

Portfolio

Vol. 28



INTERVIEW.

주 일 현

요약

개발하는 것을 좋아하고 클라우드 보안 엔지니어를 목표로 성장해 나가는 **주일현**입니다.

1. About Me

Introduction.

- 머리속에 떠오르는 걸 SW로 만드는 것을 좋아합니다.
- 1년 6개월 정도 군에서 IDC를 관리해 봤습니다.
- 새로 배운 것이 완전히 이해가 갈 때까지 끈질기게 찾아봅니다.
- 취미로 악성코드 분석과 AV Evasion 기법을 찾아보곤 합니다.

E-mail / Channel

Email : orca_eaa5a@naver.com / dlfuswn@gmail.com

Github : <https://github.com/orca-eaa5a>

Notion

<https://www.notion.so/8ffe439bc34a4b1eb64fbe763dd931c4?v=7b0fb032161248b588479f1b61881784>

2. Tech

Language

C/C++, Python, Javascript, Powershell, Bash Shell

Tech Stack

- Django, Django ORM, ExpressJS
- VueJS, CSS, JQuery
- MySQL, Docker, AWS Lambda, EC2, ALB, API Gateway ..
- AWS Cloudformation

Special Tech

Reverse Engineering, Incidence Response

3. Education & License

Education

- 세종대학교 정보보호학과 학사 (16. 3 ~ 20. 2)
- KITRI Best of the Best (19. 6 ~ 20. 3)
- 사이버작전사령부 Splunk 운영자 교육 (21. 12. 6 ~ 10)
- 사이버 전문인력 교육과정 (22. 2 ~ 22. 4)

License

- 정보보안기사 (20. 12)
- AWS SAA-C03 (22. 12)

4. Prize / Contest

Prize

- KITRI 정보보안 최고인재 [과기부장관/1000만원]) (20. 4)
- 세종대 창의SW설계 경진대회 [우수상] (19. 5)
- 세종대 창업 경진대회 [우수상] (19. 5)

Contest

- KETI Mobius IoT 경진대회 [본선] (18. 12)
- 국방부 화이트햇 콘테스트 [본선 7등] (21. 11) - 1인팀 참가
- 국정원 사이버공격방어대회 [본선 5등] (22. 10)
- 국방부 화이트햇 콘테스트 [본선 4등] (22. 11)

5. Personal Experience & Project

Project

- Go 1.16 분석용 IDA Plugin - 당시 최초 공개
- x86 악성코드 분석용 python 기반 에뮬레이터
- Stream 환경에서 Youtube 동영상 구간 추출 서비스
- 특전사 전투력관리체계 개발

Experience

- 방첩사(기무사) 사이버보안기관평가 우수부대 [국방부장관 표창]
- 육군 사이버전문인력 선발

Portfolio Contents

Directing / Editing / Design 주일현

전격!

셀프 자기소개

즉문즉답, 너를 말해줘!

능력치 공개! 너의 Tech는?

On-Prem IDC 관리 경험

프로젝트

MP4 Stream T

Stream되는 동영상의 일부

Mac Defenc

Windows Defender가 M

트 이야기

Trim

만을 추출할 수 없을까?

der

ac에서도 돌아간다고?

경험과 배움

커뮤니케이션의 중요성!

★ ★ ★의 지시와 비전공자와의 협업

첫 대외활동과 성과

KITRI BoB 이야기

대회 이야기

첫 CTF 출전 부터 아쉬움까지

직문즉답

너를 말해줘!

1

Q. 성별과 생년월일이 어떻게 되시나요?

A. 남자, 96년생입니다.

2

Q. 전공이 무엇인가요

A. 정보보안 전공했습니다.

3

Q. 개발하는 것을 좋아 하시나요?

A. 예. 특히 자동화를 하거나, 남들이 안 해본 것을 시도 하는 것을 선호합니다.

4

Q. 어떤 프로젝트들을 해보셨나요?

A. 토이 프로젝트 위주로만 해 봤습니다. Windows Defender를 Mac에서 동작하게 하기, AWS 기반으로 용량이 큰 유튜브 동영상 일부를 빠르게 추출하기 등 분야를 가리지 않고 해보고 싶은 것 같습니다.

5

Q. 수상경력이 있으신가요?

A. KITRI BOB 최고인재
(20년, 과기부장관 / 부상 1000만원)

기타 교내 수상으로 세종대 SW 경진대회, 창업경진대회 등 정도입니다.

6

Q. 경진대회 같은 것도 나가신 적이 있으신가요?

1	정조대왕	3252
2	Newtella	2252
3	NOOP	2252
4	아니다싶으면밥먹으러감	2252

A. - 국방 White Hat Contest
(21년, 본선 7등 [일인팀 참가])
- 국정원 사이버공격방어대회
(22년, 본선 5등)
- 국방 White Hat Contest
(22년, 본선 4등)

군대에서만 대회를 나갔었는데, 22년에 상을 못 탄 게 참 아쉽습니다.

7

Q. 3년을 군에 계셨는데
군에서 무엇을 하셨나요?

A. 참 이것저것 한 것 같습니다.
1년차 때는 서버를 관리하다
높은 경쟁률을 뚫고 사이버
전문인력으로 선발되었습니다.



2년차 부터 Blue Team, 서버
취약점 관리, 정보보호장비
운영 등의 임무를 수행했습
니다.

8

Q. 직접 운영한 장비는 어떤 것
들이 있나요?

A. 비밀이라 자세히 말씀드릴 순
없지만 이중화 된 서버와
서버를 구성하는 네트워크
L2~L4 네트워크 장비들,
그리고 서버의 정보보호장비
인 NAC, FW/IPS, WAF 마지막
으로 통합로그 분석 시
Splunk를 사용했습니다.
네트워크 장비는 직접 만지
지는 않았습니다.

9

Q. 개발이 하시고 싶은 건가요?
보안이 하시고 싶은 건가요?

A. 학생때는 막연히 침해사고
대응 전문가가 되고 싶다
생각했습니다. 다만, 군에서
관리자로서 일을 하다 보니
조직에 기여도가 큰 일을 하고 싶다는
생각을 했습니다. 그래서 비전,
조직에서의 중요도, 성장
가능성, 제가 그 동안
공부했던 것과 서버 운영 경험
등을 잘 살릴 수 있는게
무엇이 있을까 생각하다
클라우드 보안을 생각하게
되었습니다. 제가 좋아하는
개발도 하면 좋겠지만, 일단
우선순위는 보안에 있는 것
같습니다.

10

Q. 목표로 하시는 일이 있나요?

- A. 일단 목표로 하는 것은 세가지
입니다.
1. 조직에 기여하는 일을 하자
 2. 성장하면서 만들고 싶은 것이
있을 때 만들 수 있는 능력을
구비하자
 3. 하고자 하는 일에 전문성을
갖추자

— Fin. —





Github

<https://github.com/orca-eea5a>

Notion

<https://www.notion.so/8ffe439bc34a4b1eb64fbe763dd931c4?v=7b0fb032161248b588479f1b61881784>

Github **Star**에는
Facebook 좋아요
에 없는, 뿌듯함이 있다.

능력치 공개!

너의 Tech는?

Stacks



Languages

c/c++	★★★★
python	★★★★
javascript	★★★

Licenses

정보보안기사
AWS SAA-C03

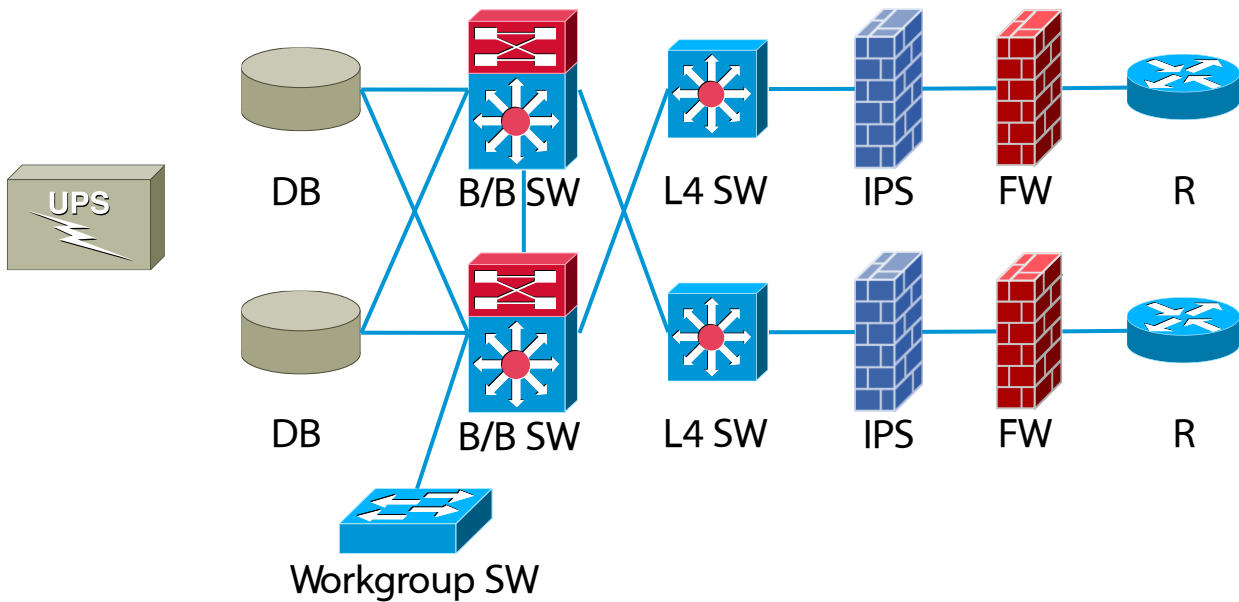


[잘하는 것]

문제해결	★★★★★
자료검색/활용	★★★★
커뮤니케이션	★★★★

[성장이 필요한 것]

실 프로젝트 경험	★
협업 경험	★★
서비스 운영 경험	★



작은 인프라를 관리 해보며..

작은 IDC를 1년 6개월 정도 관리를 해본 경험은 정말 값진 경험이었습니다.

단순히 책으로만 공부했던 네트워크를 실제로 운영해보고 장애조치도 해보면서, 단순히 "IT에서 네트워크는 기본이지"라는 생각으로 공부했던 지식이

정말로 유용하다는 것을 체감했습니다.

또한 서버관리자와 개발자가 따로 분리 되어있고, 서버에 대한 인수인계가 제대로 되지 않았을 때, 서버 관리자가 서버 관리하기 정말 엄청나게 어렵다는 것을 처음 알았습니다.

거대한 서비스는 아니지만 실제 서버/네트워크장비/정보보호장비를 운영했습니다.

인프라 관리를 주로 했고, 주로 했던 것은 장애 복구였습니다. 서버에 장애가 난 적은 거의 없었고 대부분은 네트워크 장애에 대한 조치였습니다.

서버관리자다 보니 네트워크 장비를 직접적으로 만지지는 않았고, 장애가 발생하면 구간 별로 제가 1차적으로 확인한 다음에 네트워크 담당자에게 장애 예상지점을 확인해 보라고 하거나 네트워크 구성을 바꾸라고 지시하는 정도까지 관리를 했습니다.

물론 서버에 장애가 발생한 적도 있습니다. 서버 IPfilter 방화벽을 잘못 설정해 또 다른 Active 서버와의 동기화가 계속해서 실패하면서 갑자기 Active 서버 두 개 모두 죽어 버리더군요. 그땐 정말 식은땀이 줄줄 났습니다.

다행히 인프라 모니터링 시스템을 통해 동기화가 필요한 데이터베이스 컨테이너만 재구동 해주면 되는 것을 파악했고 데이터베이스 서비스를 재시작하니 장애조치가 가능했습니다.

데이터가 지워지는 등의 장애가 아니라 장애 시간동안 가용성 문제만 발생했기 때문에 큰 사건은 아니었습니다. 나름 값지지만 다시는 하고싶지 않은 경험이었습니다.

About The Project



Windows Defender
Advanced Threat Protection

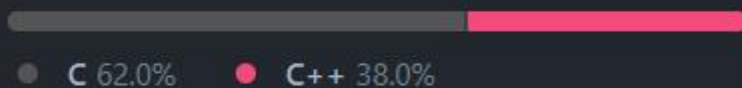
프로젝트 이야기

Packages

No packages published

[Publish your first package](#)

Languages



Windows Defender를 hooking하여
악성코드가 백신에 탐지되는 부분을
확인할 수 있는 프로젝트이다.
중국사람들 star가 많다.

Stream 환경에서 MP4의 일부 구간만 추출 할 수 있을까?

개발 난이도 : ★ ★ ★ ★ 종류 : Web Service (FE/BE)

프로젝트 기간 : 1.25개월

Git : <https://github.com/orca-eaa5a/yt-downloader>

이 프로젝트는 스트리밍 환경에서 길이가 긴 Youtube 동영상 일부를 빠른 시간 내에 추출하는 것을 목적으로 합니다. 10시간짜리 동영상이라도 1분 내에 원하는 부분을 추출할 수 있게 개발했습니다.

B/E는 AWS Lambda 기반으로 개발했습니다. F/E는 Vue를 사용하여 개발했고, AWS S3를 통해 서비스를 하게끔 했습니다. 배포는 AWS Cloud Formation을 사용하여 관리할 수 있게 했습니다.

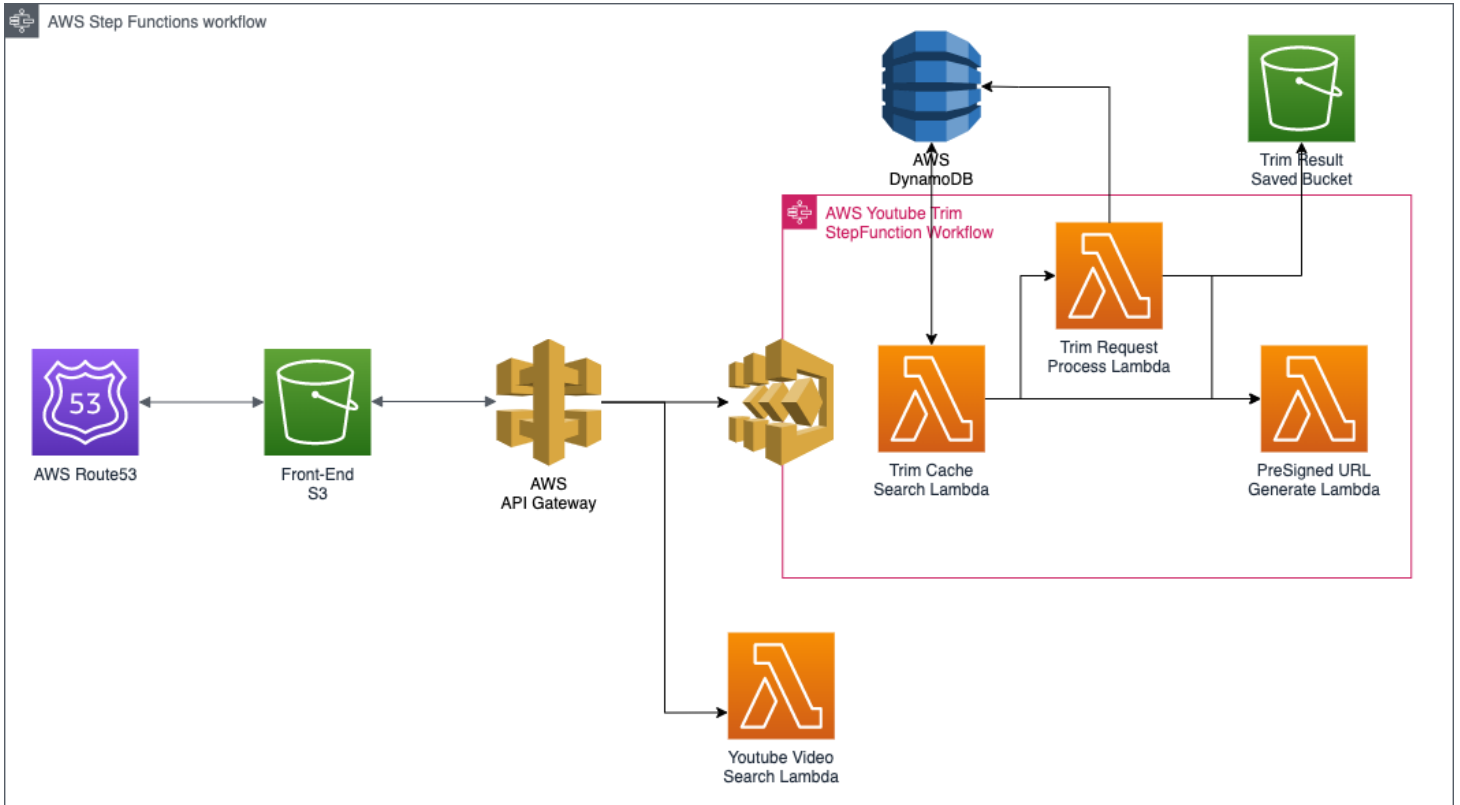
Youtube 동영상의 일부를 어떻게 추출할지 가장 많이 고민했습니다.

2~10시간 짜리 동영상은 용량이 2~15G정도 되는데, 이 큰 용량의 동영상에서 실제로 필요한 부분은 2~8분 정도라 단순히 전체 동영상을 다운로드 받아 필요한 구간을 추출하는 방법은 굉장히 비효율적이었습니다.

이 프로젝트의 핵심 기술은 다음 두 가지 입니다.

1. HTTP Range Request
2. MP4 코덱의 재생 원리

실제 Youtube 동영상이 저장되는 Cloud에서 HTTP Range Request를 지원하는 것은 쉽게 직접 확인할 수 있었습니다.



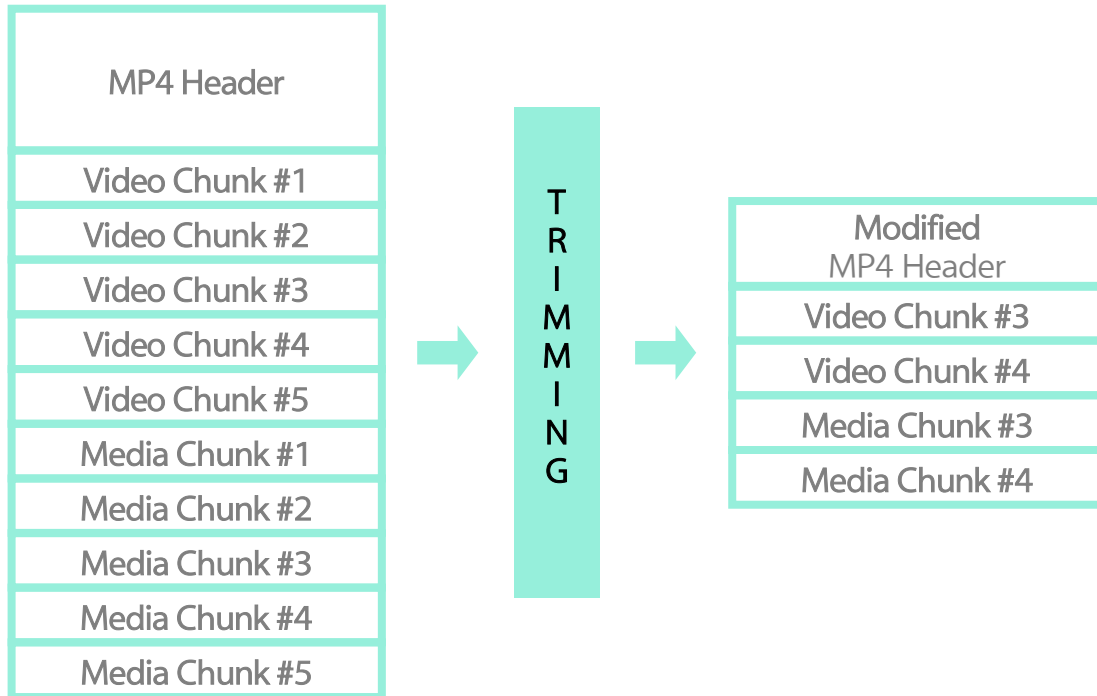
다만, HTTP Range Request로 받아온 동영상의 일부를 새로운 동영상으로 만들 수 있는지 여부는 선행 연구나 라이브러리를 찾을 수 없었기 때문에 직접 확인하고 또, 만들어야 했습니다.

“스트리밍 환경에서 초기 대기 시간 감소를 위한 MPEG-4 파일 포맷 분석”이라는 논문을 통해 아이디어가 구현 가능하겠다고 생각해 PoC 코드를 제작했습니다.

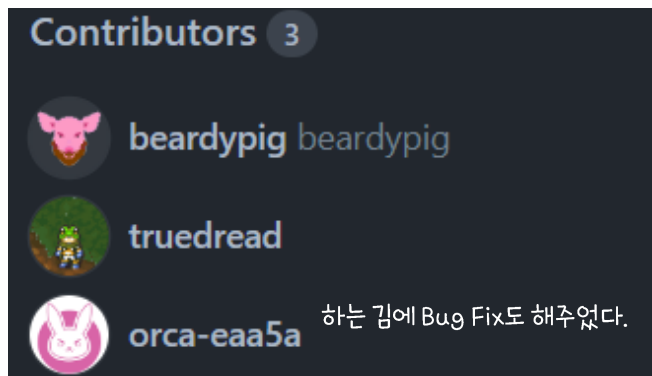
pymp4라는 오픈소스를 기반으로 PoC 코드를 제작했습니다. 아마 이 부분이 이 프로젝트에 있어 가장 도전적인 부분이지 않나 싶습니다. 기존에 있던 문제가 아닌 새로운 문제를 해결 했어야 하니까요.

아이디어의 핵심은 MP4에서 추출하고자 하는 Chunk에 맞게 MP4 Header를 재구성 하는 것이었습니다.

—Cont.—



pymp4를 이용한 PoC는 성공적으로 동작했습니다. 다만, 이 라이브러리가 기반으로 하는 construct 라이브러리가 너무 느리다는 문제가 있었습니다.



따라서 1차적으로 바닐라 파이썬으로 구현하고, 성능이 안나오면 c/c++로 다시 만들기로 했습니다.

mp4analyser라는 코드를 참고해서 만들었으며, 기존 코드에서 지원하지 않는 기능은 추가적으로 구현했습니다.

코드는 잘 동작했고 PoC보다 20배 정도 빠르게 동작함을 확인했습니다.

서비스의 핵심 기능을 구현했으니 이제 다른 사용자를 위한 서비스를 만들고자 했고, 이에 웹 서비스로 방향을 잡았습니다.

웹 서비스 개발 간 제일 많이 고려한 사항은 다음과 같습니다.

1. 어떻게 Lambda 함수의 비용을 가장 아낄 수 있을까
2. 30초 이상 걸리는 작업의 API Gateway Time out 해결하기

Lambda 함수 비용 절감을 위해 아래와 같은 방법을 사용했습니다.

1. 추출 결과를 DB에 저장하고 동일 요청에 대해서는 DB에 저장된 S3 Key 응답
2. 요청 받은 비디오의 용량에 따라 적절한 Lambda 함수 호출을 위해 AWS Step Function을 이용하여 Workflow를 설계/구현하였습니다.

Step Function과 Lambda 호출을 위해 AWS API Gateway를 사용했습니다.

Step Function을 동기적으로 사용할 경우 작업 시간이 1분이 넘어가면, API Gateway의 30초 Timeout 제한으로 사용자가 응답값을 못 받는 경우가 생겼습니다.

따라서 StepFunction은 비동기적으로 호출하고, 작업에 대한 ID를 사용자에게 응답하는 방식으로 구조를 변경하였습니다.

그리고 사용자단에서 작업ID를 가지고 작업의 진행 상황을 체크하는 Lambda 함수를 일정 주기마다 호출하게끔 하였습니다.

배포 관리를 위해 AWS 리소스들을 Cloudformation Template으로 정리하였습니다.

TODO

이 프로젝트는 아래와 같은 작업을 추가적으로 할 것입니다

1. Cloudwatch/Event Bridge를 통한 버그 모니터링 기능 구현
2. 다운로드 추천 시스템 구현

—Fin.—

OSX에서 WIN DEFENDER

실행시키기

개발 난이도 : ★ ★ ★ ★ 종류 : OSX Executable

프로젝트 기간 : 2.5개월

Git : <https://github.com/orca-eaa5a/mac-defender>

Mac Defender는 OSX에서 Windows Defender를 실행 가능하게 하는 프로그램입니다.

구글의 보안 연구원인 Tavis Ormadny의 loadlibrary를 참고하여 만들었으며, 기존 코드가 Linux OS에 종속적이고, x86 OS에서만 동작한다는 한계점이 있었습니다. 이에 x64 OSX에서 동작하는 프로그램을 만들어 보고자 했습니다.

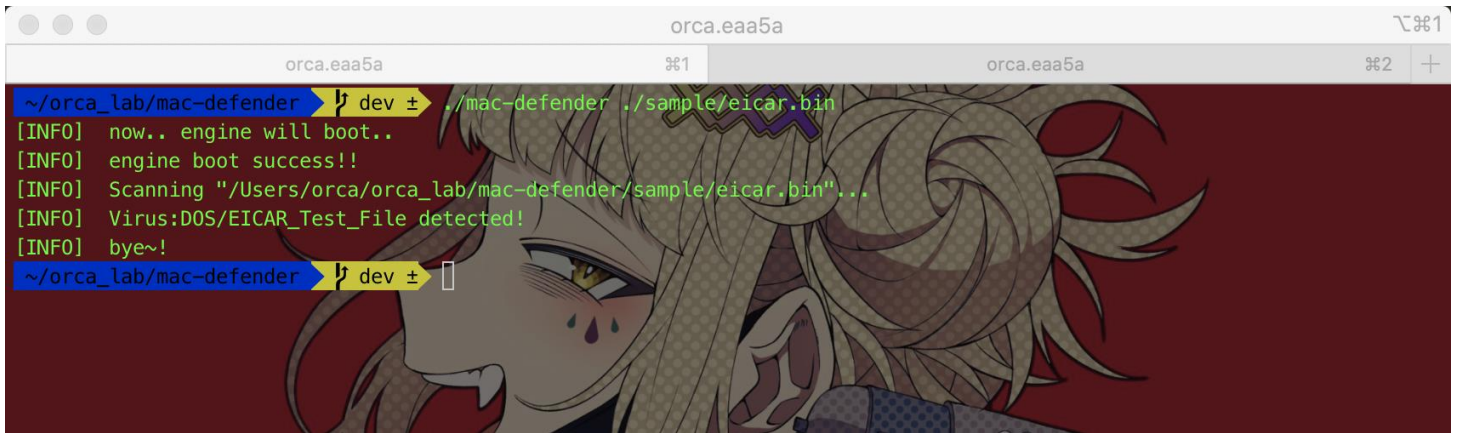
처음에는 Linux OS에 종속적인 ABI Call과 Win-Defender 내부적으로 사용하는 구조체의 자료형만 x64로 포팅하면 될 것 같다 생각했고 가볍게 시작했습니다.

“There is a difference between knowing the path and walking the path” – 매트릭스(1999)

하지만 Win-Defender 내부적으로 사용하는 구조체와 WinAPI가 버전에 따라 달라지는 것을 리버스 엔지니어링한 결과 알았습니다. 이에 어쩔 수 없이 Win-Defender 버전에 종속성을 가져야 했습니다.

PE를 다른 OS 위에서 실행시키기 위해서는 Windows에 대한 종속성을 제거해 주어야 합니다.

일반적인 방법은 다음과 같은 것들이 있습니다.



```
~ /orca_lab/mac-defender ➤ dev ± ./mac-defender ./sample/eicar.bin
[INFO] now.. engine will boot..
[INFO] engine boot success!!
[INFO] Scanning "/Users/orca/orca_lab/mac-defender/sample/eicar.bin"...
[INFO] Virus:DOS/EICAR_Test_File detected!
[INFO] bye~!
~ /orca_lab/mac-defender ➤ dev ±
```

1. VM과 같은 하이퍼바이저 사용
2. WINE 같은 에뮬레이터 사용

이 프로젝트는 직접 WinAPI를 개발하며, IAT Hooking을 통해 PE 실행간 직접 개발한 WinAPI를 호출하게 하는 일반적이지 않은 방법을 사용했습니다.

WinAPI 개발은 기존 코드를 참고하여 개발하였으나, 동작하지 않거나 기존에 없는 API역시 존재했습니다. 이러한 API는 WINE, ReactOS 소스코드를 참고하여 직접 만들었습니다.

Windows Subsystem에 종속성이 클 수록 세부적으로 구현했습니다. 최종적으로 기존 Tavis가 구현하지 않았던 x64 SEH 역시 구현하는데

성공하였습니다.

어디까지 에뮬레이팅(구현)할 것인지 판단하는 것이 어려웠던 부분입니다. 정확한 기준이 없기 때문에 아래 순서를 반복하면서 구현했습니다.

1. Microsoft Docs로 API가 어떤 기능을 하는지 확인
2. React OS 코드를 기반으로 최대한 Sub-Routine 호출 제거
3. 정상적으로 에뮬레이터가 동작하는지 동적 디버깅

—Cont.—

특징

이 프로젝트는 아래와 같은 특징을 가지고 있습니다.

1. 최초로 Mac에서 동작하는 Win-Defender 개발
2. X86용 코드를 x64까지 확장

한계점

이 프로젝트는 아래와 같은 한계점을 가지고 있습니다.

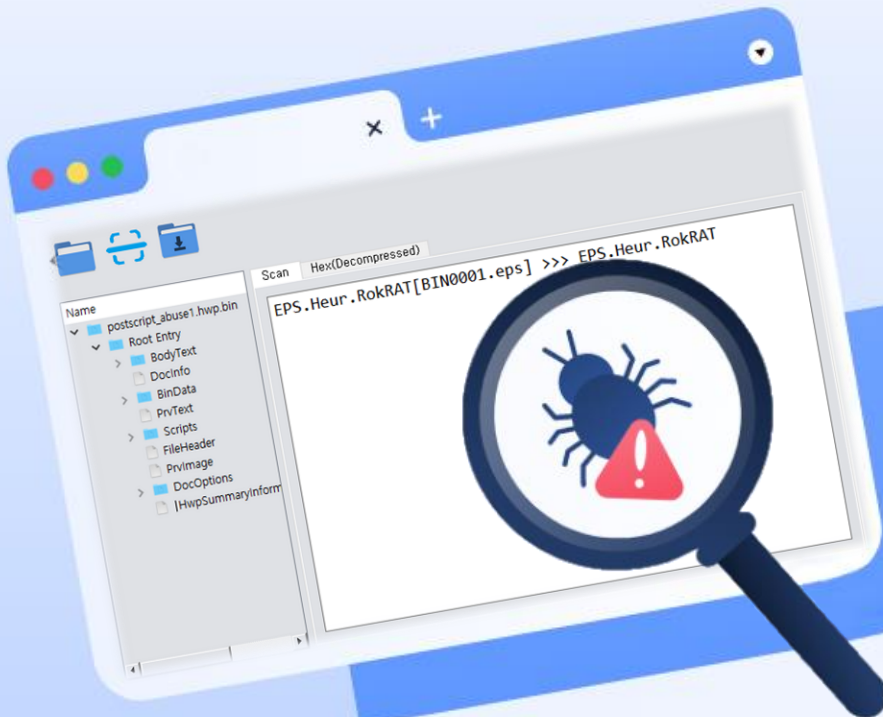
1. 구 버전 Win-Defender에 종속
 - 최신버전 동작을 위해선 WinAPI 추가 개발 필요
2. SEH 처리간 일부 경우 오류 발생
 - github issue #1 참고
 - 오류가 발생하는 원인은 파악되지 않음

— Fin. —

HWPSCAN2가 유료화 되었다구요?

DokEbin Scanner를

사용해 보세요!



https://github.com/orca-eaa5a/dokkaebi_scanner

※ 패턴 업데이트는 가끔 생각날 때 이루어집니다.

커뮤니케이션의 중요성!

★ ★ ★의 지시와 무왕좌왕 개발

군에서 있었던 일입니다. 사령관님이 웹 서비스를 만들고 싶다고 하셨고 그 일이 개발할 능력이 있는 사람이 없다고 저에게 떨어 졌습니다.

군인들의 훈련을 체계적으로 관리하는 목적이었기 때문에 해당 업무를 담당하는 군인들과 협업을 하게 되었습니다. 실제 웹서비스를 사용하고 운용할 사람들이었기 때문에 그 분들에게 기능 요구사항을 알려 달라고 했습니다.

그 분들은 이런저런 기능이 필요하다 알려줬습니다. 물론 구체적이지 않게 말입니다. 가장 기억에 남는 것은 스키마와 연관이 있는 기능을 API까지 만들어 놓고 테이블 스키마를 통째로 바꿨던 것입니다.

저는 누군가의 지시를 받고 개발 한 경험이 거의 없었고 더욱이 그 누군가가 비전공자인 적은 더더욱 없었습니다.

그 분들은 이 정도면 충분히 알려줬다 생각 했을 태고, 저는 소통 없이 "일반적으로 이렇게 하니까 이게 맞겠지?"하고 개발했습니다. 나중에 와서야 "어 뭐야 이렇게 안 했어?"하는 상황을 직접 경험하니 협업에 있어 소통이 얼마나 중요한지 잘 알 수 있었습니다.

물론 저는 협업 자체도 많이 안 해봤기 때문에 실제 필드에서 소통이 어떤 식으로 이루어지는지 잘 알지 못합니다. 하지만 위와 같은 경험을 해서 의사소통의 중요성을 알고 있고, 이에 대한 경험치를 쌓아 가야겠다는 중요성 역시 알고 있기 때문에 그 과정이 힘겹지 않을 거라 생각합니다.

첫 대외활동과 성과

KITRI BoB 이야기

저는 대학생때 대외활동을 하지 않고, 그냥 혼자서 관심있는 분야를 공부하는 것을 좋아했습니다. 하지만 군대가기 전에 뭐하나 해보고 싶은 마음에 BoB를 지원했습니다.

BoB에서 크게 기술적으로 성장하기 보다는 시야가 많이 넓어졌습니다. 과목별로 파편화되어 있던 지식들이 실제 업무에 활용되는 것을 보면서, 내가 지금 공부하는 지식이 어디에 쓰일지를 생각해보게 되는 능력을 가지게 되었습니다. 또한 보안이라는 분야를 단순히 기술적인 것으로 바라보지 않게 되었습니다.

재밌어서 열심히 했고, 그에 따라 첫 대외 활동에서 수상도 했습니다. 제가 이 분야에서 어느 정도 위치에 있고, 많은 사람들을 만났던 좋은 경험이었습니니다.





