에게는 로그가 없는 것보다 더 큰 문제	

EDR 또한 악성코드 선제적 차단 역할에 초점을 두어야 한다.

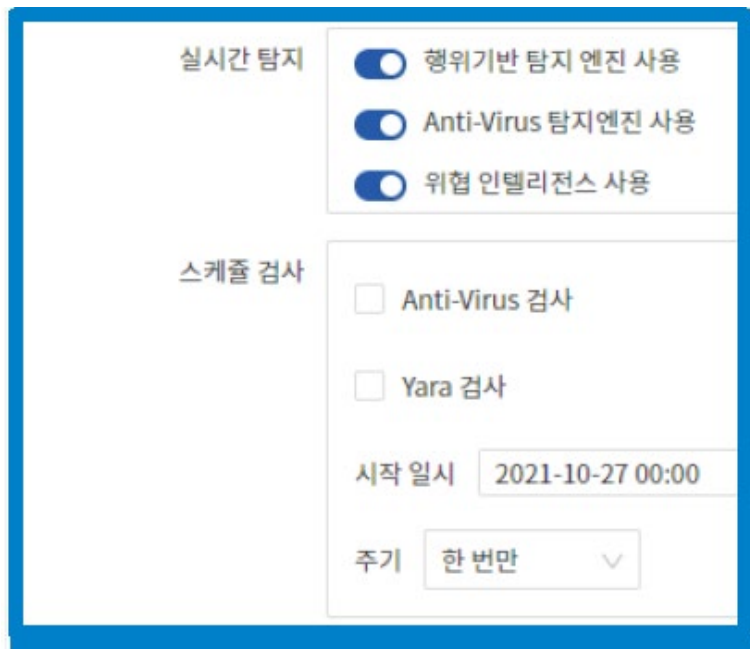
악성코드 차단을 위해서 AV, EDR 여러 개 에이전트를 설치하고 싶지 않다.

AV + EDR 행위엔진 + AI엔진
= NGAV

악성코드 차단 끝판왕

AV는 행위엔진포함으로
EDR는 AV포함으로 통합

탐지 3대 요소 : TI, AV, 행위엔진, (AI)



The image shows a configuration window with two main sections: '실시간 탐지' (Real-time Detection) and '스케줄 검사' (Scheduled Scan). The '실시간 탐지' section has three toggle switches, all of which are turned on. The '스케줄 검사' section has two checkboxes, both of which are unchecked. Below the checkboxes, there is a '시작 일시' (Start Time) field set to '2021-10-27 00:00' and a '주기' (Frequency) dropdown menu set to '한 번만' (Once).

Category	Item	Status
실시간 탐지	행위기반 탐지 엔진 사용	On
	Anti-Virus 탐지엔진 사용	On
	위협 인텔리전스 사용	On
스케줄 검사	Anti-Virus 검사	Off
	Yara 검사	Off
시작 일시		2021-10-27 00:00
주기		한 번만

- TI를 통해 사내 EDR 서버에 없는 데이터 주기적 업데이트
- 정적 탐지소스 YARA/IOC 규칙을 통해 탐지 시간 단축/효율성 강화

탐지 3대 요소 : TI, AV, 행위엔진, (AI)

항목	악성코드 검출 방식	분석성능	변종/제로데이 악성코드 대응력	비고
TI	해시(Hash) 기반	최상	낮음	1 Byte라도 달라질 경우 검출 불가
AV	시그니처(Signature) 기반	높음	중간	변종 대응력 낮음
행위기반 엔진	악성코드 행위(Event)	중간	최상	변종 대응력 높음

탐지 3대 요소 : TI, AV, 행위엔진, (AI)

				탐지/포착한 엔진명	탐지된 실행파일				공신력 있는 정보조회 출처		
부서 이름	사용자 이름	사용자 아이디	에이전트 아이피	탐지 종류	탐지 대상	파일 해시				정보 조회	대응 결과
영업본부	김현덕	hdkim	172.16.2.56	위협 인텔리전스	@C:\Users\hdkim\Desktop\Babuk(packed)\Babuk(packed).exe	296df7094a387d4c9848e02a18bbc7542e7e725810...				  	  
영업본부	김현덕	hdkim	172.16.2.56	위협 인텔리전스	@C:\Users\hdkim\Desktop\test\Babuk.exe	296df7094a387d4c9848e02a18bbc7542e7e725810...				  	  
영업본부	김현덕	hdkim	172.16.2.56	위협 인텔리전스	@C:\Users\hdkim\Desktop\Babuk(packed)\Babuk(packed).exe	296df7094a387d4c9848e02a18bbc7542e7e725810...				  	  
영업본부	김현덕	hdkim	172.16.2.56	위협 인텔리전스	@C:\Users\2taewon\Desktop\Babuk(packed)\Babuk(packed).exe	296df7094a387d4c9848e02a18bbc7542e7e725810...				  	  
영업본부	김현덕	hdkim	172.16.2.56	위협 인텔리전스	@C:\Users\hdkim\Desktop\SomansaCrypto(Packed)\Somans...	57494aec2b31e95e5be475bcb3247abac732469a1f...				  	  
소만사	김현호	hhkim1	10.0.2.15	안티 바이러스	@C:\Users\somansa\Desktop\samples\medusa.exe	dde3c98b6a370fb8d1785f3134a76cb465cd663db20...				  	  
소만사	김현호	hhkim1	10.0.2.15	안티 바이러스	@C:\Users\somansa\Desktop\samples\medusa.exe	dde3c98b6a370fb8d1785f3134a76cb465cd663db20...				  	  
소만사	김현호	hhkim1	10.0.2.15	안티 바이러스	@C:\Users\somansa\Desktop\samples\gandcrab.exe	ce8a3474f1be9				  	  





Virus Total
Hybrid Analysis
Google

통제 3대 요소 : 프로세스킬, 파일 격리, 단말 격리 (경고, 네트워크 차단)

행위기반 탐지 엔진	<input checked="" type="checkbox"/> 파일 격리		<input type="text" value="5"/>
	<input type="checkbox"/> 엔드포인트 격리		
	<input checked="" type="checkbox"/> 프로세스 차단		<input type="text" value="8"/>
	<input type="checkbox"/> 경고 생성 기준		
Anti-Virus 탐지 엔진	<input type="checkbox"/> 파일 격리		
	<input type="checkbox"/> 엔드포인트 격리		
	<input checked="" type="checkbox"/> 프로세스 차단		
위협 인텔리전스	<input checked="" type="checkbox"/> 프로세스 차단		
	<input checked="" type="checkbox"/> 네트워크 접속 차단		

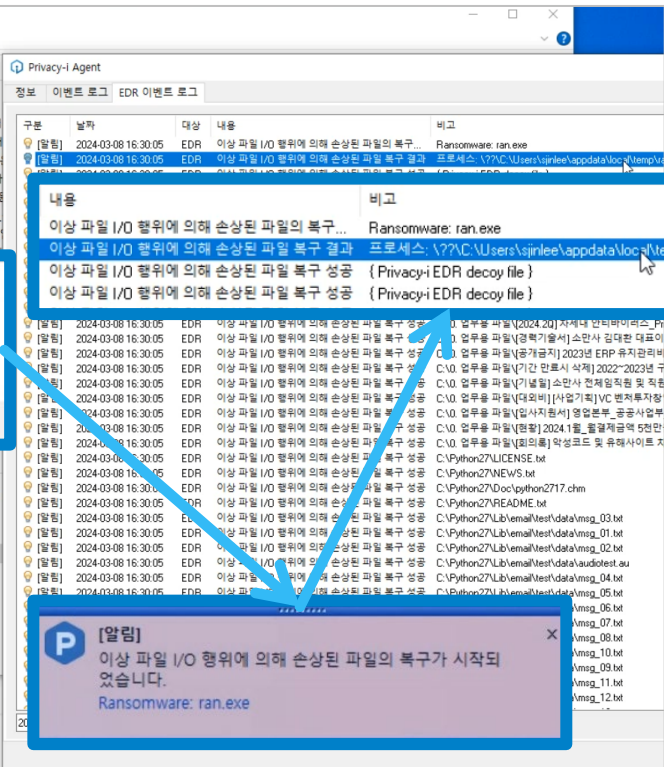
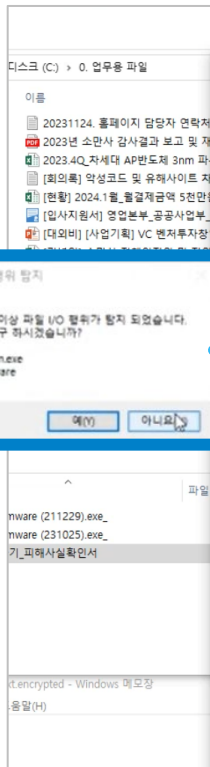
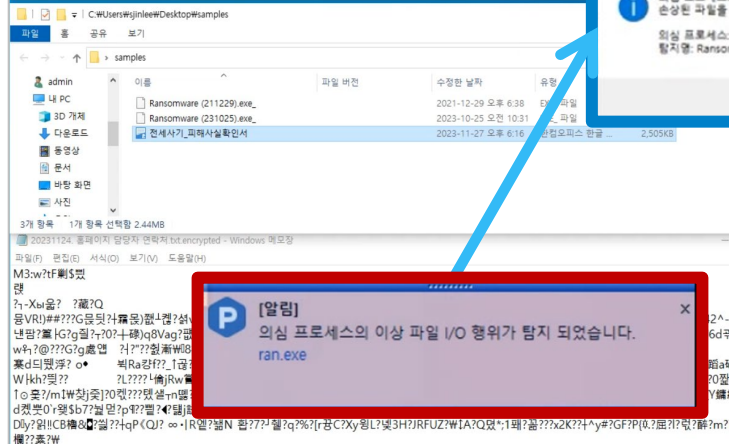
보안 위협 중 90%는 자동으로 대응 (격리, 종료)

사용자 이름	위험도 (색이 짙을 수록 ↑)	분류	발생한 공격타입	대응 결과	공격 수행한 프로세스 이름	MITRE ATT&CK	Mitre ATT&CK 전술/공격 세부 가이드 페이지 이동
김현덕(hdkim_00001)	중간	익스플로잇	impact.impactvolume-shadowcopy	  	cmd.exe	Inhibit System Recovery	
김현덕(hdkim_00001)	중간	익스플로잇	impact.impactvolume-shadowcopy	  	cmd.exe	Inhibit System Recovery	
김현덕(hdkim_00001)	높음	익스플로잇	Ransomware.Babuk	  	Babuk(packed).exe	Application Window Discovery System Information Discovery File and Directory Discovery	▲ ▼
김현덕(hdkim_00001)	높음	익스플로잇	Ransomware.Babuk	  	Babuk(packed).exe	Application Window Discovery System Information Discovery File and Directory Discovery	▲ ▼
김현덕(hdkim_00001)	높음	익스플로잇	Ransomware.Babuk	  	Babuk.exe	System Service Discovery Application Window Discovery System Information Discovery	▲ ▼



파일 격리 엔드포인트 격리 프로세스 종료

그래도 감염되면, 파일백업 및 자동복원



데모 시연



1. 변종 악성코드가

AV에서는 차단이 안 되고,

EDR에서만 차단

2. 랜섬웨어 감염된 파일 실시간 복구



악성코드 차단 성능 비교

자체 탐지성능 테스트 수행 (2023.12)

랜섬웨어 및 악성코드 샘플 1만개 차단 (2023.01~12 수집)

구분	소만사	국외 C사
EDR 탑재 패턴기반 탐지엔진	94.3%	90.3%
EDR 탑재 행위기반 탐지엔진	5.3%	3.7%
총 차단율	99.6%	94.0%

외산 비교

구분	Privacy-i EDR	외산 EDR 솔루션
에이전트 개수	싱글에이전트	EDR 이외 PC 에이전트 추가 설치
네트워크 차단과 연계 (XDR)	SWG 차단 연계	제한적
TI (Threat Intelligence: 위협 인텔리전스) 연계 차단	O	O
변종 악성코드 차단	O	O
제로데이 악성코드 차단	O	O
MITRE ATT&ACK 대응	O	O
실시간 데이터 복구	O	제한적
AV와 행위 엔진 동시 활용	O	제한적
악성코드 차단율	99%	94%

A close-up, slightly blurred photograph of a hand in a dark blue sleeve reaching out to stop a falling domino. A line of dominoes is visible, receding into the background. The scene is set on a light-colored, textured surface.

소만사 랜섬웨어 차단 로드맵

랜섬웨어 대응 끝판왕 = PC 가상화 + NGAV

접속단말(노트북이나 PC)이 설령 악성코드에 감염되더라도

컴퓨팅이 일어나는 클라우드 PC 영향 미치지 못한다. 악성코드 감염 우려없이 어디서나 접속가능

항목		클라우드 PC	비고
접속 단말	USB매체 통한 악성코드 유입	(클라우드 PC에 대한) 악성코드 영향 원천 차단	USB 이 외 RFID, 블루투스 등 디바이스 통한 악성코드 유입에 대한 대응
	외부 와이파이 접속 통한 악성코드 유입	(상동) 악성코드 영향 원천 차단	
	스마트폰 통한 악성코드 유입	(상동) 악성코드 영향 원천 차단	
	재택이나 카페에서 신뢰 할 수 없는 네트워크 연결에 따른 악성코드 유입	(상동) 악성코드 영향 원천 차단	

소만사 27주년

세계적인 보안기업으로 성장해서 보답하겠습니다.