퍼즐의 완성 : 이제 결정하세요!

평가 가이드라인

파이어아이 코리아
부성현 수석 컨설턴트

현재 고민은

해본 경험이 없기에 선택된 평가 방식

EDR도 엔드포인트 보안 솔루션이기에

갖출 건 다 갖추었는데
뚫리는데… 그래 우린
EDR이 필요해

EDR은 잘 모르겠지만
엔드포인트 보안 솔루션
이니 탐지율이 좋아야겠지

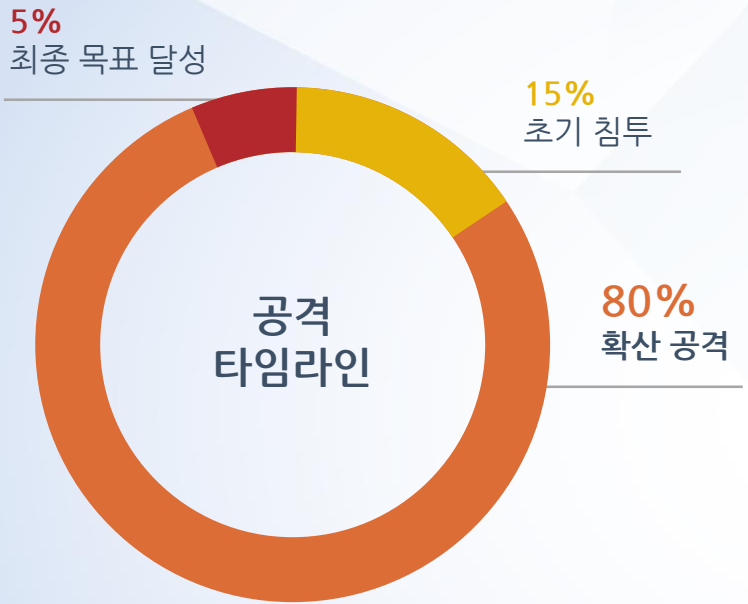
**EDR이 보안의 화두인데
어떤 솔루션이 좋을지는
고민해봐야 하지 않을까?**

엔드포인트 보안 솔루션
대표주자는 백신이자나

**얼마나 많은 샘플을 탐지하는지
비교 테스트 해봐야겠다**

악성코드 샘플 테스트의 한계

첫 번째 이유 : 악성파일은 실제 공격에서 생각보다 많이 사용하지 않는다



확산 공격에 사용된 테크닉 TOP

- Psexec
- SMB
- Remote Desktop
- Powershell
- WMI
- Scheduled tasks
- Remote registry
- Admin share
- Pass-the-hash
- VNC / Ammy Admin / Teamviewer

출처 : www.smokescreen.io

악성코드 샘플 테스트의 한계

두 번째 이유 : 테스트를 위한 악성파일 샘플의 정합성을 확인하기 어렵다

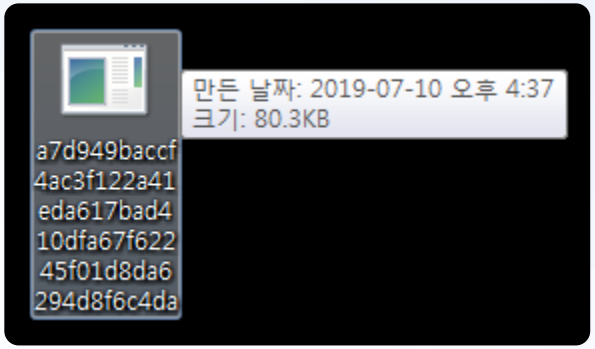
VirusTotal

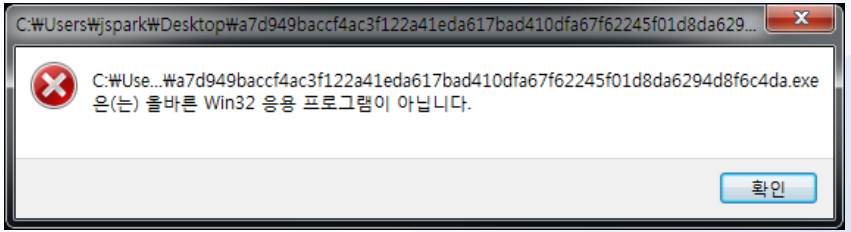
세

tag:corrupt type:peexe positives:20+ Search Hash

1000+ files found

File	Ratio	First sub.	Size
a7d949baccf4ac3f122a41eda617bad410dfa67f62245f01d8da6294d8f6c4da 85836c97a70292785e484b7feedf9936 corrupt peexe	51 / 69	2019-07-10 05:34:09	80.3 KB
24a5ca26514f66091ca2fc3cc20c9759a74933cde1cc92c8c753f900fd2016b1 03d510a2cac9ea4c40c229dd7be426fa corrupt peexe	49 / 69	2019-07-10 05:34:08	97.0 KB
82cc23a63800f78891dcaaf8afb44b80d1a35dd0edff58b8dffa822740def90c 49d97b416c15b56d0951feb92e364d8d corrupt peexe	53 / 71	2019-07-10 05:34:06	76.6 KB
d8141b39039c801a97b19ccd4ea7bfb87e521848bafd4ba61c7c65fa659c1036 e57452915a408ddf7dd6371682d3773a corrupt peexe	47 / 72	2019-07-10 05:30:50	178.3 KB
a04bb086386320d850fa44ec98ca53de922a0ff220a2b77b921e0fdeb56421fd ccd57184c39b407589029cf5cc92f5db corrupt peexe	32 / 70	2019-07-10 05:30:47	7.0 KB





악성코드 샘플 테스트의 한계

세 번째 이유 : 수집된 샘플은 이미 알려져 있다라는 의미이다

자체적으로 샘플을 만들기엔 한계가 있다

샘플을 알려진 공유 사이트에서 수집한다

결국 수집된 샘플은 이미 알려진 샘플이다

EDR의 목적을 상기해보자

알려지지 않은 공격에 대한 대응이라는점!!!

악성코드 샘플 테스트의 한계

네 번째 이유 : 악성파일이 탐지되고 치료되었다고 대응이 끝나는 것이 아니다

대응의 의미가 무엇일까요

119877258d9e5ff6b4e1a70a3c8f3692

?

Ad-Aware	Gen:Variant.Zusy.210214	**K7AntiVirus**	Trojan-Downloader (00505d4c1)
AegisLab	Trojan.Win32.Generic.4!c	**K7GW**	Trojan-Downloader (00505d4c1)
AhnLab-V3	Malware/Win32.Generic.C1628944	**Kaspersky**	HEUR:Trojan.Win32.Generic
ALYac	Gen:Variant.Zusy.210214	**MAX**	malware (ai score=100)
Antiy-AVL	Trojan/Win32.AGeneric	**McAfee**	Artemis!119877258D9E
Arcabit	Trojan.Zusy.D33526	**McAfee-GW-Edition**	BehavesLike.Win32.Dropper.ch
AVG	FileRepMetagen [Malware]	**Microsoft**	Backdoor:Win32/Joanap.K!dha
Avira	HEUR/AGEN.1034033	**MicroWorld-eScan**	Gen:Variant.Zusy.210214
AVware	Trojan.Win32.Generic!BT	**NANO-Antivirus**	Trojan.Win32.Agent.elqesg
BitDefender	Gen:Variant.Zusy.210214	**Paloalto**	generic.ml
CAT-QuickHeal	Trojan.Dynamer.9130	**Panda**	Trj/GdSda.A
ClamAV	Win.Trojan.Ratankba-6042510-0	**Qihoo-360**	Win32/Trojan.5a2
CrowdStrike	malicious_confidence_70% (D)	**Rising**	Backdoor.Joanap!8.1E23 (CLOUD)
Cybereason	malicious.58d9e5	**Sophos**	Mal/Generic-S
Cylance	Unsafe	**Symantec**	Downloader.Ratankba
Cyren	W32/Trojan.RWAG-7913	**Tencent**	Win32.Trojan-downloader.Agent.Dwtk
DrWeb	Trojan.MulDrop6.62805	**TrendMicro**	TROJ_RATANKBA.A
Emsisoft	Gen:Variant.Zusy.210214 (B)	**TrendMicro-HouseCall**	TROJ_RATANKBA.A
Endgame	malicious (high confidence)	**VBA32**	suspected of Trojan.Downloader.gen.s
ESET-NOD32	a variant of Win32/TrojanDownloader.NukeSped.B	**VIPRE**	Trojan.Win32.Generic!BT
F-Secure	Gen:Variant.Zusy.210214	**Webroot**	W32.Trojan.Gen
Fortinet	W32/Generic.AC.39AB6D!tr	**Yandex**	Trojan.Agent!AWHbj0rN0pw
GData	Gen:Variant.Zusy.210214	**Zillya**	Downloader.Agent.Win32.322085
Ikarus	Trojan-Downloader.Win32.Agent	**ZoneAlarm**	HEUR:Trojan.Win32.Generic
Jiangmin	Trojan.Generic.askzk		

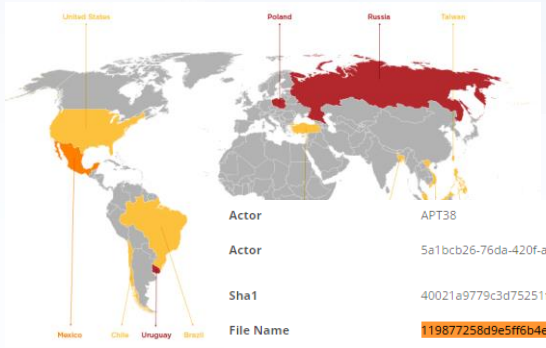
악성코드 샘플 테스트의 한계

다섯 번째 이유 : 공격자가 누구였는지를 모른다면 재공격을 당할 수 있습니다

Once a Target, Always a Target

Region	2017	2018
Americas	44%	63%
EMEA	47%	57%
APAC	91%	78%
Global	56%	64%

119877258d9e5ff6b4e1a70a3c8f3692



Actor	APT38
Actor	5a1bcb26-76da-420f-ad17-cfdbaa3d2f1b
Sha1	40021a9779c3d75251fe50c833b917d5a73c9d01
File Name	119877258d9e5ff6b4e1a70a3c8f3692.virus
Identifier	Attacker
File Size	128512
Fuzzy Hash	3072:b4N6zXn2iTGCoYrIvhOaR8X3dfE8VQKMVZJl:b4N6zXmCoZOaR8X3ZoKM7JI
Packer	Microsoft Visual C++ 8,VC8 -> Microsoft Corporation,Microsoft Visual C++ 8,
Sha256	52de4a4a2bdc7dc5c64bb5b6032df6ffd37c512c694993c337d6913eab316d78
Type	fileType
Md5	119877258d9e5ff6b4e1a70a3c8f3692

Endpoint Detection & Response

앞으로 고민해 봐야 할 평가 방식

EDR의 목표는 무엇일까

EDR(Endpoint Detection and Response)의 핵심은 탐지와 대응

안정성 테스트 평가

- 다양한 OS에 대한 융합
- 기 도입된 엔드포인트 솔루션과의 적절한 융합
- 지원 조직에 대한 평가

기능 테스트 평가

- 공격 그룹이 사용하는 공격 프레임워크 채택
- 탐지 : 단순 악성여부가 아닌 무엇을/어떻게 탐지했는가에 대한 정보 제공
- 대응 : 대응을 위한 분석기술 및 방법, 이를 통한 영향도 판단 가능 여부

EDR 평가 방법 : 안정성 테스트

안정성에 대한 지원이 잘 되는지가 중요한 평가 요소 중 하나임

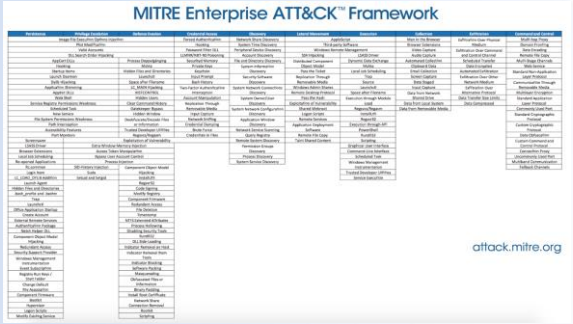
• **지원 조직의 전문성**	• 엔드포인트 솔루션 경험의 국내 사용자 대상 운영 경험 여부
• **제품 호환성 테스트**	• 다양한 운영체제와의 충돌 • 국내 보안 모듈과의 충돌에 대한 사전 QA검증 • 각 기업의 엔드포인트 환경에 대한 사전 검증
• **지원 콜센터 체계**	• 지원 서비스의 형태, 전화/이메일/포털
• **전문 교육 지원**	• 엔드포인트 솔루션 구축, 운영 교육 • 침해사고 대응에 대한 기술 교육
• **벤더사의 국내지사 여부**	• 해외벤더 제품의 경우 국내 지사가 존재하는지 여부

EDR 평가 방법 : 공격 프레임워크 채택

실제 공격 그룹이 사용하는 기법을 수행할 수 있는 공격 프레임워크를 사용하자

MITRE | ATT&CK™

metasploit



중요한 건 대응/분석을 할 수 있는 내용이 포함되어 있는지
전체 호스트 대상 감염 범위가 어느 정도인지

EDR 평가 방법 : 탐지 기능 테스트

부족한 탐지 정보의 단편적인 대응이 아닌 실질적인 대응을 할 수 있는 내용이 포함된 탐지

어떠한 방식으로 탐지를 했는지, 탐지 시 풍부한 정보를 제공하는지

EDR의 기본 요소 중 하나가 이상 행위에 대한 IOC 탐지 룰임

IOC 탐지 룰 출처가 단순 시그니쳐 집합인지 실제 침해사고 경험이 밑바탕이 된 인텔리전스 기반인지 구분하는 것은 상당히 중요합니다. 단순 시그니쳐는 단편적인 정보만을 제공하기에 누가 왜 어떤 공격을 시도했는지 알기가 어렵습니다.

탐지한 이벤트를 가지고 공격 단계를 알 수 있는지

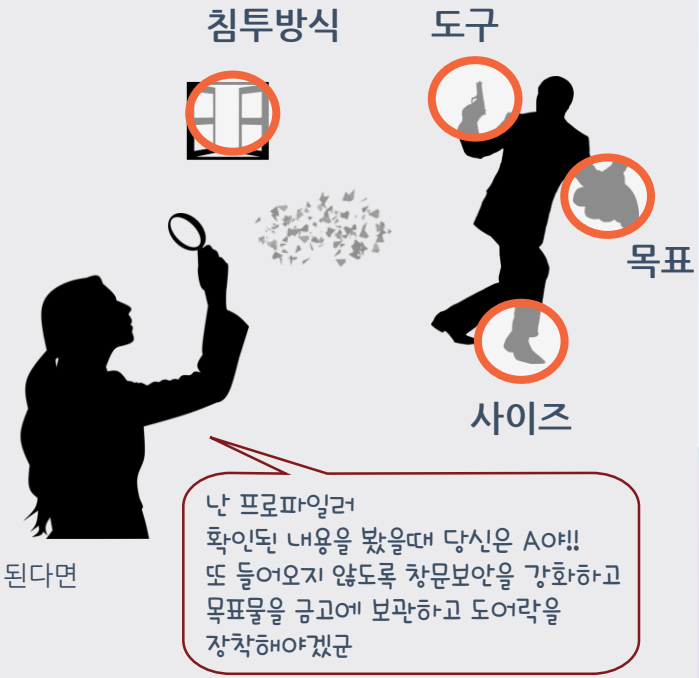
APT와 같은 고 위험성 공격은 치밀하게 여러 단계로 수행이 됩니다.

탐지 내용이 초기침투인지 확산공격인지가 판단할 수 있다는 건 상당히 중요합니다.

이에 따라 대응의 관점이 달라질 수 있기 때문입니다.

탐지 내용을 기반으로 공격 시나리오를 재생산 할 수 있는지

공격자가 어떤 기법을 통해 어느 깊이까지 침투를 하였는지 전반적인 공격 시나리오가 확인이 된다면 예상되는 2차, 3차 시나리오에 대한 접근을 할 수 있어 향후 공격에 대한 대응이 가능합니다.



EDR 평가 방법 : 대응 기능 테스트

상세한 분석을 통해 얻어진 정보는 대응의 속도를 빠르게 해줌

호스트 분석에 대한 상세 분석이 가능한지

OS에서 제공되는 RAW데이터는 분석에 상당한 이점을 줍니다. 탐지된 내용을 기반으로

RAW데이터 기반의 타임라인 분석이 가능한지에 따라 정확하고 빠른 대응을 할 수 있습니다.

전사 피해 범위에 대한 확인이 가능한지

얼마나 많은 호스트가 감염이 되어있는지 인지할 수 있는 건 상당히 중요합니다.

눈에 띄지 않은 호스트가 상당한 피해로 퍼질수 있습니다.

확산을 막을 수 있는지

EDR영역에서의 직접적인 대응은 호스트 격리입니다. 호스트를 직접 컨트롤을 하게 되면

무결성이 손상되기 때문입니다.

EDR 평가 방법 : 공격 프레임워크에 기반한 평가(예)

APT 공격 단계 중 권한 상승 (Eventvwr을 통한 권한 상승 예시)

공격 예시

1. 레지스트리 수정

[HKEY_CURRENT_USER]₩Software₩Classes₩mscfile₩shell₩open₩command

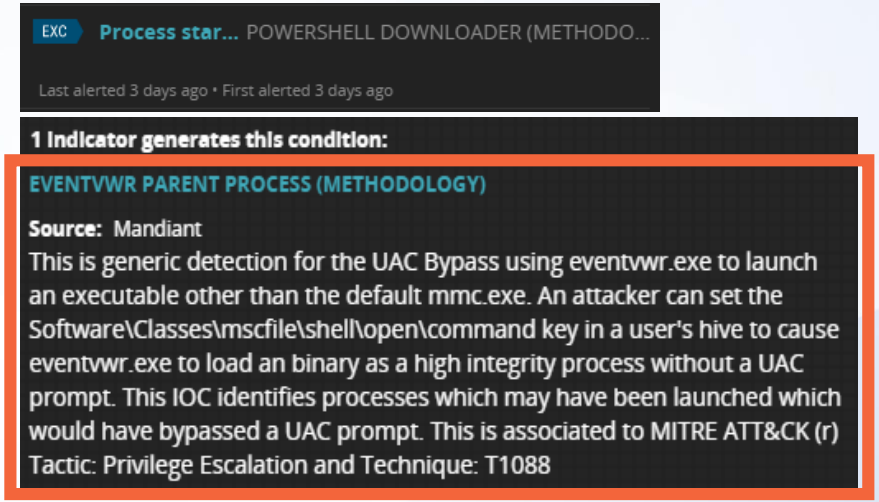
Value : C:₩Windows₩System32₩svch0st.exe

2. eventvwr.exe 실행

svch0st.exe가 SYSTEM 권한으로 수행됨

탐지 예시

권한 상승 공격 기법이며 Mitre Attack T1088에서 사용된 기법임을 알 수 있음



FIREEYE™

감사합니다