Cyber Kill Chain 관점에서

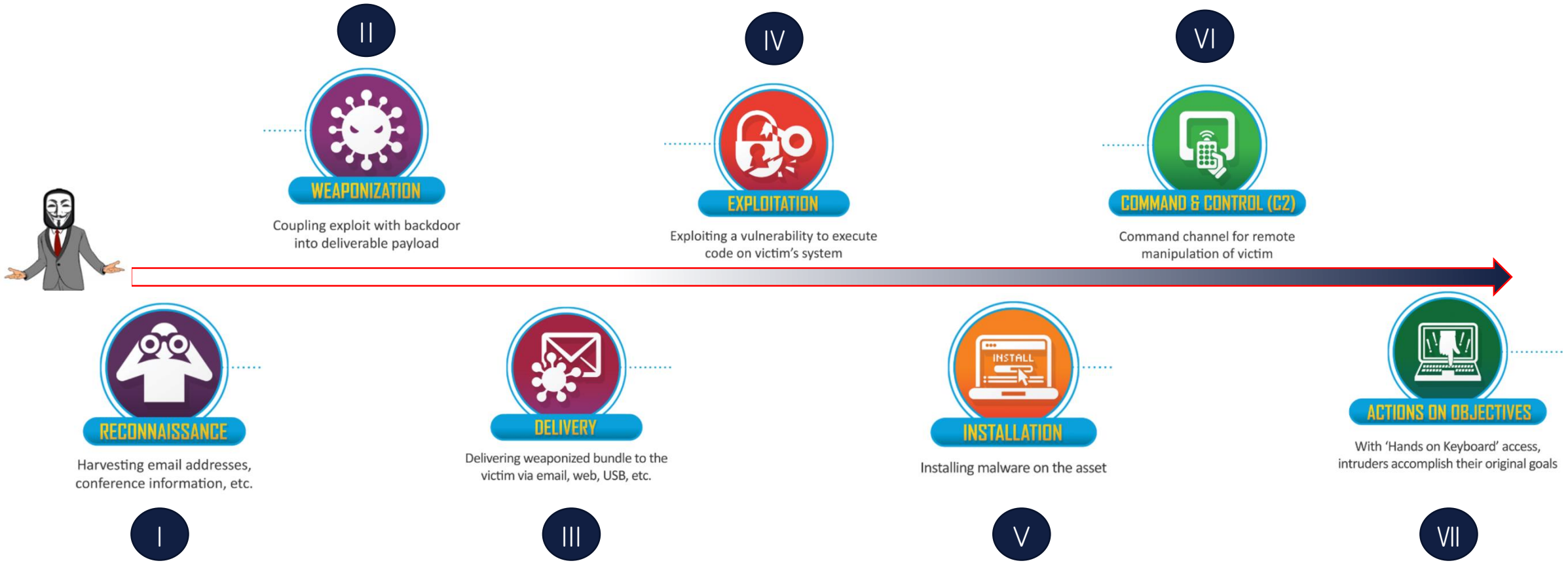
MultiScanning(멀티백신)과 Deep CDR 기술

- 차세대 APT 방어 기술 -

CK시스템즈 주식회사 | OPSWAT 한국 총판
www.cksystems.co.kr

OPSWAT.
www.opswat.com

Cyber Kill Chain



KISA – 2022년 글로벌 해킹그룹 동향보고

- **해킹그룹 섹터B07** — **취약점을 악용한 문서(파일) 악성코드 및 악성코드 포함된 압축파일**

섹터B07 그룹은 취약점을 악용한 문서 악성코드를 공격 대상에게 전달 후 변조된 웹 서버로 접근하게 했다. 섹터B25 그룹은 러시아어로 작성된 RTF(Rich Text Format) 형식의 악성코드를 공격에 사용했다. 러시아에서 해킹 활동이 발견된 섹터B31 그룹은 VBA 매크로 스크립트가 포함된 워드 문서를 공격해 사용했다. 섹터B34 그룹은 MS 문서에서 임의의 명령을 실행할 수 있는 취약점을 사용했다. 태국과 중국에서 다수의 정부 기관 관계자에게 스피어 피싱 이메일을 발송한 섹터B38 그룹은 워드 악성코드가 포함된 압축 파일의 비밀번호를 첨부했다.

- **해킹그룹 섹터D/E** — **PDF로 위장한 문서(파일) 악성코드 MS Excel, Word문서 및 RTF 문서(파일) VBA매크로 스크립트 악성코드**

섹터D 그룹에서는 이번 6월에 섹터D05, 섹터D10, 섹터D14, 섹터D22 등 4개 해킹 그룹의 활동이 발견됐으며, 각각 스피어 피싱 이메일을 발송하거나, 미국 대학 도서관 포털 페이지로 위장한 피싱 사이트 접속, 온라인 신문 PDF 기사로 위장한 악성코드를 사용했다. 또한, 채용 담당자로 위장해 시스템 내부 금융정보 및 자격증명 정보를 탈취하는 악성코드를 사용하거나 정부 반대 인물 또는 국가 정치, 외교활동 등 정부 관련 정보를 수집하는 것으로 분석됐다.

섹터E 그룹은 4개 해킹 그룹이 있으며, 파키스탄, 중국 등지에서 발견됐다. 이들은 VBA 매크로 스크립트가 포함된 MS 엑셀 문서를 정부기관 내용으로 위장해 공격하거나, MS 워드와 RTF 파일 등 문서형 악성코드 배포, CHM(Compled HTML Help) 파일 공격에 사용했다.

- **해킹그룹 섹터H** — **PPT 문서배포를 통한 문서(파일) RTA 악성코드**

섹터H 해킹 그룹 중 6월에는 섹터H03 그룹만이 인도 방위산업 수출 검토 주제의 파워포인트 문서 파일을 배포했으며, RAT(Remote Administration Tool) 기능을 가진 악성코드 피해자 시스템에 설치해 피해자 시스템에서 시스템 정보, 키로깅, 화면 캡처 등의 정보를 탈취했다.

한편, NSHC는 지난해 주목할 만한 랜섬웨어로 △ Clop △ Myransom △ CoderWare △RegretLocker △Fonix △Ranzy Locker △Nefilim 등 7개를 언급했다.

- **해킹그룹 섹터H** — **서면 인터뷰 이메일 첨부문서 위장한 문서(파일) 클릭 시 매크로 악성코드**

서면 인터뷰 위장, 첨부 파일 클릭 시 매크로 악용해 개인정보 유출

올해 7월 6일 싱가포르 국영 뉴스 채널 CNA의 이현석 프로듀서라는 이름으로 불특정 이메일 사용자에 북한의 핵실험과 동아시아의 군비 경쟁 우려에 대한 다큐멘터리 제작 관련 인터뷰 계획과 북한 전문가 섭외로 서면 인터뷰를 진행한다는 내용과 함께 수신자를 현혹했다.

SOURCE (2022년 9월 23일) : HTTPS://WWW.BOANNEWS.COM/MEDIA/VIEW.ASP?IDX=110081

2022년 랜섬웨어 동향보고

- **LockBit 3.0 랜섬웨어**

  저작권, 입사지원서 등으로 위장한 이메일을(첨부파일) 통해서 위장한 문서(파일) 클릭 시 랜섬웨어 유포

- **매그니베르 랜섬웨어**

  불특정 다수에게 업데이트 파일로 위장한 파일을 자동으로 내려주는 공격 방식,
  유포 파일의 종류(확장자) .msi, .cpl, .jse, .wsf 등으로 다양하고 지속적으로 변경

이스트시큐리티 시큐리티대응센터(ESRC)는 올해 7월부터 9월까지 국내에서 발생한 랜섬웨어의 특징을 △록빗(LockBit 3.0) 위협 지속 및 랜섬웨어 빌더 유출 △매그니베르(Magniber) 랜섬웨어 확장자 변경을 통한 지속 유포 △북한 배후 랜섬웨어 △국내 기업을 타깃으로 하는 랜섬웨어 △Go 프로그래밍 언어로 작성된 새로운 타깃형 랜섬웨어 등으로 요약했다.

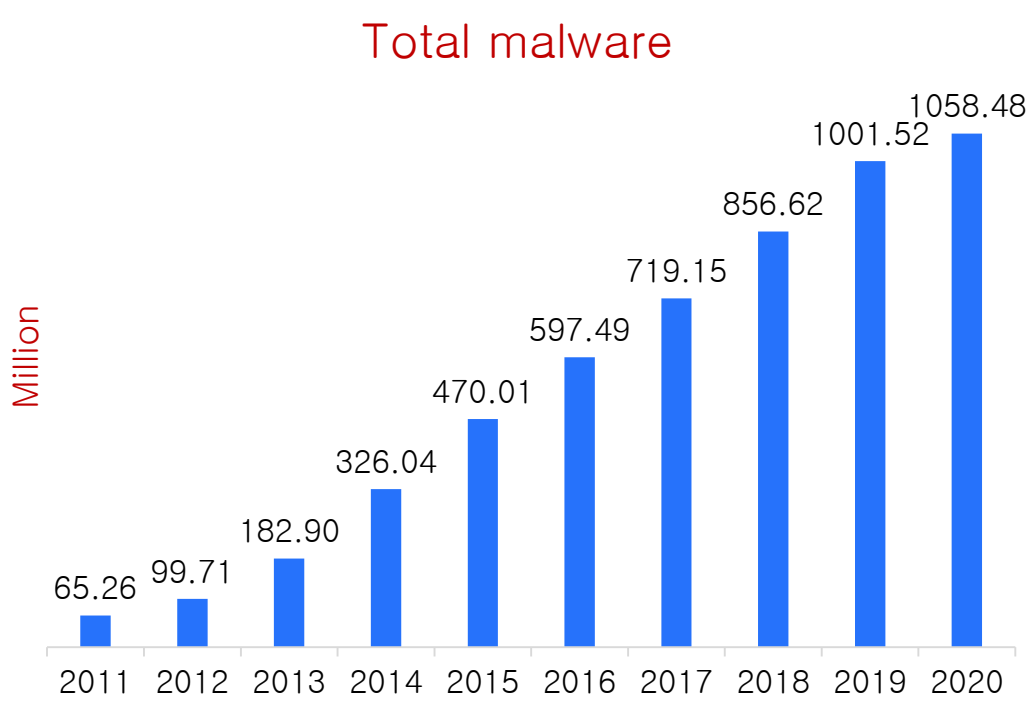
첫 번째로 LockBit 3.0 버전은 지난 7월 초에 발견됐다. LockBit은 2019년 처음 등장한 서비스형 랜섬웨어(RaaS)로 발견된 이후 꾸준히 업데이트 후 활동을 해오고 있다. LockBit은 저작권, 입사지원서를 위장한 이메일을 통해 국내에도 지속해서 유포되고 있어 주의가 필요하다. 9월 말에는 LockBit 3.0 빌더가 외부에 공개되기도 했다. 이 공개된 빌더를 이용하면 비전문가도 쉽게 LockBit 3.0 랜섬웨어를 커스터마이징해 제작할 수 있어 LockBit 3.0의 위협은 시간이 지날수록 더욱 증가할 것으로 예상된다.

매그니베르 랜섬웨어는 2017년 케르베르(Cerber) 랜섬웨어의 후속으로 등장했으며, 현재까지 활발히 활동 중인 랜섬웨어로, 유포 방식은 지속해서 변화하고 있다. 최근에는 대량 유포를 위해 타이포스쿼팅 및 광고 서버 해킹을 통해 불특정 다수에게 업데이트 파일로 위장한 파일을 자동으로 내려주는 공격 방식을 사용하고 있다. 유포 파일의 확장자도 .msi, .cpl, .jse, .jse, .wsf 등으로 지속적으로 변경하며 보안 프로그램 우회를 시도하고 있다.

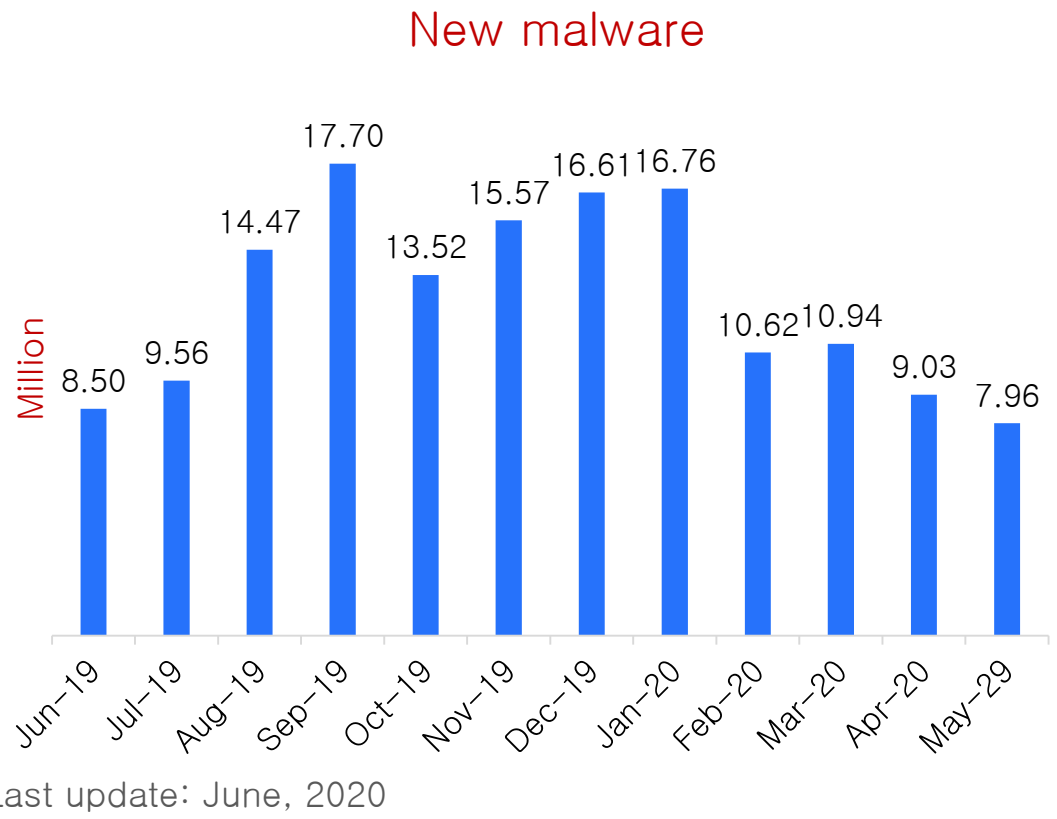
SOURCE (2022년 10월 4일) : HTTPS://WWW.BOANNEWS.COM/MEDIA/VIEW.ASP?IDX=110396&KIND=1

SECURITY & BUSINESS CHALLENGES

매일 35만개의 새로운 멀웨어 위협



Last update: June, 2020



Last update: June, 2020

Source: AV-TEST GmbH, www.av-test.org

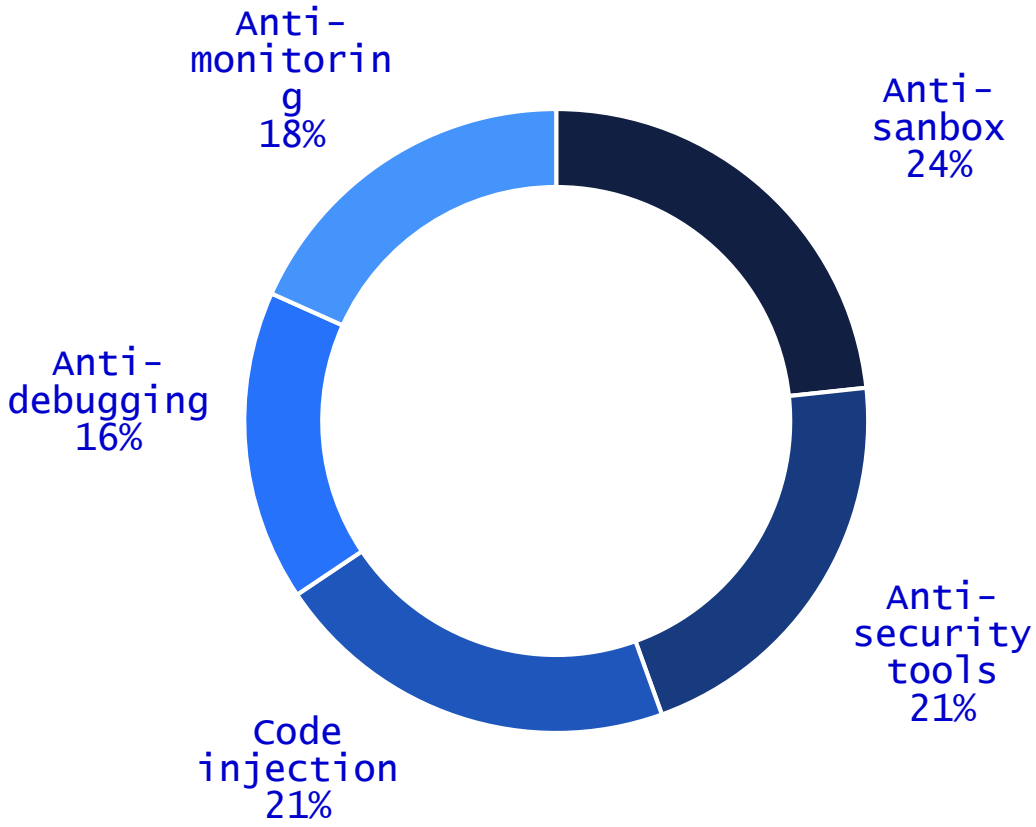
Anti-Malware 회피전술

98%의
멀웨어는 적어도 하나이상의 회피전술을 사용함

32%의
멀웨어는 “Hyper-Evasive" (6가지이상의 회피전술 사용)

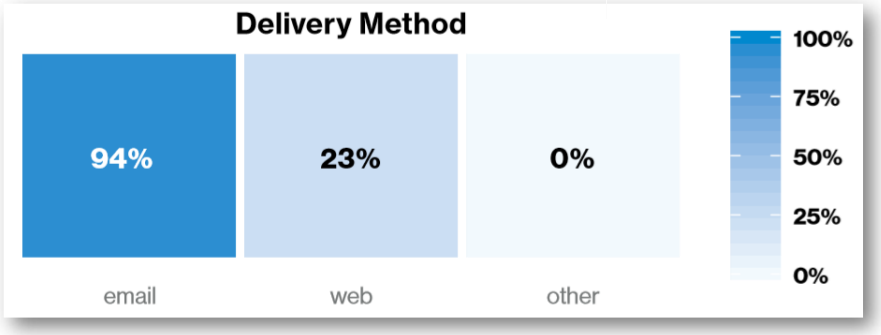
27%의
멀웨어는 단일 Sandbox에서 탐지 회피함

Source: Evasive Malware Now a Commodity' Security Week – Siggi Stefnisson, 2018



Source: VirusTotal and McAfee report

이메일 위협 - 94% 멀웨어는 **이메일**을 통한 감염



2019 Data Breach Investigations Report
Source: https://enterprise.verizon.com/resources/reports/dbir/

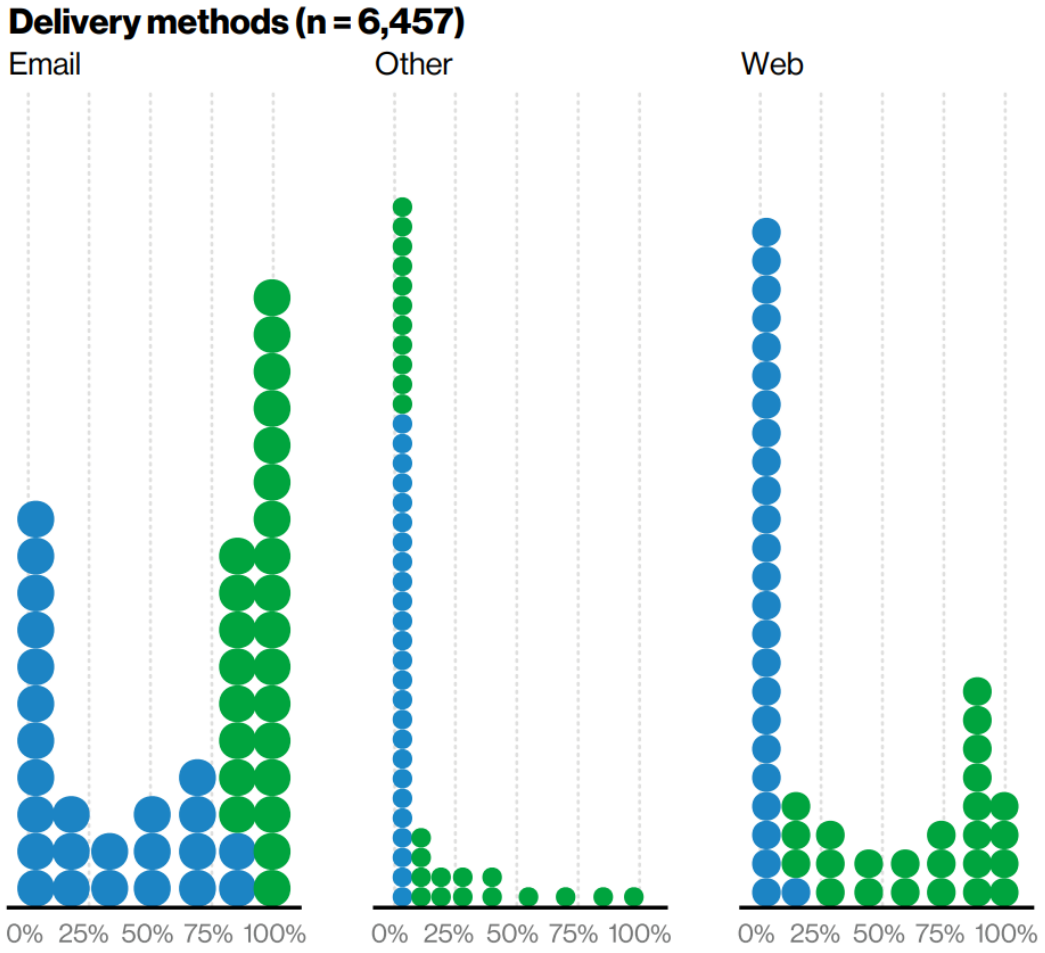


Figure 18. Top malware delivery methods 2020 Data Breach Investigations Report

망연계 보안위협 – 망분리 환경에서 보안에 가장 취약한 Point

최근 업무 망, 방산 망 등 외부와 독립적으로 분리되어 있는 산업기반 시설에 대한 사이버 공격이 급증하고 있는 추세입니다.

망 보안 강화를 위한 위협 대응

○ 어떤 환경에서든 바이러스/랜섬웨어/악성코드 등 Malware에 감염될 수 있지 않을까?

○ 어떤 파일이든 CVE취약성을 이용하여 내부 네트워크를 공격할 수 있지 않을까?

○ 망연계를 즉 망접점을 통해서 중요망으로 유입되는 파일에 어떤 보안위협이 존재한다면 상당히 치명적이지 않을까?

○ 기존 보안체계(NG Firewall, 단일Anti-Virus)로도 보안에 대해서는 그 보안 위협과 취약점을 대응 할 수 있는가?

【 망연계 보안위협 현황 및 이슈 】

news1 KOREA

더 이상 안전하지 않은 폐쇄망, 보안 인식 제고해야

망분리, 보안 점검과 보안 위협 제거해야...산업제어시스템도 점검 필요

(서울=뉴스1) 김수정 기자 | 2020-03-13 15:23 송고

https://www.news1.kr/articles/?3872950

아이뉴스24

'폐쇄망이라 문제없다'는 인식 안돼...시스템 구축·관제서비스 도입 필요

[아이뉴스24 김혜경 기자] 디지털 전환 가속화로 과거에는 별개로 여겨졌던 정보기술(IT)과 운영기술(OT) 영역이 밀접하게 연결되면서 산업기반 시설을 겨냥한 사이버 공격도 늘어나고 있다. 그동안 산업제어시스템(ICS)은 폐쇄망 운영으로 안전하다는 인식이 있었지만 최근

https://www.inews24.com/view/1467958

보안뉴스

"보안 USB 활용한 사이버공격, 내부망 장악 노렸다"

특정 프로그램으로 위장해 보안 USB에 악성코드 심어... 내부망에 연결된 시스템 노려

보안 USB의 인증제도 보안성 재검토, 침해사고 라이프사이클의 변화 추적 필요

https://www.boannews.com/media/view.asp?idx=70749

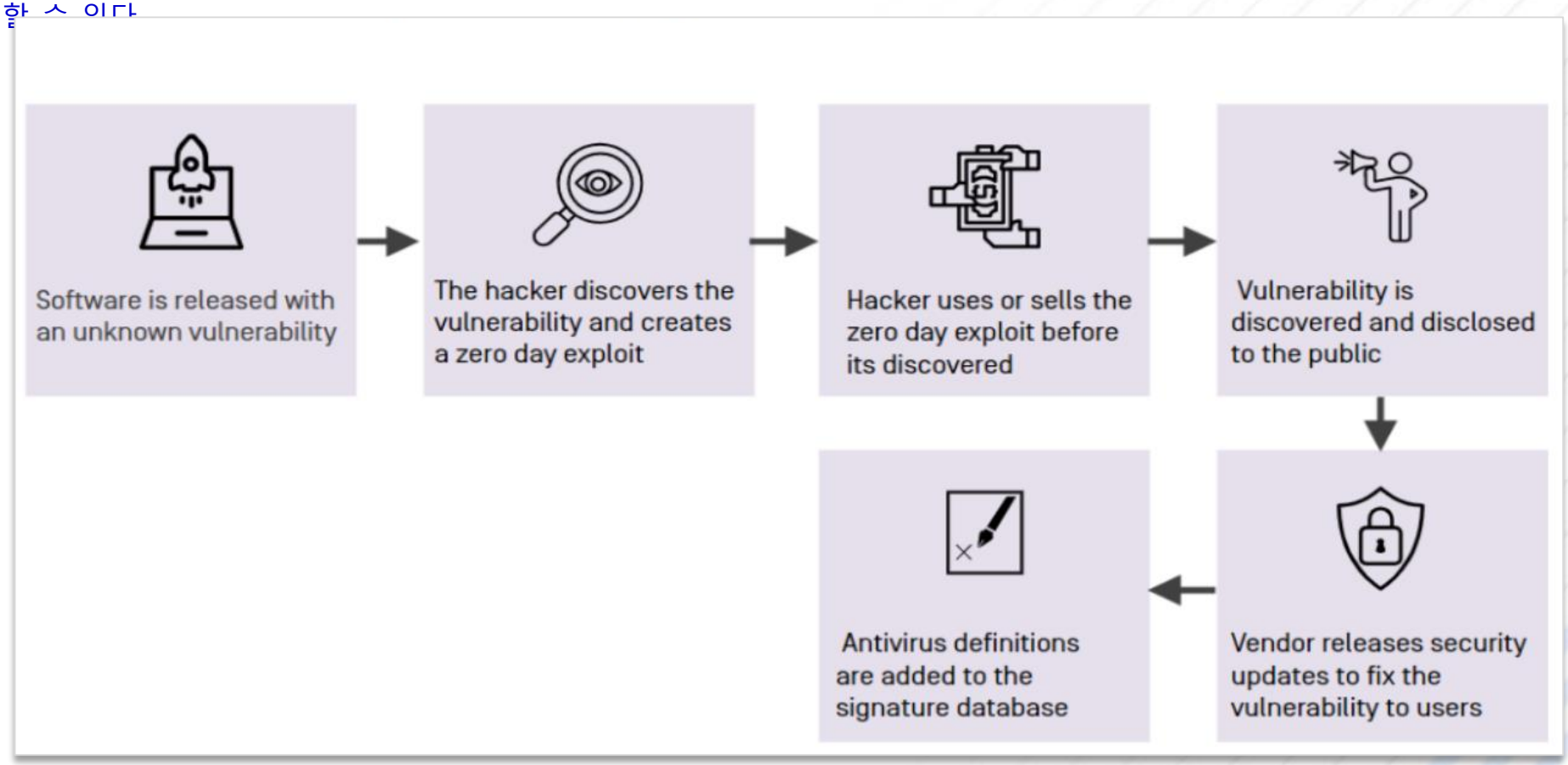
스토리지 보안 위협

다양한 경로로 다양한 형태의 악성코드, 랜섬웨어, APT공격코드, 피싱코드 등의 위협이

이미 스토리지 데이터까지 침입되어 수주일, 수개월 동안 악성코드화 및 C2서버화 되어

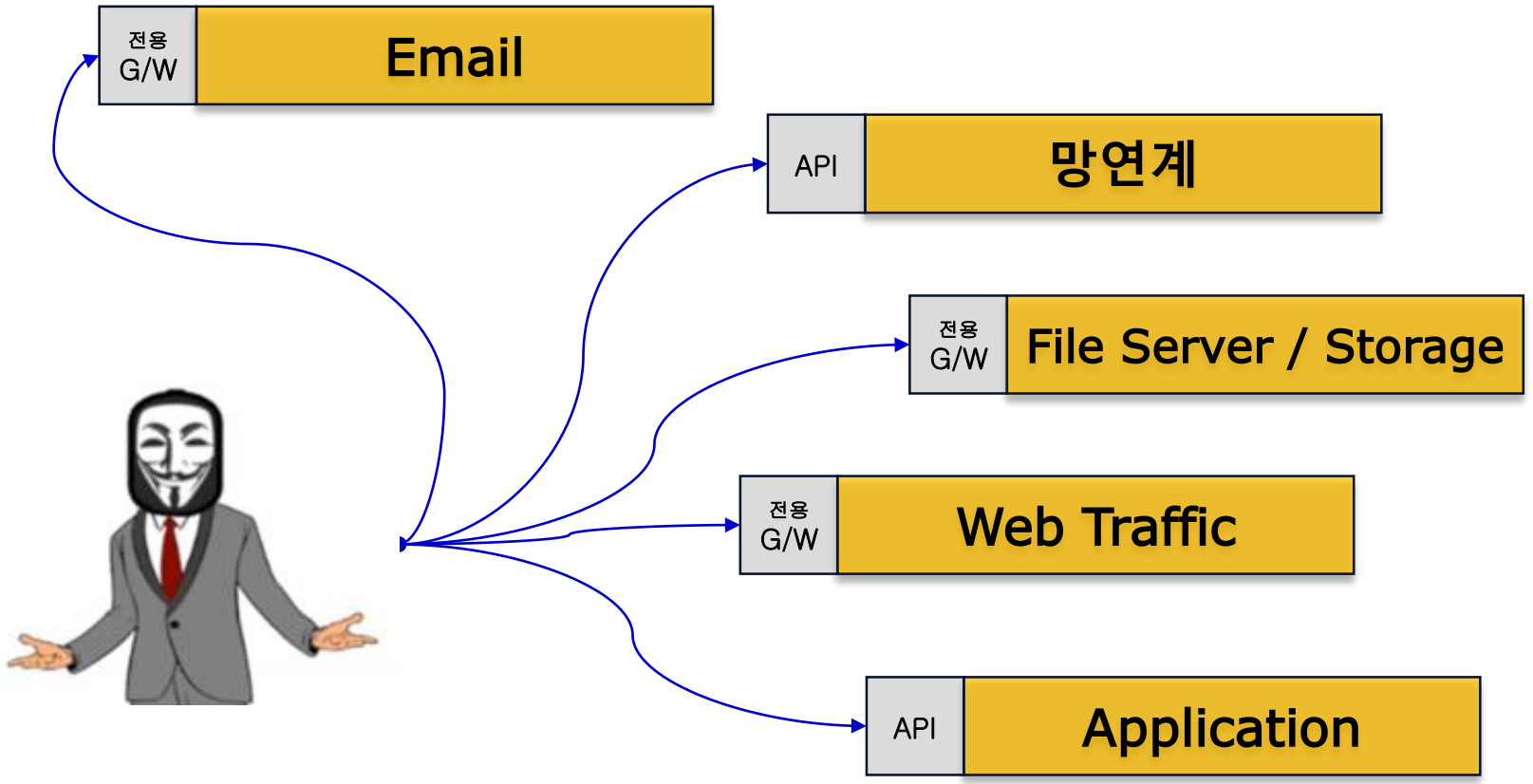
해커의 Command Channel 연결을 받을 수 있는

상태에 있다고 할 수 있다.



Attack Vector

Cyber Kill Chain 1단계에서 7단계에 이러러 조직내.외부로부터 유입되는 다양한 경로의 다양한 형태의 악성코드, 랜섬웨어, APT공격,
스팸/피싱 등 공격Vector별 즉 이메일, 망연계, 웹트래픽, 파일서버/스토리지, 어플리케이션 보안을 위협



- ▷ 랜섬웨어 확산
- ▷ 개인정보 탈취/유출
- ▷ 바이러스 확산
- ▷ 이메일 계정 탈취/원격조작
- ▷ 시스템 (Root)계정 탈취
- ▷ 피싱 사이트/피싱공격
- ▷ 시스템 마비
- ▷ 시스템 침투 Backdoor 확산
- ▷ C&C(C2) 서버 확산

Cyber Kill Chain 방어

- Threat Intelligence
- Multi A/V Scanning
- Deep CDR
- CVE Detection
- Sandbox
- Anti-Phishing

Cyber Kill Chain

1 단계~ 6 단계 방어

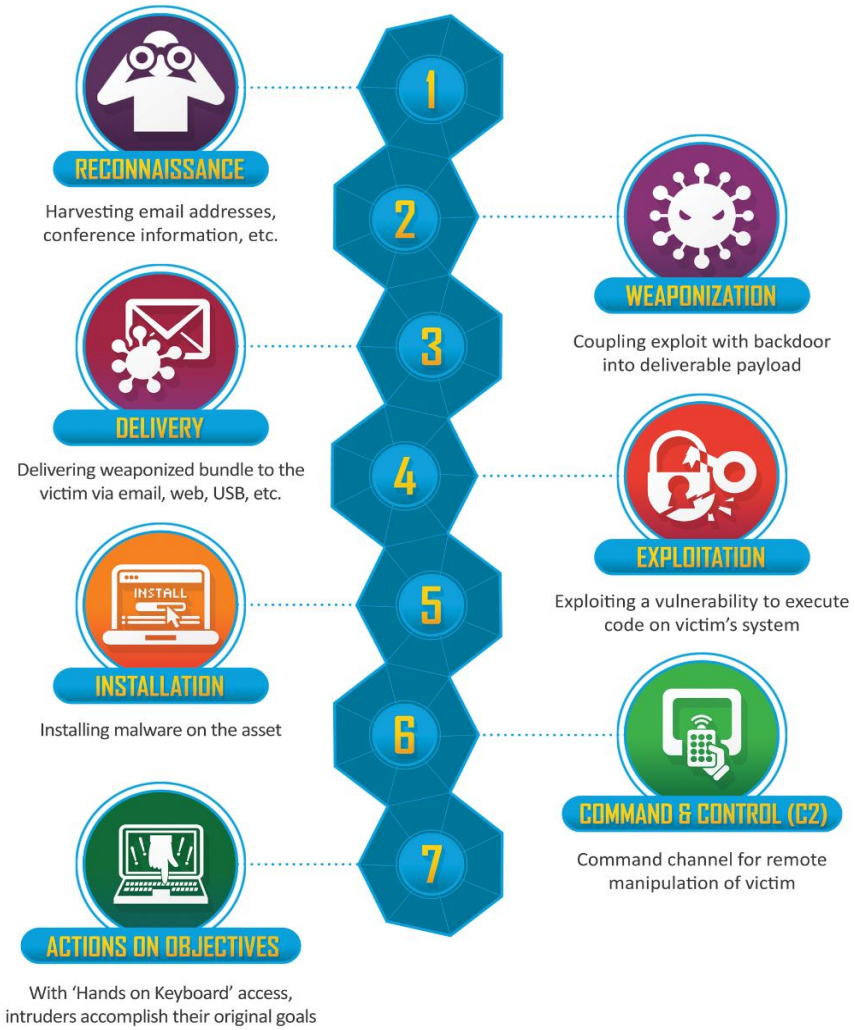
할 수 있는 검증된 기술

?

차세대 APT 기술의 Cyber Kill Chain 방어

Cyber Kill Chain 1단계에서 6단계를 커버가 가능한 조직내.외부로부터 유입되는 다양한 경로의 악성코드, 랜섬웨어, APT공격, 스팸/피싱 등 공격Vector별 즉 이메일보안, 망연계보안, 웹트래픽보안, 파일서버/스토리지보안, 어플리케이션 보안에 적용 가능 한 기술

- CVE Detection
- Threat Intelligence
- MultiScanning
- Deep CDR
- 차세대 Sandbox



Sandbox
(기존 VM기반 APT)

MultiScanning 멀티백신 기술

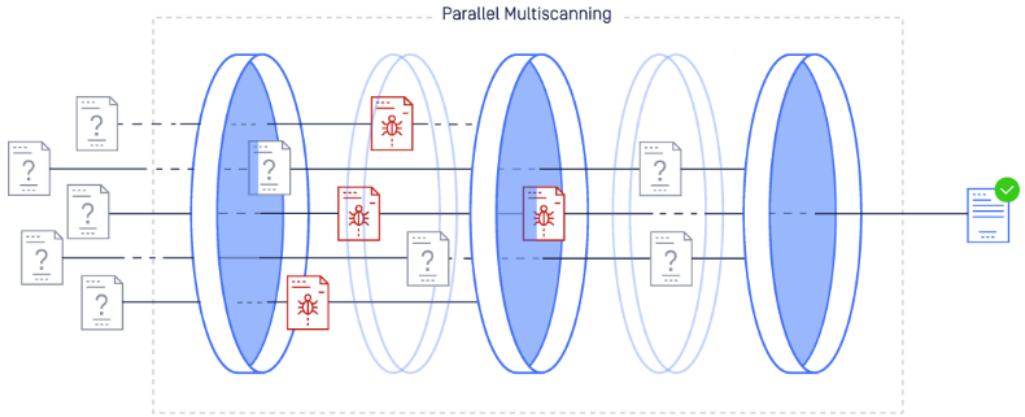
여러 개의 A/V엔진을 패러렐하게 스캔하는 기술

Multiscanning

Advanced Threat Prevention: Simultaneous Analysis with Multiple Anti-Malware Engines

Multiscanning is an advanced threat detection and prevention technology that increases detection rates, decreases outbreak detection times, and provides resiliency for single vendor anti-malware solutions.

OPSWAT pioneered Multiscanning to deliver enhanced protection to its customers from a variety of cyber threats.



A single antivirus engine can detect 40%-80% of malware / viruses. OPSWAT Multiscanning allows you to scan files with over 30 anti-malware engines on-premises and in the cloud to achieve detection rates greater than 99%.

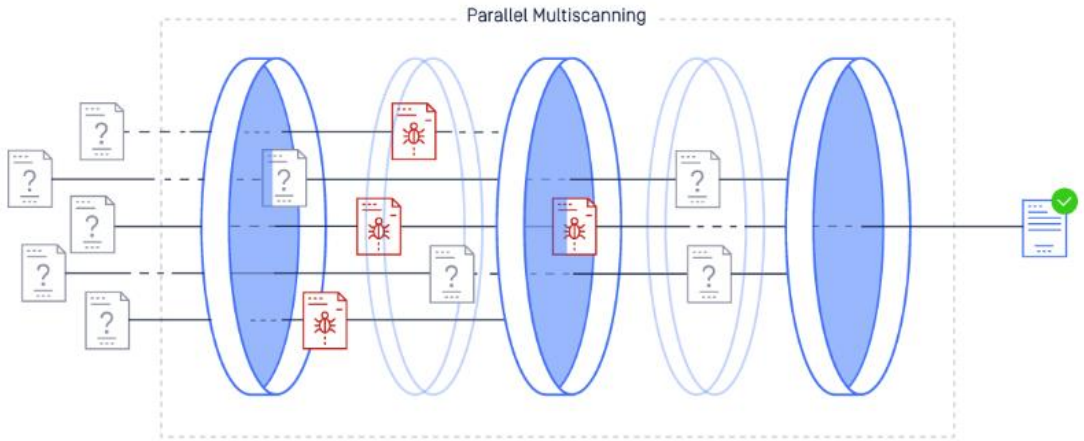
See our full list of AV engine partners.

- **Google 에서 사용하는 기술**
  - VirusTotal
  - Google 자체의 보안을 위해서 (2012년부터)
  - 일반 개인 사용자들에 무료 서비스

- **Google 과 OPSWAT 만이 유이하게 구현하는 기술**
  - 여러 A/V엔진을 패러렐하게 스캔하는 기술
  - 여러 A/V엔진을 패러렐하게 스캔하기 위한
    - **플랫폼 기술**
    - **성능적인 기술**
    - 글로벌 40여개 A/V엔진회사 들과 Alliance 필요

MultiScanning 멀티백신 기술

최대 35~45개의 A/V엔진을 패러렐하게 스캔하는 멀티백신 기술



AhnLab, Avira, ESET, COMODO CYBERSECURITY, RocketCyber, Bitdefender, TREND MICRO, CYREN, kaspersky, TACHYON, Zillya, McAfee, Virit, IKARUS, SOPHOS, Symantec, EMSISOFT, CROWDSTRIKE, ANTIY, Quick Heal, K7 SECURITY, NANO

- 이렇게 패러렐하게 처리할 수 있는 기술자체가 거의 독보적인 기술이며, 일부 업체가 2~3개의 백신으로 멀티백신이다라고 하며 제시하는 경우도 패러렐이 아니라, 직열로 side by side 방식으로 처리를 합니다.

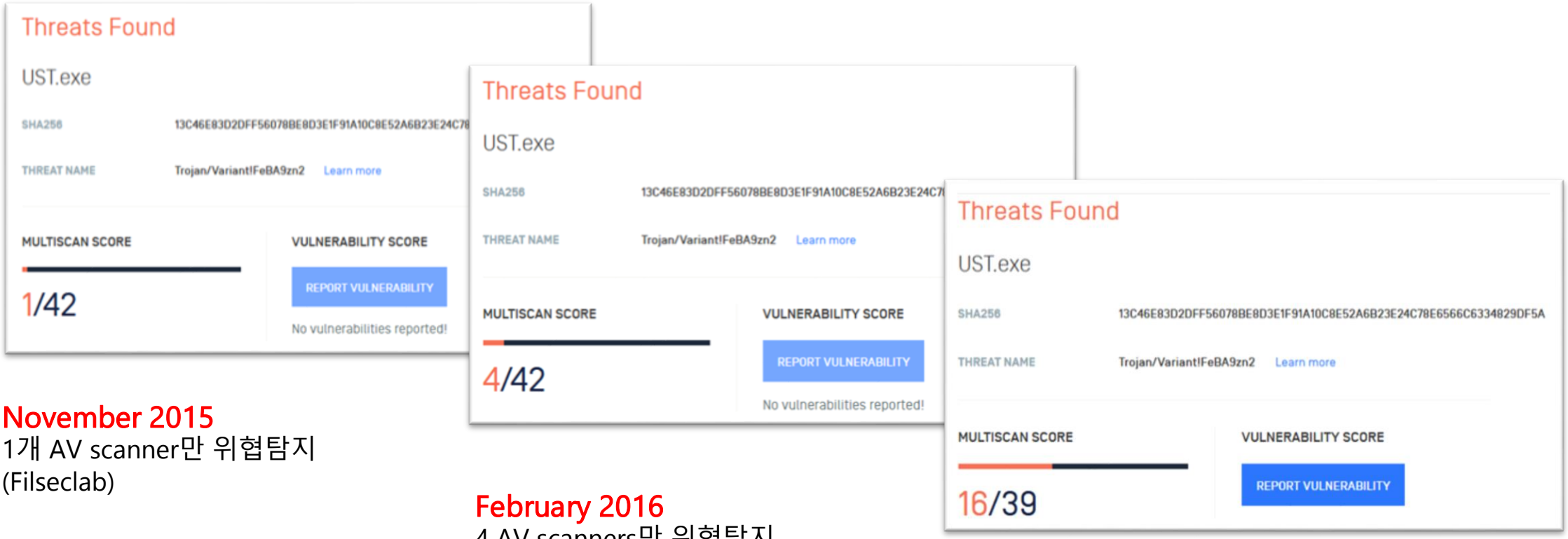
- 성능과 효용성
  - Detection Rate 획기적 증가
  - Outbreak detection times(발생탐지시간) 획기적 감소를 할 수 있는 기술

- Outbreak Detection
  - 어떤 A/V엔진은 악성프로그램을 탐지하는데 수일, 수주, 수개월이 걸릴 수도 있다 즉 Outbreak(발생) detection을 단일 A/V엔진으로는 아예 못 할 수 있습니다.

- Detection 알고리즘 융합 기술
  - 여러 A/V엔진이 각기 다른 알고리즘을 사용하는데 이러한 여러 알고리즘을 하나의 Detection 메커니즘으로 Platform화 한 기술

Anti-Virus 제품의 위협탐지 예시

Trojan/Variant!FeBA9zn2 에 대한 탐지 결과



November 2015
1개 AV scanner만 위협탐지
(Filseclab)

February 2016
4 AV scanners만 위협탐지
(Antiy, AegisLab, Filseclab, and Zillya)

May 2020
16 AV scanners만 위협탐지

Threat Intelligence – MultiScanning 기술에 융합

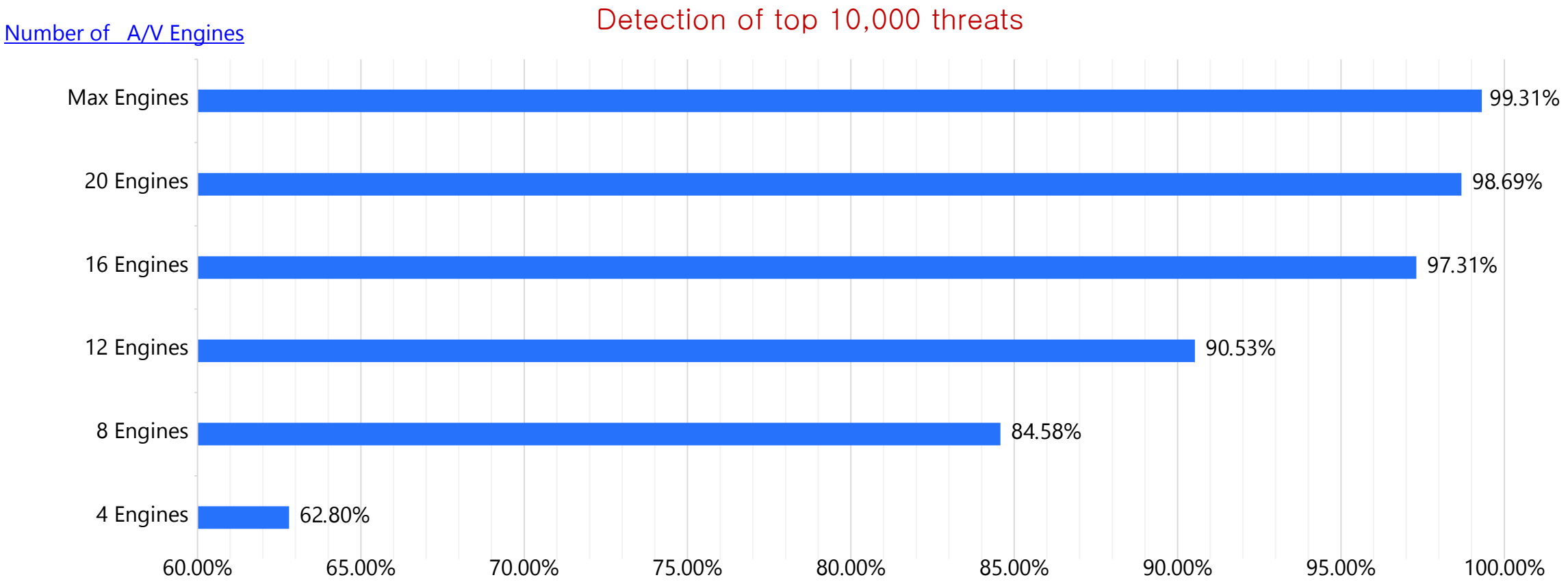
Threat Intelligence

다양한 TI평판 소스와 기능

- 클라우드 기반 소스
- 전문가 그룹
- 다양한 글로벌 고객사s
- 옵스왓 OEM 그룹
- 사이버보안전문 벤더 협력 그룹

- 위협 명칭
- 파일 타입
- 위협 카테고리
- 히스토리컬 데이터
- 랜섬웨어/악성코드 시그니처

Network MultiScanning 멀티백신 탐지능력



Source: https://metadefender.opswat.com, May 2020

Deep CDR 기술

파일 내부의 Malware를 근원적으로 제거 Deep CDR 기술

- Gartner 자료 - CDR기술

Gartner: CDR content sanitization technology scores high in network infrastructure security

Content Disarm and Reconstruction (CDR) technology is identified by Gartner as a 'high benefit' technology for network infrastructure security as it continues to mature towards mainstream adoption.

In the latest edition of Gartner's Hype Cycle report on network security (July '21)[1], content sanitization technology rates high on the priority matrix for network security, due to its ability to 'protect against exploits and weaponized content without the need for lengthy dynamic analysis or traditional content inspection techniques (such as signatures) for identifying malicious content.' Gartner's analysts identify CDR technology as being particularly useful 'where files are crossing organizational boundaries such as email, web and file content sharing sites.'

Table 1: Priority Matrix for Network Security, 2021

Benefit	Years to Mainstream Adoption	
	Less Than 2 Years	2 - 5 Years
Transformational		SASE
High	SD-WAN Secure Web Gateways Web Application Firewall Appliance	Content Disarm and Reconstruction DDoS Defense NDR Network Access Control Network Firewalls NSPM Remote Browser Isolation Security Service Edge
Moderate	Identity-Based Segmentation IPS	Enterprise Key Management Firewall as a Service Hardware-Based Security TLS Decryption Platform ZTNA
Low		

Source: Gartner (July 2021)

Deep CDR 기술

다양한 공격 Vector별로 악성코드/랜섬웨어/APT공격으로 인한 위협을 글로벌 최고의 Deep CDR 기술을 통해서
이에, 전세계 124종의 다양한 형태의 파일에 대해서 파일 내부의 Malware, Ransomware, Zero-Day Attack, APT Attack을 근원적으로 제거하여 악성코드를 Prevention 할 수 있는 솔루션을 추천 드립니다.

Deep CDR 기술이란 ?

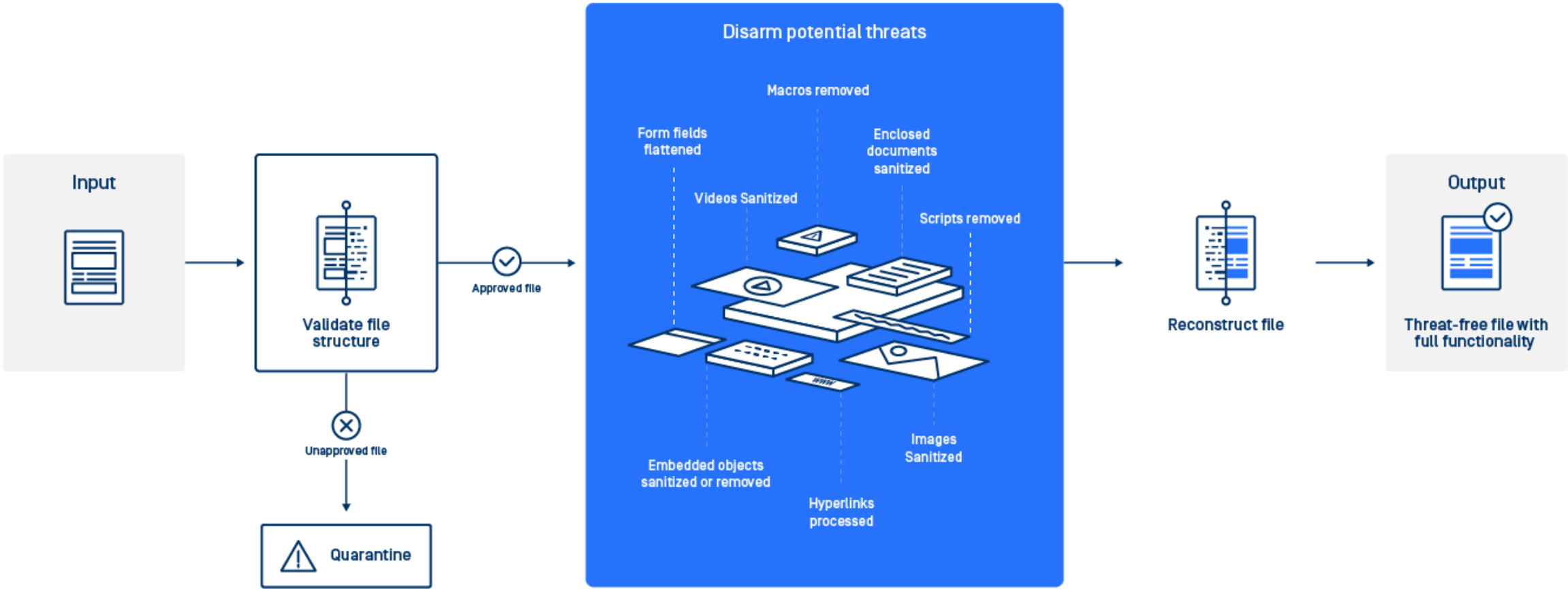
- 파일 내부의 악성코드 의심 요소 무해화 및 제거
  - Macro 살균처리.제거.무해화
  - Scripts 살균처리.제거.무해화
  - Embedded OLE Objects 제거.무해화
  - Hyperlinks 살균처리.제거.무해화
  - Image 살균처리.제거.무해화

기술의 성숙도/완성도에 대한 측도 ?

1. 전세계 다양한 형태의 파일 형태를 얼마나 많이 또 원활하게 지원하는가?
2. 파일 타입별로 데이터 살균.무해화 및 변환 옵션 제공하는가?
3. 원본 파일 별도 보관
4. 다양한 설정을 통해서 Processing 이 가능한가?
   - 분석.살균처리만 하는 옵션
   - 분석 후 분해 및 무해화 처리하는 옵션 등 가능
   - Monitoring & As goes by 방식

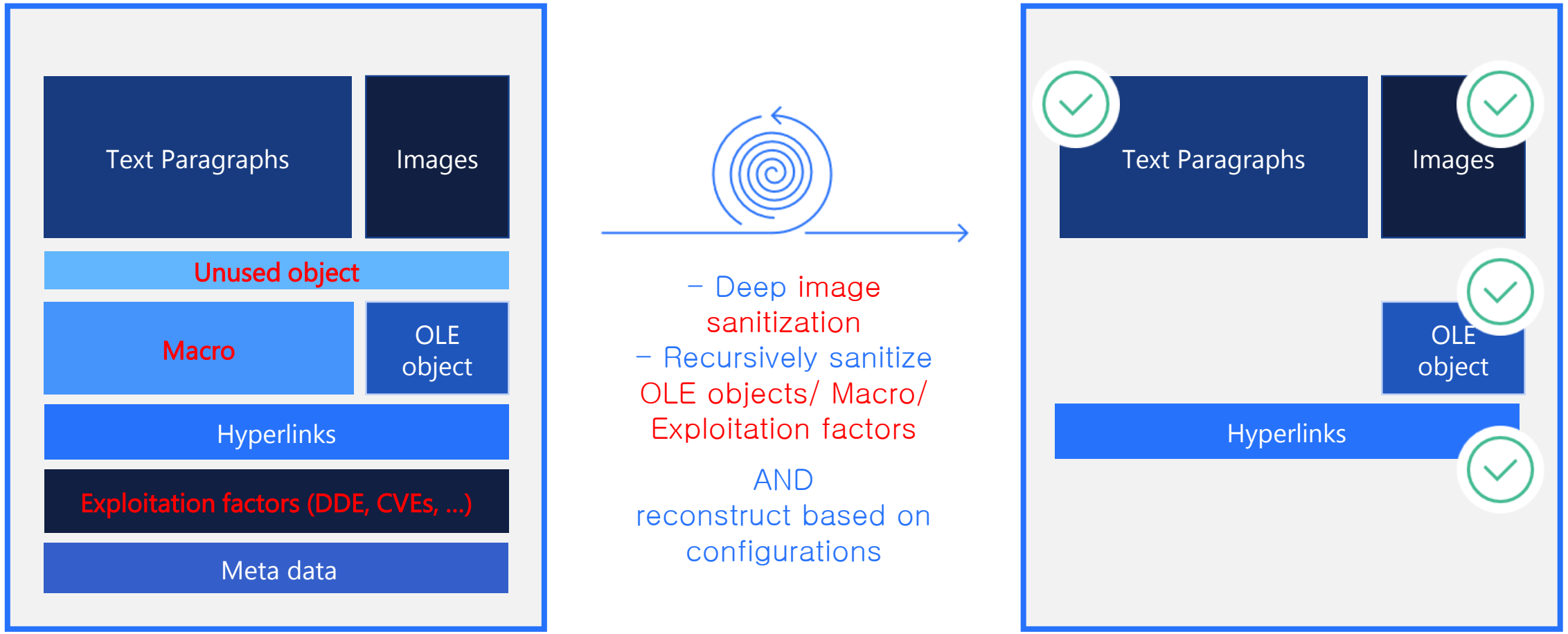
Deep CDR 기술

다양한 공격 Vector별로 악성코드/랜섬웨어/APT공격으로 인한 위협을 글로벌 최고의 Deep CDR 기술을 통해서
이에, 전세계 124종의 다양한 형태의 파일에 대해서 파일 내부의 Malware, Ransomware, Zero-Day Attack, APT Attack을 근원적으로 제거하여 악성코드를 Prevention 할 수 있는 솔루션을 추천 드립니다.



Deep CDR 기술

다양한 공격 Vector별로 악성코드/랜섬웨어/APT공격으로 인한 위협을 글로벌 최고의 Deep CDR 기술을 통해서
이에, 전세계 124종의 다양한 형태의 파일에 대해서 파일 내부의 Malware, Ransomware, Zero-Day Attack, APT Attack을 근원적으로 제거하여 악성코드를 Prevention 할 수 있는 솔루션을 추천 드립니다.

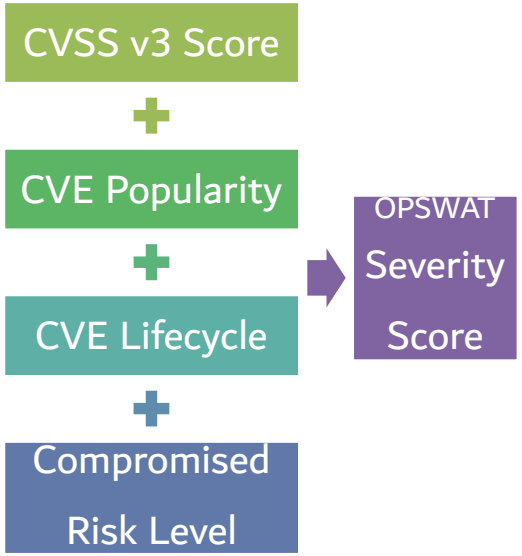


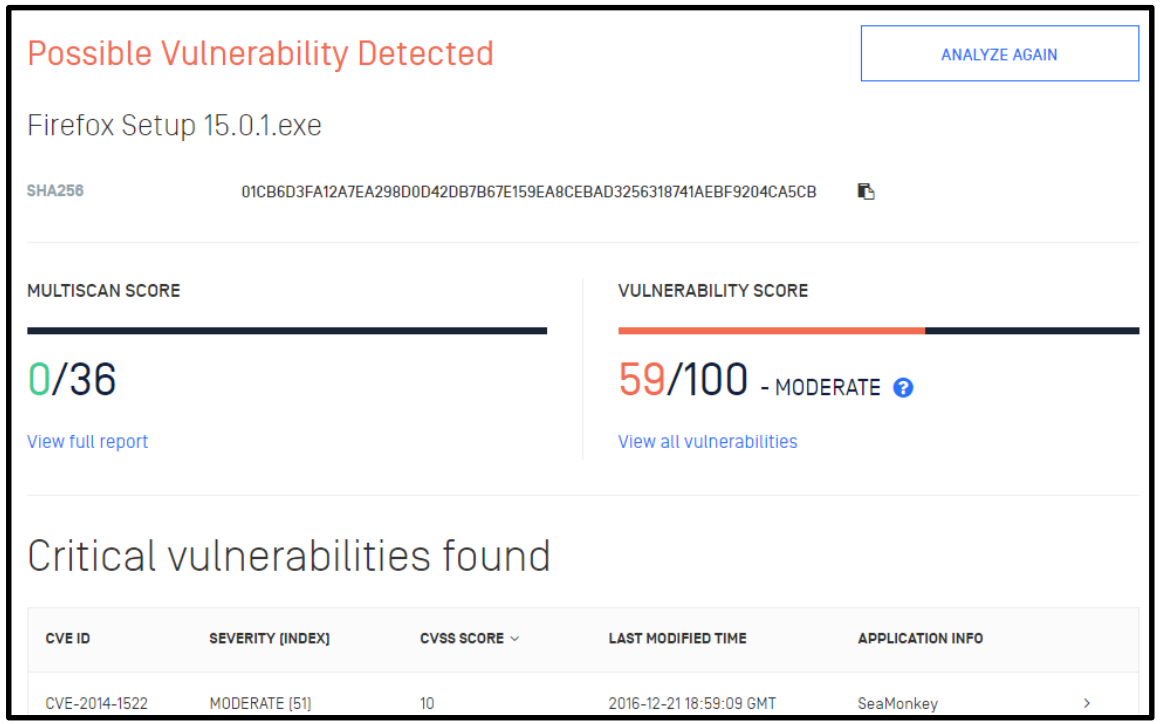
Network CVE 취약점 탐지 기술

Network Flow 상의 CVE취약점은 어떻게 대응하는가?

다양한 공격 Vector별 망 內 악성코드 유입이 가능합니다.
글로벌 20,000개 이상의 CVE취약점 특허기술이 탑재된 파일이 설치 실행되기 전에 CVE취약점을 탐지.제거하고 방어할 수 있는 솔루션 적용을 추천합니다.

CVE취약점 탐지.제거 스코어링 기술





Network CVE 취약점 탐지 기술

CVE취약점 Feed의 신뢰성 검증

- 설치프로그램 및 오프라인 장비 대상
- 검증된 CVE 취약성 소스(Feed) 활용하고 있는가?

  : MITRE, NIST, CVE, US-CERT, CPE, CVSS, OWAST
- 모발일 취약성에 대응이 가능한가? (Android, iOS)
- 자동 패치 적용이 가능한가?

차세대 Sandbox 기술

기존 Sandbox의 한계를 어떻게 극복할 것인가?

- 기존 동적분석(Dynamic 분석기술의 진화가 되었는가 ?
- VM사용하는 방식을 탈피하여 에뮬레이션 등의 자동화된 적응형 동적위협분석 기술을 구현한 기술인가?
- 에뮬레이션을 사용한다는 것은 동적 환경이 OS에 독립적인가?
- 악성 프로그램은 올바른 대상 환경이 존재하는 경우에만 코드의 진정한 악의적인 부분을 실행하며, VM을 사용하는 기존의 Sandbox는 일반적으로 이러한 위협을 간과합니다.
- Next-Generation SANDBOX 엔진은 은 분석의 확장성, 속도 및 깊이가 기존 Sandbox 기술을 훨씬 능가하며, 자동화된 적응형 위협 분석으로 Zero-Day 멀웨어 및 APT공격을 방어 근원적으로 방어 가능해야 합니다.

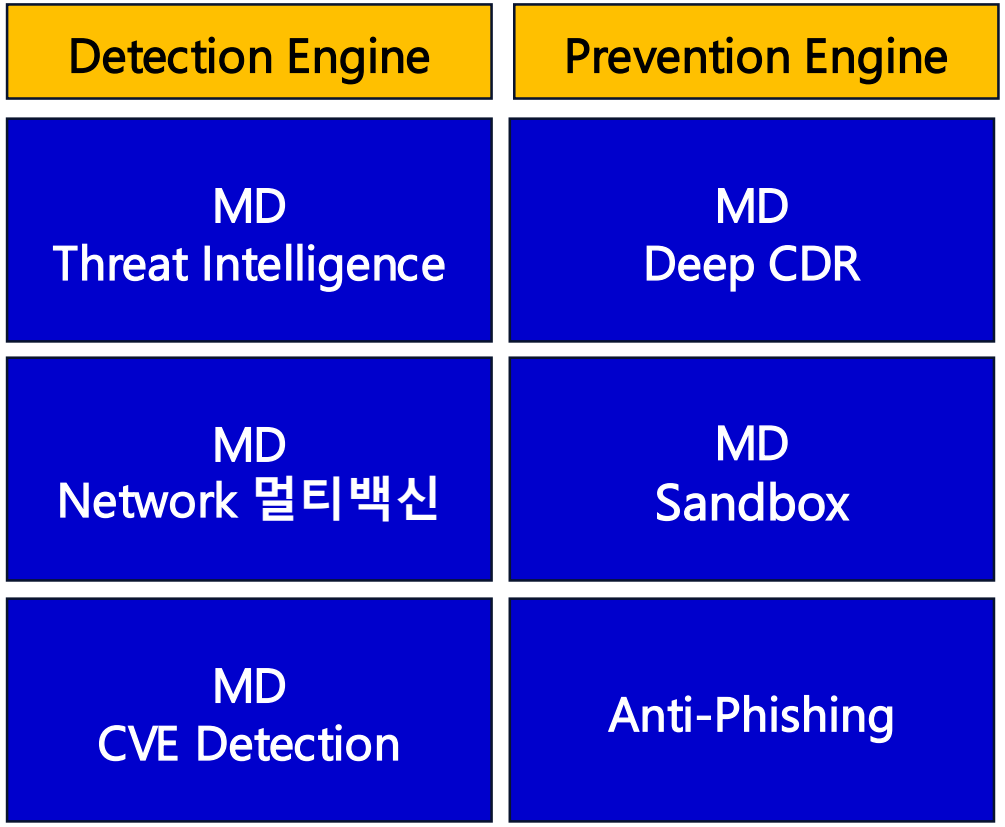
차세대 Sandbox 요건

- **APT 공격을 제대로 방어하는 솔루션 인가?**
- **기존 APT(Sandbox)의 한계점인 성능을 얼마나 극복 가능한가? (수십배 ~ 100배)**
- **VM의 한계를 극복한 자동화된 적응형 동적위협분석 기법으로 분석의 확장성, 속도, 분석레벨**
- **악성프로그램의 행위를 탐지할 수 있는 환경을 만들어 내는 기술인가? 이를 통한 Zero-Day Attack/ 멀웨어 방지에 탁월한가?**
- **MITRE ATT&CK 플랫폼에 Mapping (CERT 침해대응 전문가 등에 제공)**

차세대 APT 솔루션 - 악성코드·랜섬웨어 ·APT 공격 대응 솔루션

MetaDefender Security Suite 6**개 엔진으로 구성**

① **Threat Intelligence** 엔진 (글로벌 악성코드 평판DB)
② Machine Learning 기반의 **Multi A/V**(최대35개) 패러렐 스캔 엔진
③ **Deep CDR** 파일내부의 위해요소를 살균처리, 무해화 엔진
④ 글로벌 20,000이상의 **CVE취약성 탐지.제거** 엔진
⑤ 차세대 **Sandbox** 엔진 (기존 Sandbox솔루션 대비 100배 이상 성능)
⑥ 다양한 이메일 BEC 공격에 대응하는 Anti-Spam/Phishing 엔진



차세대 APT 대응 기술 - 실제 방어사례 예시

랜섬웨어 방어: TA505 ransomware attack

- HTML redirector가 첨부된 이메일로 배달됨
- 피해자가 HTML 파일을 열면 자동으로 악성 매크로 엑셀파일을 다운로드
- 엑셀파일은 피해자가 열었을 때 악의적인 페이로드를 떨어뜨리고 매크로를 활성화 함

탐지 실사례
MetaDefender Core removes Javascript in the HTML file

No malware downloaded

CVE취약점 방어: HAWKBALL Backdoor

- 악용된 MS 취약성 CVE-2017-11882 and CVE-2018-0802
- doc.rtf는 임베디드 페이로드 셀코드를 삭제하기 위해 방정식 편집기를 사용하는 OLE 객체를 포함
- 이 셀코드는 EQENDT32.EXE를 통해서 메모리에서 해독됨
- 암호 해독된 셀코드가 MS Word 플러그인 WLL로 삭제 됨
- 삭제된 페이로드의 DllMain이 문자열 WORD 여부를 확인하였으며, 샘플의 명령줄에 EXE가 있음, 문자열이 없으면 악성 프로그램이 종료되고, 문자열이 있는 경우 악성 프로그램은 RunDll32.exx 명령을 실행 함

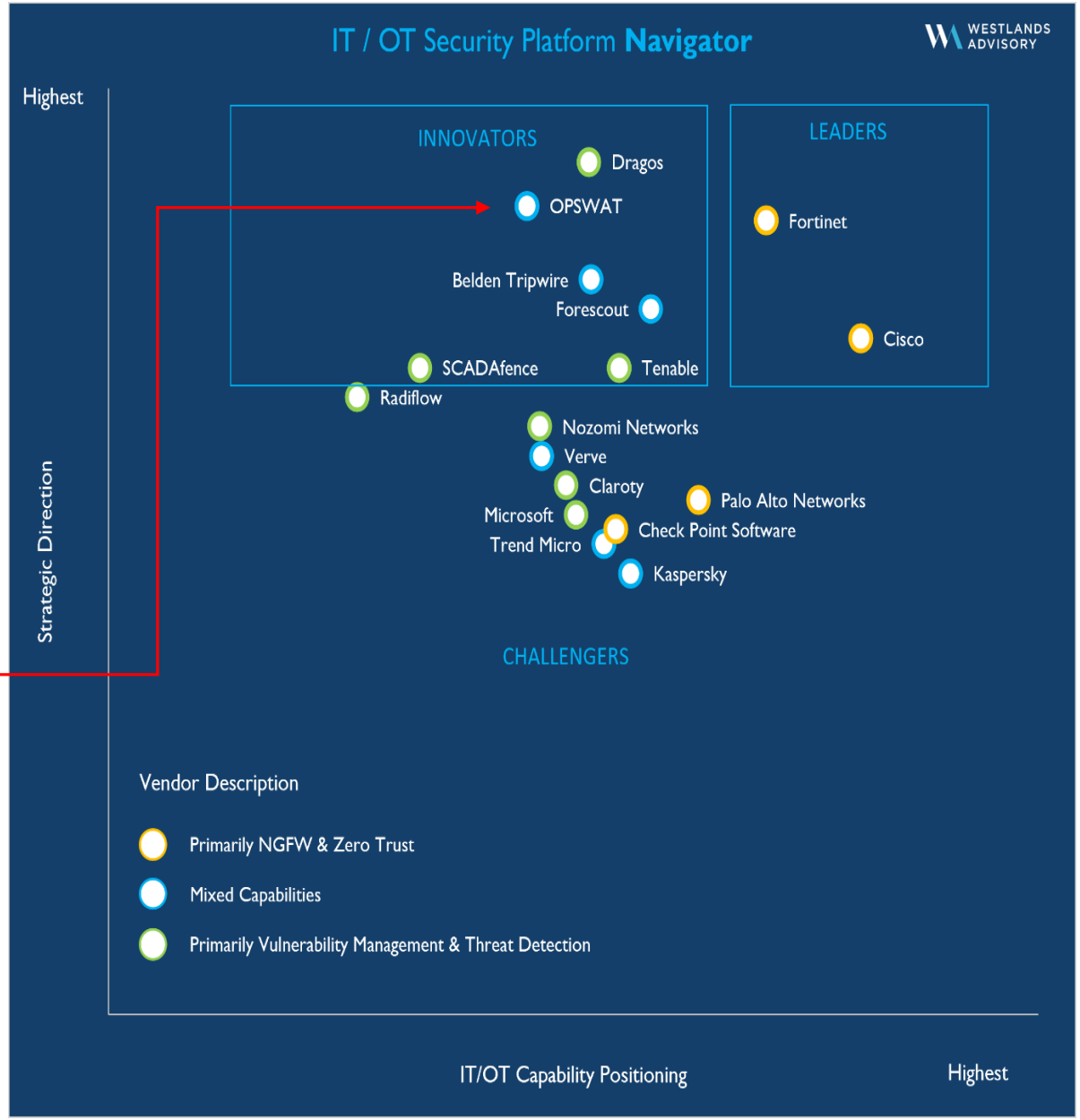
탐지 실사례
MetaDefender Core removes OLE objects

No shellcode dropped

Reputation

Westlands Advisory

- **IT/OT Security Navigator (MQ)**



차세대 APT 대응 기술 - Global Reference

중요 산업전반에서 시장과 고객 및 국방성, US-CERT, Homeland Security, NATO 등 중요 CIP고객사

GOVERNMENT

Ministry of Defence

NATO

UK Parliament

DEFENSE

Raytheon

RAFAEL
SMART AND TO THE POINT

leidos

Elbit Systems

LOCKHEED MARTIN

ENERGY

ONTARIO POWER GENERATION

Exelon

Chevron

Bruce Power

FINANCE

Canada Life

ZURICH

AMERICAN EXPRESS

Deutsche Bank

usbank

UK

BT

BOSCH

TELEDYNE

SONY

Lenovo

PHILIPS

TECHNOLOGY

CISCO

RSA

McKESSON

intel

CROWDSTRIKE

HEWLETT PACKARD

차세대 APT 대응 기술 - Korea Reference

한국 시장은 초기 시장진입 및 2022년 지사설립 및 본격적인 진출 및 진입 단계

OPSWAT.

www.opswat.com

감사합니다

차세대 APT 솔루션

Malicious Code | Malware | Ransomware | APT attack

공격 대응기술 비교 : 멀티백신, Deep CDR, Sandbox(기존 APT솔루션)

항목	MetaScan (멀티백신)	Deep CDR	Sandbox (기존 APT 솔루션)
요약	. 글로벌 실시간 업데이트 되는 시그니처 DB를 기반으로 파일이 안전한지, 악성코드가 포함된 것인지 결정(Detection)	. 파일이 안전한지, 악성코드가 포함된 것인지 탐지(Detection)하고 악성코드가 포함되었다면 제거(Prevention)	. 파일에 포함된 악성코드가 (해커에 의해서) 어떤 행위를 일으킬 때 그 행위를 분석하여 탐지.제거
작동 방식	. 파일을 스캔하기위해서 멀티 A/V엔진 사용 . 이는 Detection Rate, 노출시간을 줄여주며, 각 A/V엔진의 다양한 기술을 통합하여 악성코드 탐지	. 파일 내부의 구성요소들 Macro, Script, OLE Object, Picture, 내부 File, URL Link 등 일체에 대해서 무해화 및 살균처리	. VM을 load해서 파일에 여러 시리즈의 테스트 수행 . 테스트결과에 기반해서 악성코드 여부 판단
IT자원 사용	. 각 A/V엔진은 microsecond에서 몇 초 내에 스캔 및 판단 (CPU, Memory 사용율이 낮음)	. 각 A/V엔진은 microsecond에서 몇 초 내에 스캔 및 판단 (CPU, Memory 사용율이 낮음)	. Sandbox는 리소스를 상당히 많이 사용하며 (CPU, Memory 사용율이 높아 고사양 HW필요)
성능	. 일반적으로 Sandbox에 비해 30배 이상 빠른 성능	. 일반적으로 Sandbox에 비해 30배 이상 빠른 성능	. 행위분석 및 판단에 상당한 시간이 소요됨
적용/도입 주 목적	. 대량의 파일 트래픽에 대해서 효과적으로 악성코드 스캔	. 대량의 파일 트래픽에 대해서 가장 원천적으로 악성코드 탐지 및 제거	. Block된(Detection된) 파일에 대한 악성코드 분석 . Block된(Detection된) 파일에 대한 오탐 여부 분석
Cyber Kill Chain 커버리지	. 3단계 DELIVERY / 4단계 EXPLOITATION / 5단계 INSTALLATION 3개 영역의 광범위한 시그니처기반 Detection 에 초점	. 3단계 DELIVERY / 4단계 EXPLOITATION / 5단계 INSTALLATION 3개 영역의 전세계 124종의 파일에 대한 근원적인 Detection & Prevention	. 6단계 Command & Control 영역을 담당하여 (해커의) 행위에 대한 Detection & Prevention
결 론	MetaScan(멀티백신), Deep CDR, Sandbox 기술은 적용 및 사용 목적이 다르며, 따라서 Cyber Kill Chain 7개단계에서 각각 방어하는 영역과 기술이 다름		