RANSOMKEEPER

RANSOME KEEPER

2021

SECURELINK

©SECURELINK Inc 2021. All rights reserved.

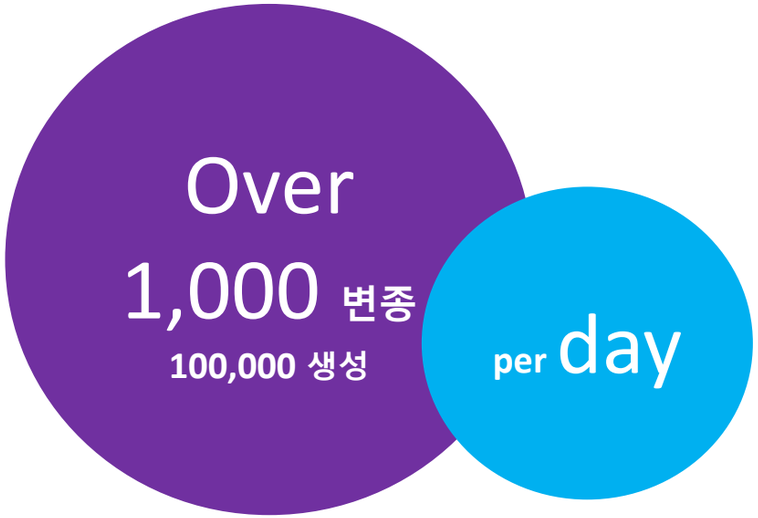
1. 랜섬웨어 개요

변종공격

유럽 중심 급속확산 워너크라이 랜섬웨어 국내 공격 – 2017

국내 환경을 대상으로 전문화된 Driven by 랜섬웨어 그랜크랩/ 메그니베르 공격증가 – 2018~2020

- 최악의 랜섬웨어 '워너크라이' 국내 유포 (2017년 5월 12 일)
- 유럽 및 미국 병원 중심으로 급속한 감염 공격
- 네트워크에 연결된 경우 윈도 취약점을 공격 네트워크 전체 피해
- 문서, 이미지, 동영상 등 거의 모든 자료에 대해서 암호화
- 급격히 상승한 비트코인 요구
- 비트코인 지불한 이후에도 복구 가능성 불투명



출처: 연합뉴스, 뉴시스

위협증대

개인 및 가정 공격이 가장 높고,
모든 형태의 기업 공격 급증
(Broad Spread)

Enterprise, Small & Medium Companies

Home

Hospital

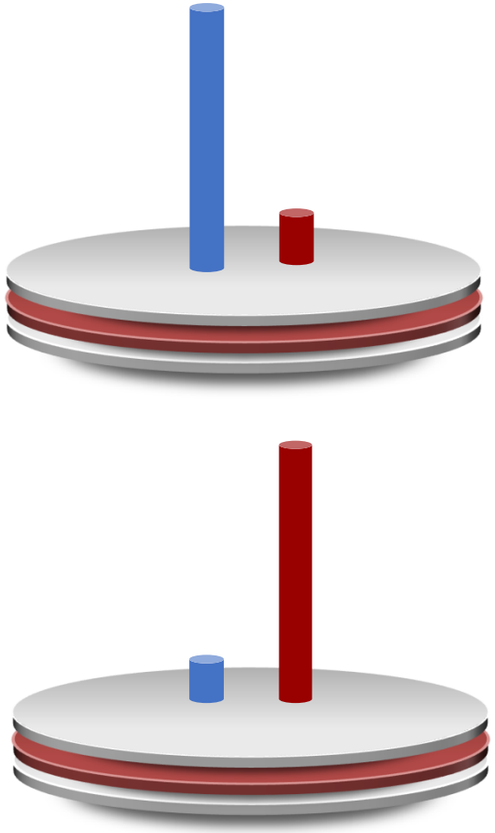
병원, 정부, 군 등
특정 기관에 대해 사전분석
취약점 통한 전문 랜섬공격
(APT + Ransom)

Government, Military

전통적 시그니처 방식

효과

국내 및 해외 검출 테스트 (2017, S사외 평균)



변형전 알려진 악성코드

93% 검출(TPR)

7% 미탐(FNR)

다형성 변형엔진 (Polymorphic) 적용

8% 검출(TPR)

92% 미탐(FNR)

피해화면

https://blog.naver.com/dr_hamlet/221055816737

랜섬웨어 종류와 특징

01 Cerber(크레베르)

확장자명 : 숫자 + 알파벳 혼합으로 4자리

강력한 AES-256 알고리즘으로 문서, 그림, 음성파일 등 파일을 암호화하며 국내에 가장많이 유포되었으며 많은 피해를 입힌 대표적인 랜섬웨어 바이러스입니다. 감염경로는 스팸메일로 시작하여, 해외결제가 많은 요즘시대를 이용한 결제메일, 해외사이트 등 광범위합니다.

02 Sage(세이지)

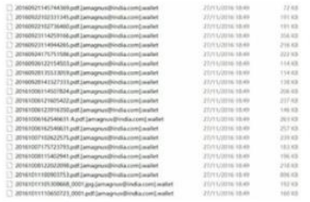
확장자명 : sage

크레베르랜섬웨어와 함께 가장 많이 유포된 랜섬웨어 중 하나입니다. 피해범위로는 하드디스크는 물론 PC에 연결되어 있는 이동식디스크, Cloud Drive, Network Drive 모두 감염시키며, 특히 볼륨쉐도우을 삭제해 윈도우 복원을 불가능하게 합니다.
(IHELP_SOS.tha)라는 파일을 생성합니다.

03 Matrix(매트릭스)

확장자명 : 변경되지 않음

전 세계를 강타한 워너크라이, 페트야에 이어 매트릭스 랜섬웨어가 제작 및 유포되었습니다. 이 랜섬웨어의 가장 큰 특징은 확장자명을 변경하지 않으며, 12시간마다 100달러씩 금액을 올리며, 요구하는 금액이 암호화된 파일 갯수로 책정이 됩니다.
!WhatHappenedWithMyFiles.rtf 을 생성합니다.



04 Wallet(월렛)

확장자명 : wallet, onion, felix, haapydays 등

월렛 랜섬웨어는 보안이 취약한 중소기업, 병원, 학교 등 서버를 주로 공격하는 서버 랜섬웨어입니다. 이 랜섬웨어는 cerber, sage 보다 알려지지 않았지만 피해규모는 훨씬 큽니다. 윈도우에서 기본으로 지원하는 remote APP를 통해 침투하기 때문에 서버 비밀번호를 주기적으로 바꾸셔야 합니다.

05 Petya(페트야)

독일에서 처음 발견된 랜섬웨어로 가장 큰 특징은 기존의 랜섬웨어는 파일만 암호화하여 열지 못하게 하였지만 페트야 랜섬웨어는 하드웨어 자체를 인질로 삼아 비용을 요구하는 아주 악질적인 바이러스입니다. 이 랜섬웨어에 감염되면 MBR(마스터 부트 레코드) 영역의 로더를 악성코드로 대체시켜 강제 재부팅을 시도하여 MFT 자체를 암호화 시켜버리는 것입니다.

06 Venus Locker(비너스락커)

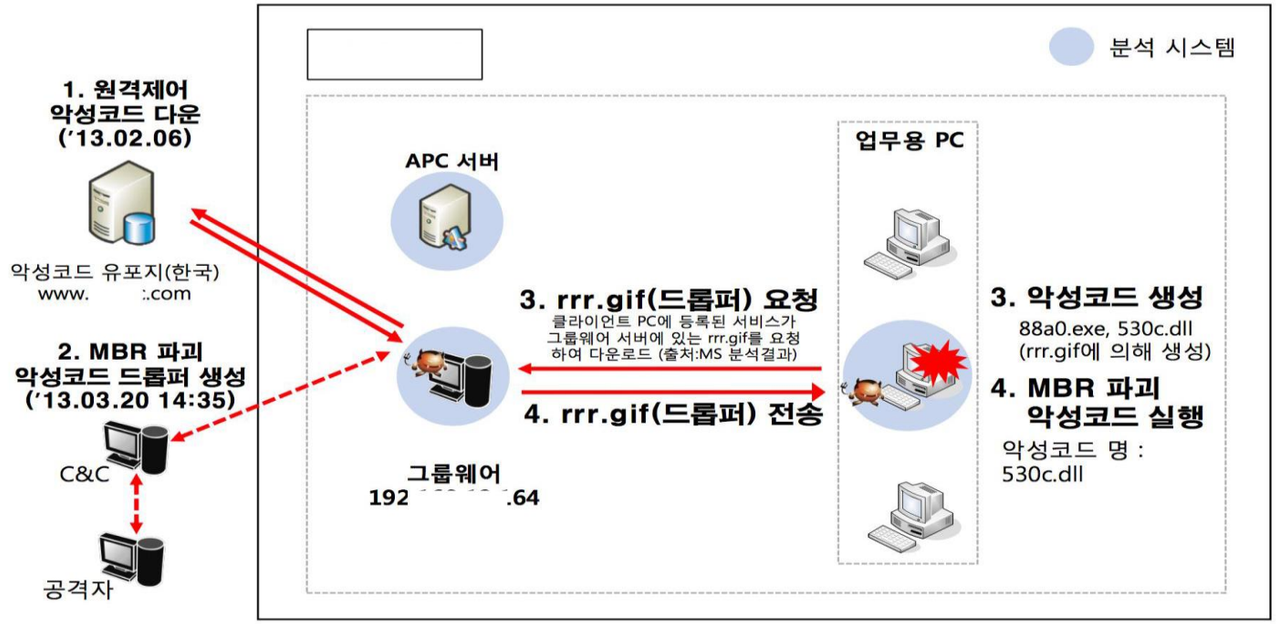
확장자명 : venusf, venusp, V3a4rad4ga

비너스락커 랜섬웨어는 리그익스플로키드(Rig Exploit Kit) 기반으로 하여 유포하며 특히 [eFINE] 차량 법규위반 과태료 통지서와 같은 스팸메일을 위주로 하며 한국형 랜섬웨어 바이러스입니다.
현재 대한민국 사이버수사대에서 조사에 착수하였으며 저희 닥터헬렛에서 수사협조하였습니다.

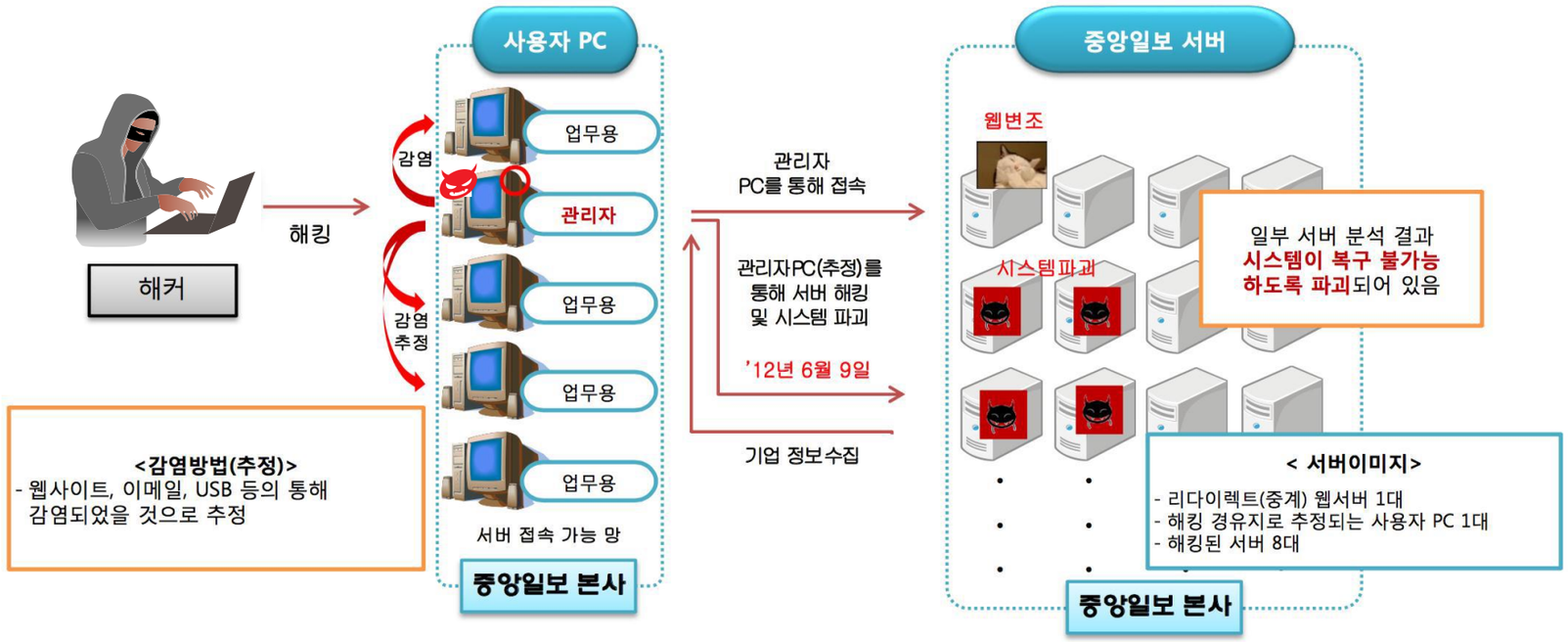
이 외에도 수많은 신종 변종 랜섬웨어 바이러스가 유포되고 있으며 컴퓨터 사용에 각별한 주의가 필요합니다.

랜섬웨어 감염사례

K 회사 HDD 시스템 공격 사례
지속적인 웹 취약점 공격이후(APT) – 이미지 파일을 통해서 악성코드 생성 후 감염
변종에 대한 충분한 백신 방어가 이뤄지지 못해 발생
(* 망분리 및 망연계 방어를 위한 CDR 또는 문서내 악성코드 탐지 솔루션이 있더라도 침입경로 탐지 불가)



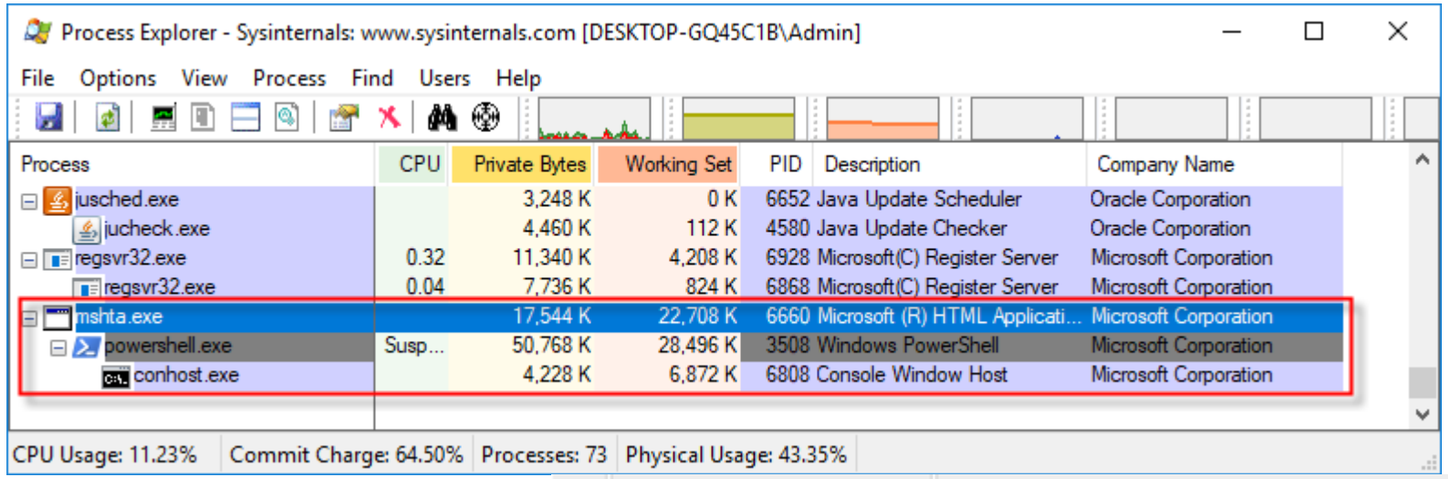
랜섬웨어 감염사례 (초기)



중앙일보 해킹 및 서버 파괴 (2012.6)

본격적인 랜섬웨어 공격 (2017년 나야나 호스팅사태)에 앞서 파타야 같은 HDD 파괴 형태

랜섬웨어 – 매그니베르 파일리스



소	검출 파일	검출 경로	검
14	DELFINO.EXE	C:₩PROGRAM FILES (X86)₩₩IZVERA₩DELFINO-G3···	2018-11
14	MOVIECOLORENHANCER.EXE	C:₩PROGRAM FILES (X86)₩SAMSUNG₩EASY SETTI···	2018-11
14	DMHKCORE.EXE	C:₩PROGRAM FILES (X86)₩SAMSUNG₩EASY SETTI···	2018-11
14	GOOGLETOOLBARUSER_32.E···	C:₩PROGRAM FILES (X86)₩GOOGLE₩GOOGLE TO···	2018-11
14	CROSSEXSERVICE.EXE	C:₩PROGRAM FILES (X86)₩INLINE₩CROSSEX₩CR···	2018-11
14	BTPLAYERCTRL.EXE	C:₩PROGRAM FILES (X86)₩INTEL₩BLUETOOTH₩B···	2018-11

2. 알파시큐어 랜섬키퍼

개요 – 기존 솔루션 단점 (백신)

전통적 백신 (블랙리스트)

1일 1,000건 이상의 변종 출현
신형 변종에 대해서 방어 **취약**

파일 훼손에 대한 대응 불가

정책 및 룰 **업데이트에 종속**적

개요 – 기존 솔루션 단점 (백업)

백업 솔루션

문서 중앙화
백업 TOOL

- 설치/ 운영/ 관리**비용 이슈**
- 백업 주기에 따른 **공백**
- 근본적 방어 불가
  지속적 공격, 백업 **경로 위협**

개요 – 기존 솔루션 단점 (행위기반)

기존 상황인식(행위기반) 솔루션

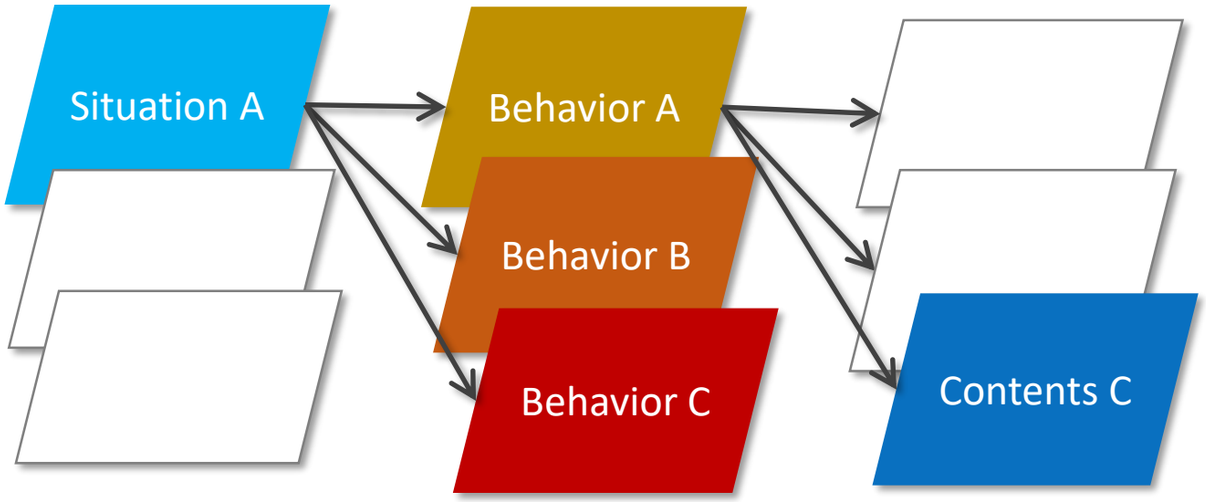
- **미끼** 및 지표파일 (decoy, litmus)
  우회, 오탐
- 파일 **변형 감시 부하**,
  정상 프로세스 **오탐**
- 신뢰기준 미흡
  시스템 **공통 예외처리 공백**발생
- **실시간 백업 부하**,
  감염이전 백업처리의 **한계**

특징요약 (행위 및 상황인식 차별성 1: 인식엔진)

ABC – P 엔진

알파시큐어 랜섬제로 키퍼는
– 누적적으로 발생하는 프로세스의 행동과 해당 시점의 상황을 인지, 학습하여
– 프로세스별 프로파일을 생성, 이를 통해 랜섬웨어의 행동을 사전에 탐지하는

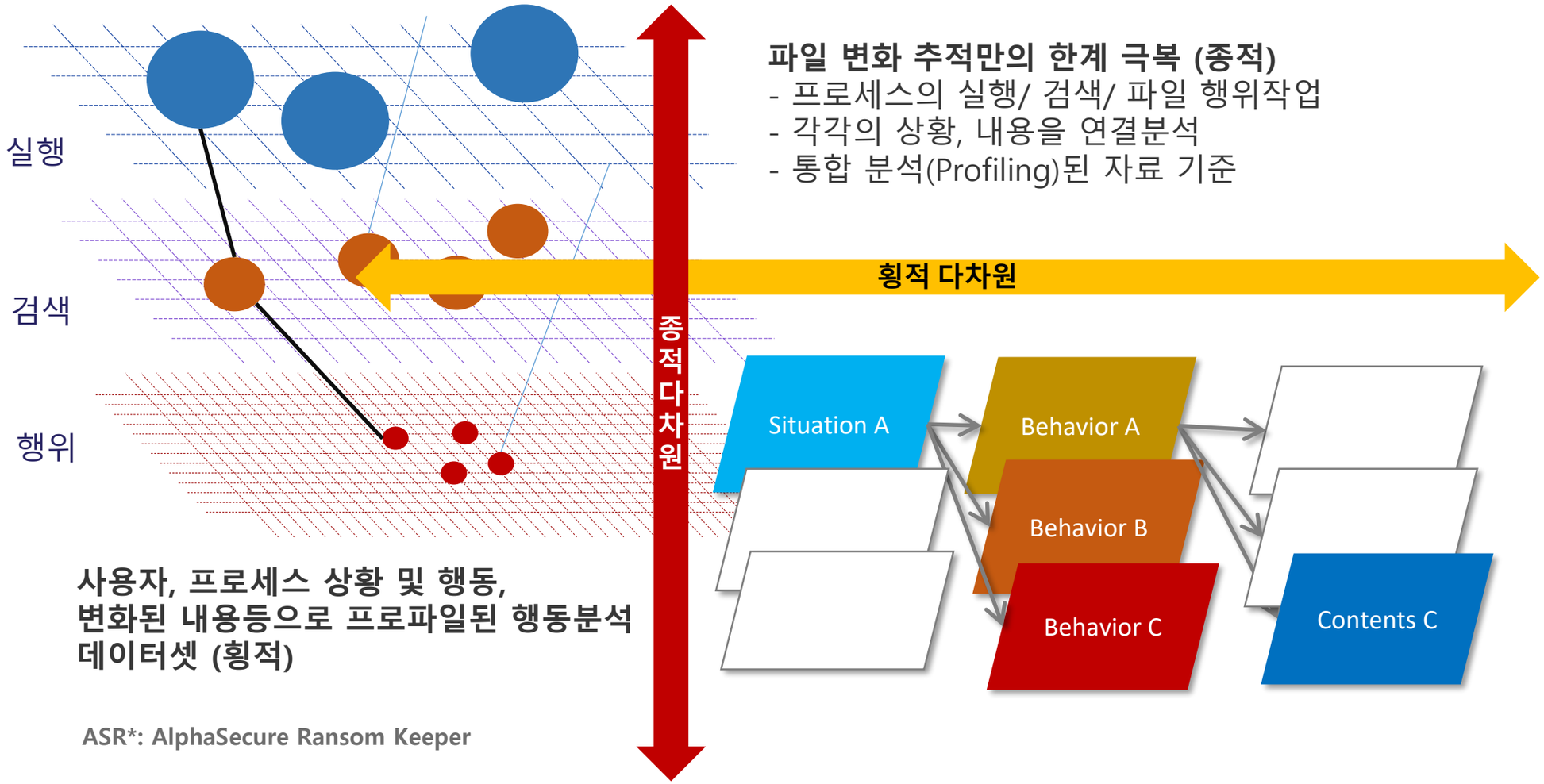
누적 행위 상황감지 프로파일링 (Awareness of Behavior and Contents based Profiling: ABC – P) 엔진 기술을 사용합니다.



행위 상황인지 프로파일 A, B, …

사용자 및 전체 네트워크를 통한
피드백 반영 (머신러닝beta)

특징요약 (행위 및 상황인식 차별성 2: 다차원 검증 프로파일)



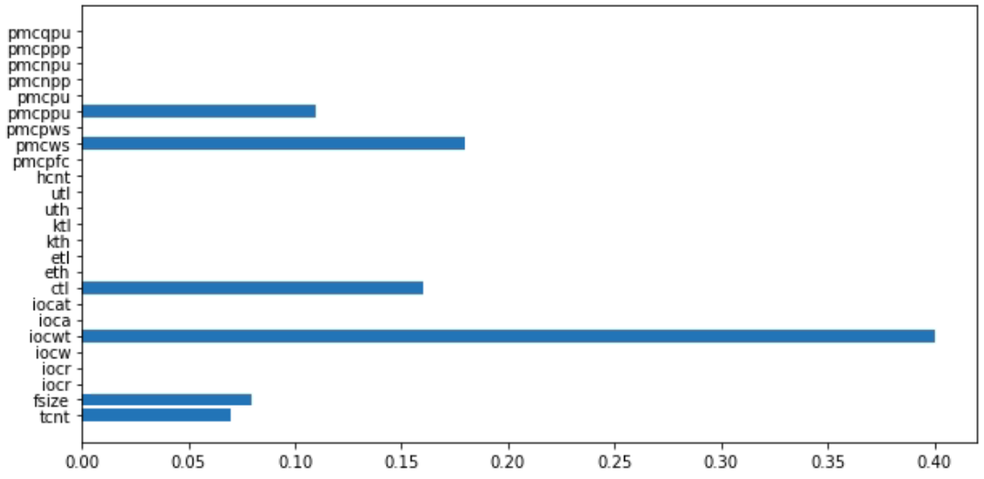
파일 변화 추적만의 한계 극복 (종적)
- 프로세스의 실행/ 검색/ 파일 행위작업
- 각각의 상황, 내용을 연결분석
- 통합 분석(Profiling)된 자료 기준

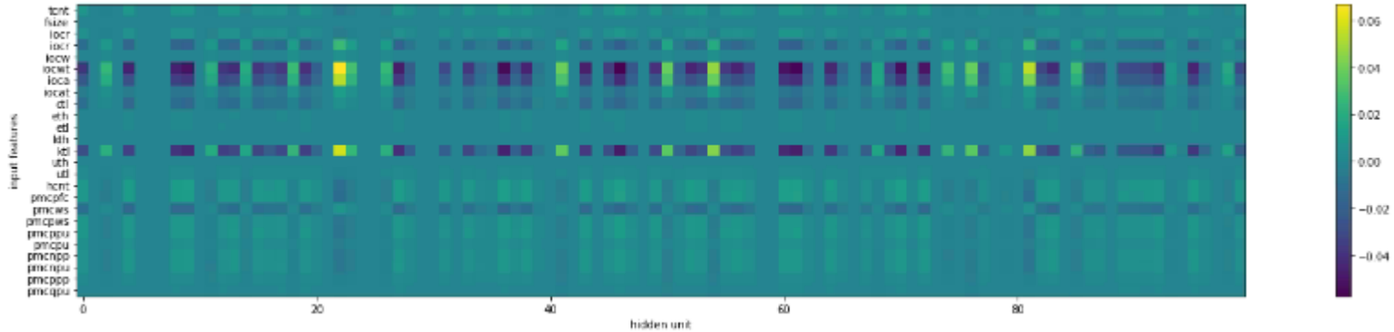
사용자, 프로세스 상황 및 행동,
변화된 내용등으로 프로파일된 행동분석
데이터셋 (횡적)

ASR*: AlphaSecure Ransom Keeper

특징요약 (ABC-P : 행동 프로파일 / 머신러닝특성)

2E+13	2368	852	568	8	60928	01d29ea4	36e57c00	01d29ea4	36e57c00	01d38b89	f8671e03	44	44	000000
2E+13	2512	852	568	15	48688	01d33928	afba82ac	01d33928	afbce517	01d33928	afba82ac	000000d9	000000d9	000000
2E+13	2980	852	568	4	48688	01d33928	afba82ac	01d33928	afbce517	01d33928	afba82ac	0	0	
2E+13	3172	852	568	10	20888	01d33928	afa50d26	01d33928	afa50d26					
2E+13	3228	960	568	9	489984	01d33928	bd2b2af6	01d33928	bd2b2af6					
2E+13	3272	1212	568	9	78336	01d33928	a8d87482	01d33928	a8d87482					
2E+13	3316	852	568	13	48688	01d33928	afba82ac	01d33928	afbce517					
2E+13	3392	1212	568	11	87384	01d33928	bab5b143	01d33928	bab5b143					
2E+13	3552	1276	568	8	10752	01d33928	b9dcb6bf	01d33928	b9dcb6bf					
2E+13	3876	3856	568	74	3903784	01d373bc	fb19669c	01d36fb2	f806bacc					
2E+13	3480	960	568	6	965664	01d33928	a5e23929	01d33928	a5e23929					
2E+13	4124	852	568	9	146944	01d33928	aed7fec9	01d33928	aed7fec9					
2E+13	4340	960	568	35	2010520	01d33928	a126f58c	01d33928	a126f58c					
2E+13	4532	960	568	28	12378520	01d3732f	ee30ac3a	01d3732f	ee3515e7					
2E+13	4656	960	568	4	96672	01d33928	a502176c	01d33928	a502176c					
2E+13	4492	960	568	42	86528	01d39a41	bec9e749	01d39a41	c973d22f					
2E+13	5160	960	568	10	96672	01d33928	a502176c	01d33928	a502176c					
2E+13	5440	852	568	18	982016	01d33928	a71a93b6	01d33928	a71a93b6					
2E+13	3208	960	568	3	96672	01d33928	a502176c	01d33928	a502176c					
2E+13	6444	3876	568	6	82920	01d								





2. 알파시큐어 랜섬키퍼

ABC-P 엔진 동작개요

동시반복 수행

다양한 형태로
실행 (메일, 웹,
스크립트,
매크로, 네트워크)

시스템 전체에 대해서
훼손 대상파일
검색 및 네트워크
공유폴더 검색

시스템 잠입	실행	대상파일 검색	파일 훼손 (암호,삭제)	비용요구 (화면변경 등)
RANSOMKEEPER	알파시큐어는 신뢰정보를 바탕으로 사용자에게 **1차 실행경고** (확실한 프로그램의 경우, 별도 조치없이 예외처리가능 ➔ 단, 예외처리되어도 종합 상황판단에서 악성코드 행위시 재 차단)	알파시큐어는 해당 프로세스의 디스크 검색행위 프로파일링을 통해 사용자에게 **2차 실행경고** (확실한 프로그램의 경우, 별도 조치없이 예외처리가능 ➔ 단, 예외처리되어도 종합 상황판단에서 악성코드 행위시 재 차단)	알파시큐어는 암호화 및 삭제 등, 파일 훼손 행위에 대해서 – 종합적인 프로파일링을 실시하고, 즉각적으로 해당 **악성코드 차단 및 격리** 조치함 시스템 프로세스가 감염된 경우, 윈도우 시스템 클린업 및 복구 프로세스를 가동	파일 복구 알림 • 파일 백업리스트 • 파일 자동복원 또는 확인 수동복원 (대부분 이전 단계에서 차단되어 화면에 표시불가 단, 훼손단계중 먼저 화면 변경하는 경우 및 파일 훼손이 없는 경우는 화면 표시되는 경우 있음)

프로파일 검토/ 생성/ 전파

랜섬키퍼 – 서버 버전

DB 접근제어
지정된 프로세스외 접근차단

DB 및 공유파일 주기백업
(준비 중)

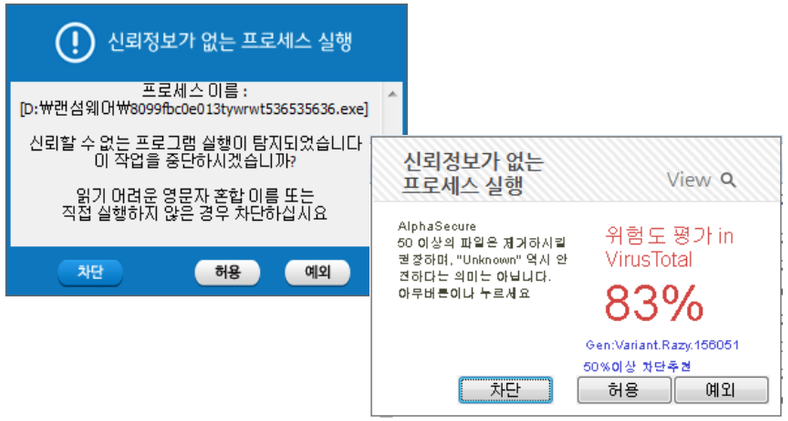
RANSOMKEEPER

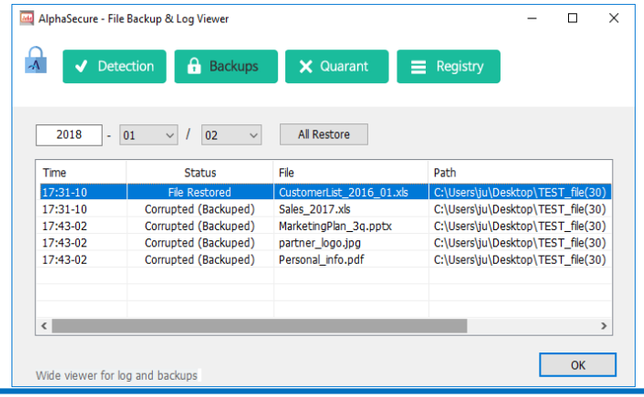
실행경고 숨김/자동
검색경고 숨김/자동

레지스트리/
스케쥴러 감시 및 자동처리

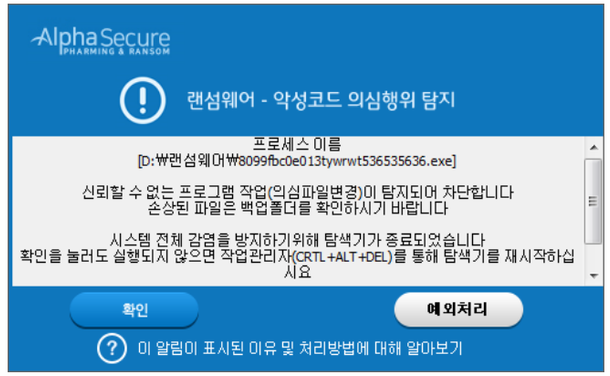
동작 – 동작 예

실행 및 행위 기반 프로파일링 엔진



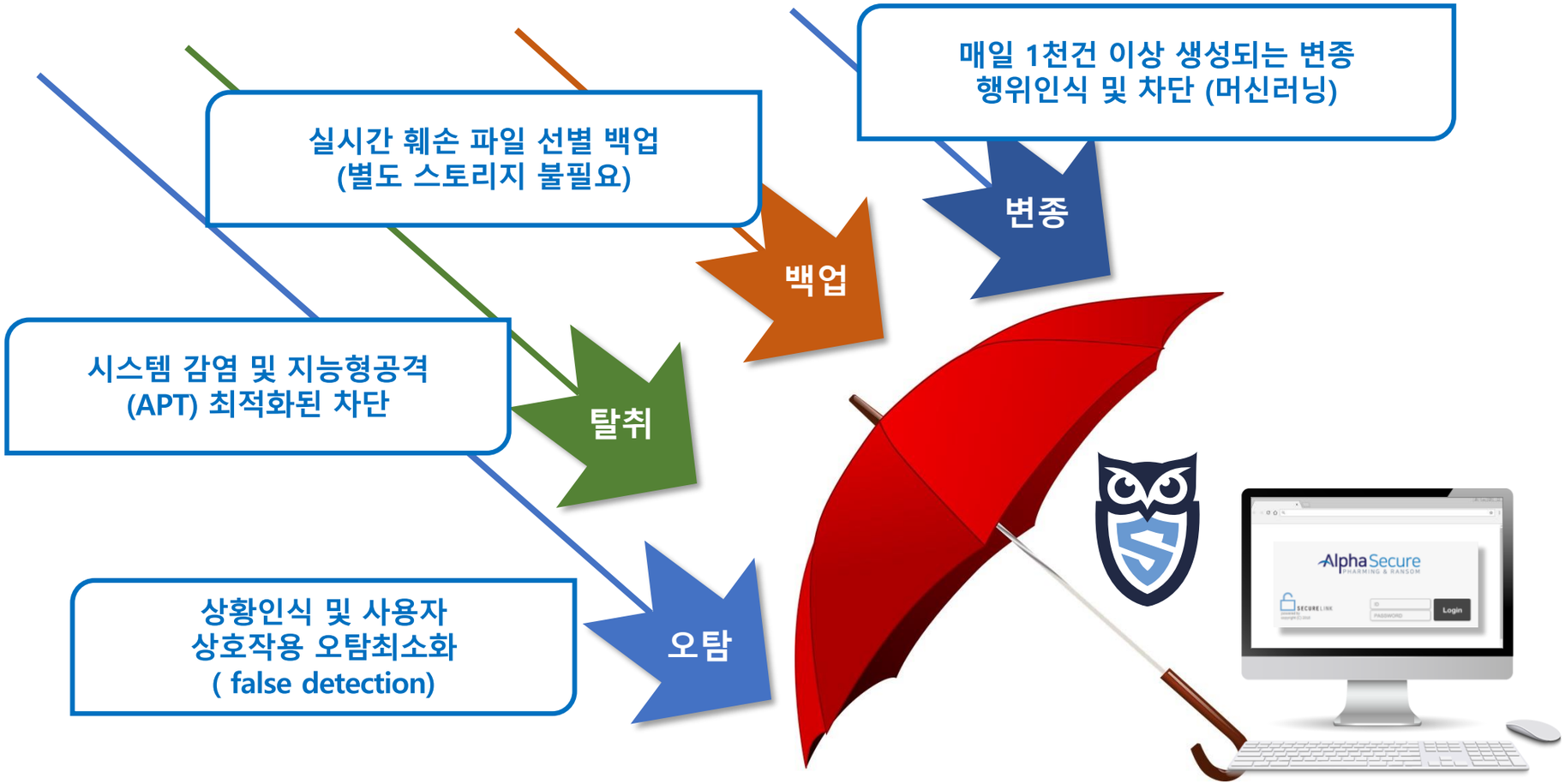


랜섬웨어 감염 백업파일



비신뢰 프로세스 및 감염행위 인지/차단

특징요약 (행위 및 상황인식)



상황 인식 및 학습된 프로파일링
랜섬/악성코드 대응

알파시큐어만의 고유 강점

다차원 검증

실행시점부터, 검색시점, 최종 파일 훼손 단계까지 다차원 행위 상황 인지

➔실행단계 사용자 반응 및 선택기회

➔ 최소 리소스로 최대의 사전차단효과

➔ 오탐 최소화를 위한 다양한 연동기회

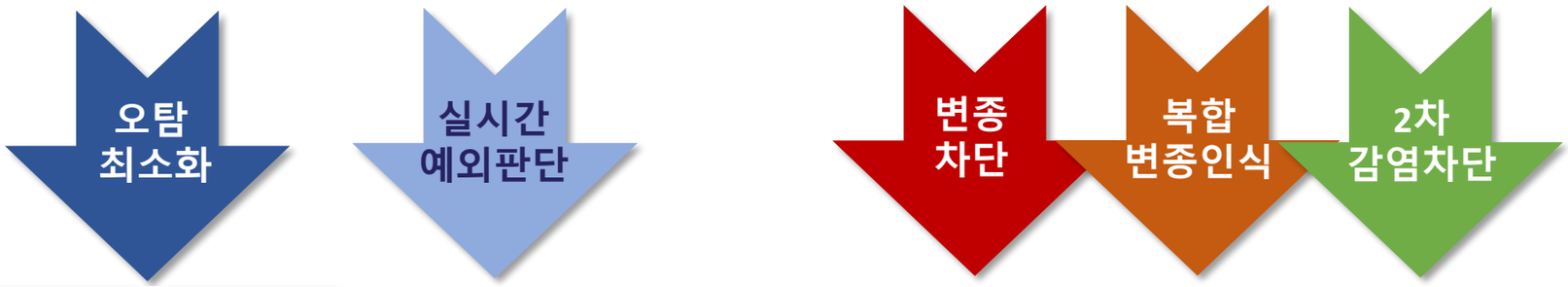
상황 및 내용기반 프로파일링 엔진 (ABC-P)

프로세스의 행위와 해당 시점에서의 시스템 상황 및 파일내용까지 전체적인 프로파일링

➔ 단순한 파일 변화감지 방식이 아닌 종합적 판단

➔ 신규 변종 차단 및 복합(Polymorphic) 변종 차단

➔ 윈도우 및 신뢰프로세스 2차 감염 차단



기존 및 신규변종차단 | **블랙리스트(시그니처) 방식이 아닌 다차원 , 상황 및 내용인식 프로파일링 엔진**

알파시큐어만의 고유 강점

경량화
(Light Weight)

단일 에이전트 확장성
(Extensions in One Agent)

➔ 기 구축된 보안 인프라와 최적의 연동

- 방화벽/ 메일보안/ iRM, DRM/ DLP/ 백신
- 기 **구축된 보안 인프라에** 또 다시 복잡한 **관리업무와 비용 추가의 부담 최소화**
- 리소스 및 가격에서 최소의 부담으로 가장 효율적이며 최종적인 엔드포인트 랜섬웨어 차단 기능 제공

➔ 원 에이전트 - 중장기 보안인프라 확장

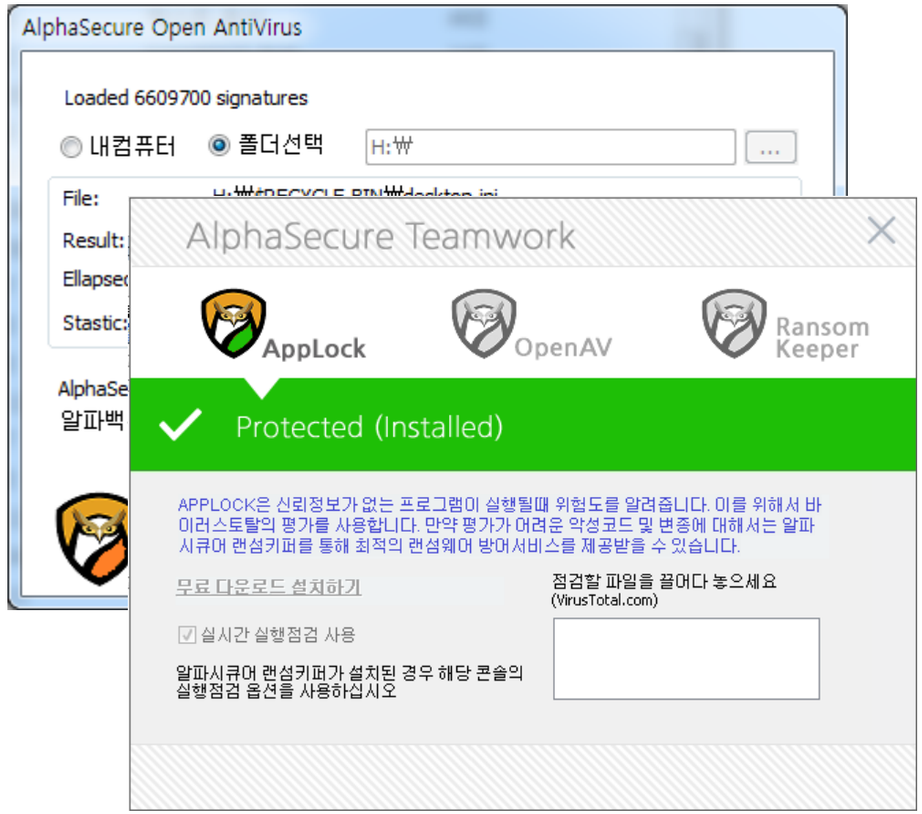
- 알파시큐어 **통합 보안 엔진을** 통해,
- **매체** 및 **출력**보안, **문서보안** 등 정보 암호화에 대한 통합 보안 인프라 구축이 가능
- 랜섬웨어에서 악성코드 전체를 대상으로, 실행 프로그램의 신뢰성을 확보할 수 있는 블록체인 및 EDR, 머신러닝 기반의 맞춤형 보안 엔진으로 확장

알파시큐어 확장 – 팀워크 (TeamWork)

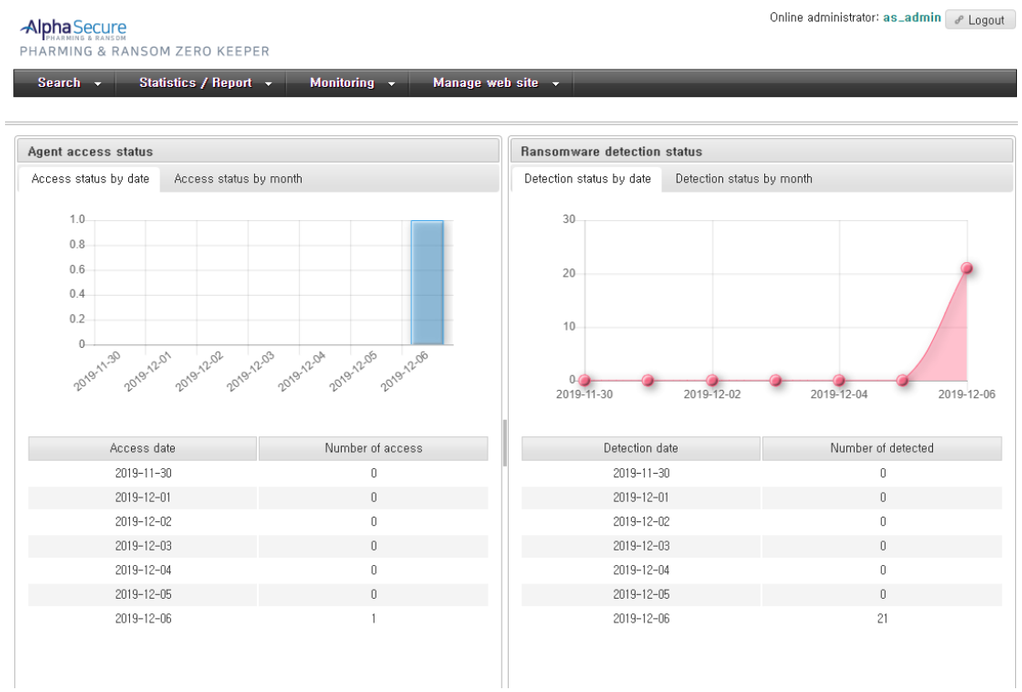
➔ **알파시큐어 AppLock**

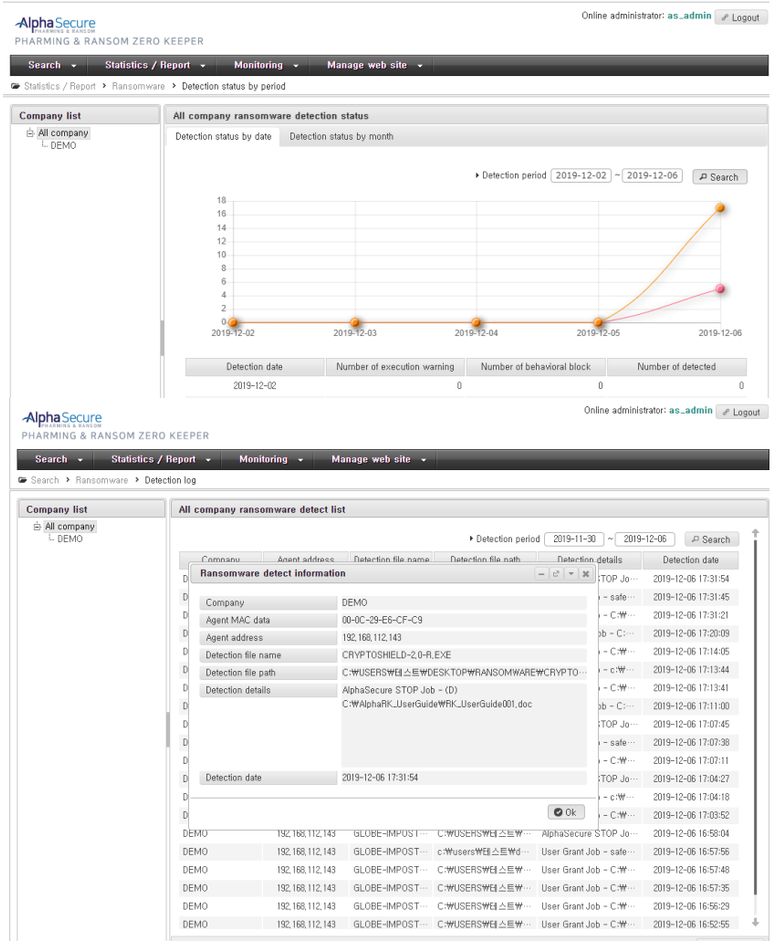
- Teamwork 패키지내 무상서비스
- 실행시점 검증에서 VirusTotal 연결 서비스
- Teamwork의 Cisco 시스템 ClamAV 백신서비스 연동

➔ **알파시큐어 팀워크(Teamwork)**



알파시큐어 서버 – 클라우드 대시보드

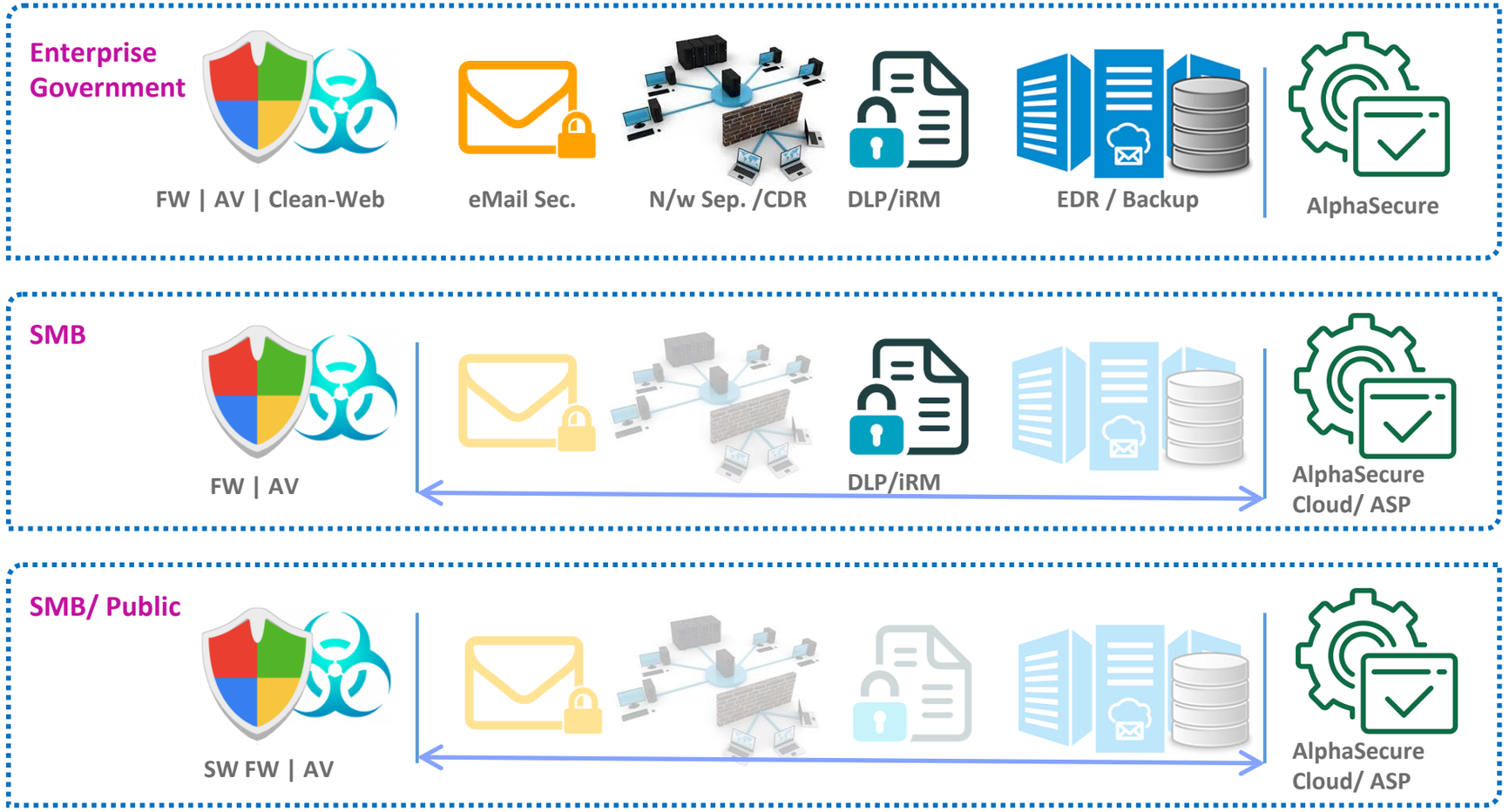




➔ 관리자 계정 (클라우드 접속)

- 공격 탐지 알림
- 에이전트 접속/ 상태 조회
- 사용자 및 사업장 옵션 정책 관리

알파시큐어 – 기존 보안체계 취약점 보강 : 최종 방어벽



제품 특허 및 인증 내역

특허증
CERTIFICATE OF PATENT

특허 Patent Number 제 10-1937325 호
출원번호 Application Number 제 10-2017-0142506 호
출원일 Filing Date 2017년 10월 30일
등록일 Registration Date 2019년 01월 04일

발명의 명칭 Title of the Invention
악성코드 감지 및 차단방법 및 그 장치

특허권자 Patentee
주식회사 시큐어링크(110111-*******)
서울시 서초구 강남대로 39길 26-7, 2층

발명자 Inventor
등록사항란에 기재

위의 발명은 「특허법」에 따라 특허등록원부에 등록되었음을 증명합니다.
This is to certify that, in accordance with the Patent Act, a patent for the invention has been registered at the Korean Intellectual Property Office.

2019년 01월 04일
특허청장
COMMISSIONER,
KOREAN INTELLECTUAL PROPERTY OFFICE
박 원주

특허청
Korean Intellectual Property Office

1등급
GOOD SOFTWARE

소프트웨어품질인증서
Certificate of Software Quality

상호 또는 성명 Name of Company / Name of Applicant : 주식회사 시큐어링크(655-87-00515) Securelink Inc.
소프트웨어의 명칭 Name of Software : 알파시큐어 랜섬키퍼 v1.0 AlphaSecure RansomKeeper v1.0
인증등급 Certification Level : 1등급
인증번호 Certification No. : 18-0246
제조자 및 제조국가 Manufacturer and Country of Manufacture : 주식회사 시큐어링크/대한민국 Securelink Inc./Republic of Korea
인증연월일 Date of Certification : 2018년(Year) 4월(Month) 26일(Day)
기타 Additional Information :

위 소프트웨어는 「소프트웨어산업 진흥법 시행규칙」 제5조제1항에 따라 인증되었음을 증명합니다.
I hereby confirm that the quality of the foregoing software has been certified under Article 5.1 of the Enforcement Decree of the Software Industry Promotion Act.

2018 년(Year) 4 월(Month) 26 일(Day)

TTA 한국정보통신기술협회장
CEO & President
Telecommunications Technology Association

특허등록 :

악성코드 감지 및 차단방법 및 그 장치

GS인증 :

한국정보통신기술협회 GS인증(1등급) 획득

해외 진출 및 R&D

뉴욕/코너티컷
Sacred Heart Univ. 공동 R&D 협의

Sacred Heart UNIVERSITY

➔ AI 및 행동프로파일 기반 차세대 EDR
➔ 블록체인 기반 폐쇄형 앱 신뢰 네트워크

SECURELINK GLOBAL

워싱턴
해외시장 마케팅 협의

➔ 북미, 유럽 및 글로벌 마켓 전문 공급 합작법인 검토
➔ 워싱턴 동부 보안업체 협력사 협의

3. 서비스 제공

서비스 현황 : 2017 서비스 시작 ~ (유료사이트)

55 + 만명

With pharming Zero

300 + sites

SMB 기업/ 병원/ 치과
시중 및 저축은행/ 손해보험
공공 및 퍼블릭 서비스

서비스 현황 : 2017 서비스 시작 ~ (유료사이트)

Government/ Public

Korea Institute for Advancement of Technology

Korea Culture and Tourism Institute

Korea Organ Donation Agency

Korea Fire Institute

Mutual Saving Bank

Real Estate Trust / Investment Bank

Public Bank

SMB/ Pharmacy/ Hospitals

AlphaSecure Cloud Service for Manufacturing
Over 100 ~ Companies :
Robesta Engineering, SeongKwang Laser,
Oand Design, JeongDo-Industry etc
Korea Dental Association
Over 150 Pharmacy Stores
SMB Hospitals

블랙리스트 기반 백신과 연동할 때 최적의 효율

1차 방어	2차 방어
잘 알려진 블랙리스트 기반 랜섬웨어 차단 (백도어 등 비 랜섬웨어 형 바이러스는 백신 고유영역)	**블랙리스트에 없는 변종 랜섬웨어 차단** (수많은 변종 및 고도화 변형 Polymorphic 악성코드)

3. 서비스 제공 – 기존 백신 연계

구축 (서비스) 타입

A-Type SaaS / Cloud type

B-Type Enterprise installation type

설치방법

1. 알파시큐어 보안센터 웹 페이지에서 설치 파일 다운로드
2. 또는 기업 자체 구축 페이지에서 다운로드
3. 또는 그룹웨어 등 연계된 서비스 페이지에서 배포

RANSOMKEEPER

제품 문의 및 상담 연락처

(08389) 서울특별시 구로구 디지털로 272 한신IT타워 807호 보안사업부

솔루션 문의

jslink82@securelink.co.kr

junyongko@securelink.co.kr

T. 02-3472-2136 F. 02-6953-2137

www.securelink.co.kr

www.secudog.com

SECURELINK

©SECURELINK Inc 2021. All rights reserved.