

포트폴리오를 날려먹은 내가

십덕 화이트 해커 및 악성코드 분석
가로 자리잡은

방법 & 노하우



목차

간단한 자기 소개 및 깃허브 및 노션 소개

깃허브 및 노션을 해오면서 얻은 간단한 노하우?

제가 하고 있는 분야 및 했었던 분야 소개

시행 착오, 고민, 좌절 및 그 순간 이겨낼 수 있었던 노하우

포트폴리오

제가 만들었던 포트폴리오와 노하우, 논문, 특허, 개발 작업 등등

마지막 - 후배들에게 하고 싶은 말 / 조언

프로젝트 개요와 목표를 작성해 주세요

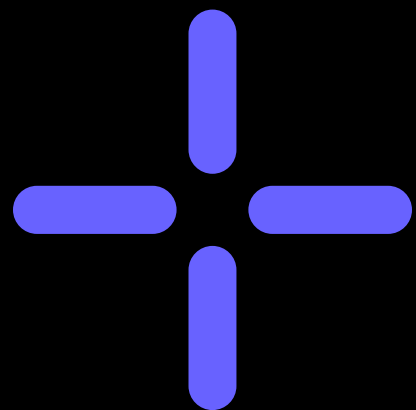


INFO

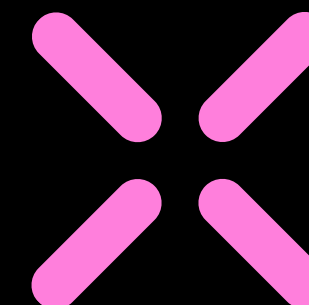
간단한 소개



이름	정준영
닉네임	KaztoRay
깃허브	KaztoRay
전화번호	010-2167-7246
인스타	KaztoRay
메일	dsph9245@naver.com
주분야	모의해킹, 악성코드 분석, 인공지능 보안 등



해왔던 분야 소개



모의해킹

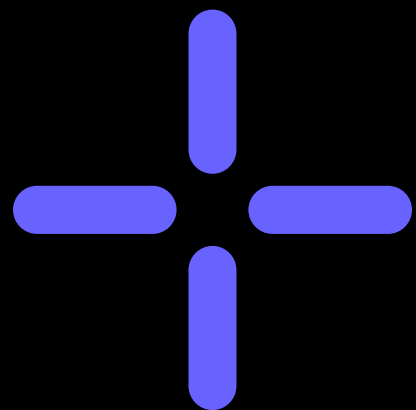
인공지능

게임 개발

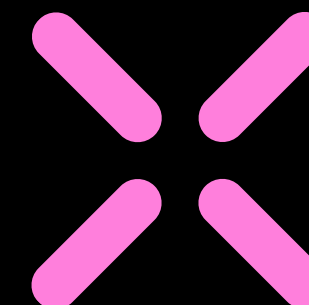
웹 개발

모바일 앱 개발

클라우드 연구 (서버
관리)



현재 하고 있는 분야 소개



모의해킹



악성코드 분석



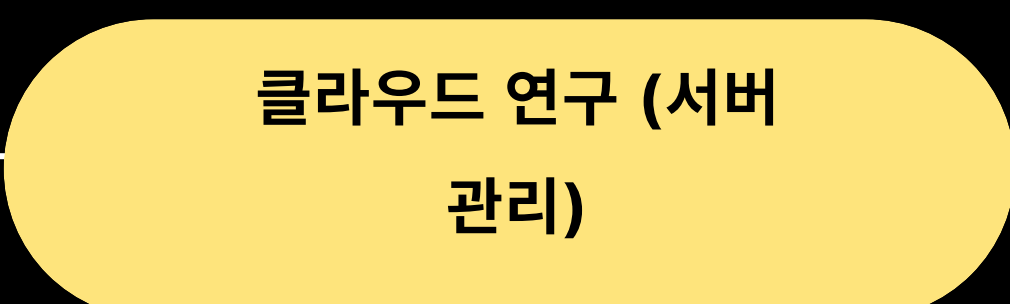
인공지능 보안



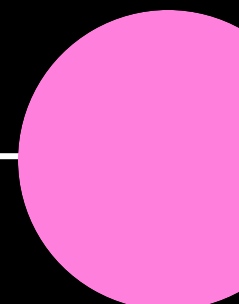
웹 개발 및 보안



보안 컨설팅



클라우드 연구 (서버
관리)



notion 소개 (최고의 포트폴리오2)

Reserved Area

- Reserved Area는 총 32개의 섹터로 구성되며, Boot Sector, FSINFO, Boot Strap이라는 구성 요소를 가진다.
 - 각 구성 요소는 원본과 백업으로 나뉘며, 아래와 같은 위치에 존재한다.
 - Boot Sector : 0번 섹터 (원본), 6번 섹터 (백업)
 - FSINFO : 1번 섹터 (원본), 7번 섹터 (백업)
 - Boot Strap : 2번 섹터 (원본), 8번 섹터 (백업)
 - Reserved Sector : 나머지 섹터들에 해당하며, 일반적으로 비어 있음
 - 그 중에서도 디지털 포렌식적으로 주요한 데이터들은 Boot Sector에 위치한다.
 - HxD를 관리자 권한으로 실행하여 논리 디스크를 선택하면 볼륨 데이터를 직접 확인할 수 있다.

- 아래 사진은 Boot Sector의 구조이다.

Offset(h)	00	01	02	03	04	05	06	07	08	09	0A	0B	0C	0D	0E	0F	Decoded text
00000000	EB	58	90	4D	53	44	4F	53	35	2E	30	00	02	08	DE	12	ëX.MSDOS5.0...p.
00000010	02	00	00	00	00	F8	00	00	3F	00	FF	00	00	08	00	00ø...?.ÿ.....
00000020	00	C0	DA	00	91	36	00	00	00	00	00	00	02	00	00	00	.AÜ.'6.....
00000030	01	00	06	00	00	00	00	00	00	00	00	00	00	00	00	00
00000040	80	00	29	80	E9	1E	0E	4E	4F	20	4E	41	4D	45	20	20	€.)ëë..NO NAME
00000050	20	20	46	41	54	33	32	20	20	20	33	C9	8E	D1	BC	F4	FAT32 3E2N%0
00000060	7B	8E	C1	8E	D9	8D	00	7C	88	56	40	88	4E	02	8A	56	{ZAZ0%. `vø`N.Sv
00000070	40	84	41	88	AA	55	CD	13	72	10	81	F8	55	AA	75	0A	@`A»#UÏ..r..üü*u.
00000080	F6	C1	01	74	05	FE	46	02	EB	2D	8A	56	40	B4	08	CD	öA..t..bF..ë..Svø".I
00000090	13	73	05	89	FF	FF	8A	F1	66	0F	B6	C6	40	66	0F	B6	.s.'ÿÿSñf..5øøf..9
000000A0	D1	80	E2	3F	F7	E2	86	CD	C0	ED	06	41	66	0F	B7	C9	Nëã?>ã!IAi..Af..É
000000B0	66	F7	E1	66	89	46	F8	83	7E	16	00	75	39	83	7E	2A	f:äfføf~..u9f~*
000000C0	00	77	33	66	88	46	1C	66	83	C0	CC	0B	00	80	89	01	.w3f<F..ffa..»..€¹.
000000D0	00	E8	2C	00	E9	A8	03	A1	F8	7D	80	C4	7C	88	F0	AC	..ë..ë".{ø}€Ä <ð~
000000E0	84	C0	74	17	3C	FF	74	09	B4	0E	BB	07	00	CD	10	EB	„Ät.<ÿt..`»...I..ë
000000F0	EE	A1	FA	7D	EB	E4	A1	7D	80	EB	DF	98	CD	16	CD	19	I{ü}ëä)€ë8`I..I.
00000100	66	60	80	7E	02	00	0F	84	20	00	66	6A	00	66	50	06	f`€~..»...fj..fP.
00000110	53	66	68	10	00	01	00	84	42	8A	56	40	8B	F4	CD	13	Sfh....`BSvø<öI.
00000120	66	58	66	58	66	58	66	58	EB	33	66	30	46	F8	72	03	fXfXfXfXø3f;Før.
00000130	F9	EB	2A	66	33	D2	66	0F	B7	4E	18	66	F7	F1	FE	C2	üø*f30f..N..f:ñpÄ
00000140	8A	CA	66	8B	D0	66	C1	EA	10	F7	76	1A	86	D6	8A	56	SÉf<øfAø..v..I0SV
00000150	40	8A	E8	C0	E4	06	0A	CC	B8	01	02	C0	13	66	61	0F	@SeAä..I...I..fa.
00000160	82	74	FF	81	C3	00	02	66	40	49	75	94	C3	42	4F	4F	..tÿ..Ä..f@Iu`A800
00000170	54	4D	47	52	20	20	20	20	00	00	00	00	00	00	00	00	TMGR
00000180	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
00000190	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
000001A0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	0A	44	69.....Di
000001B0	73	68	20	65	72	72	6F	72	FF	00	0A	50	72	65	73	73	sk errorÿ..Press
000001C0	20	61	6E	79	20	68	65	79	20	74	6F	20	72	65	73	74	any key to rest
000001D0	61	72	74	00	0A	00	00	00	00	00	00	00	00	00	00	00	art.....
000001E0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
000001F0	00	00	00	00	00	00	00	AC	01	B9	01	00	00	55	AA	~¹...U#

FAT32 Boot Sector 구조

이름	오프셋	설명
Jump Command	0x0 - 0x2	부트 코드로 점프
BPB(Bios Parameter Block)	0x3 - 0x5A	볼륨의 전반적인 설정을 포함
부트 코드	0x5B - 0x1FD	볼륨 부트 코드
시그니처	0x1FE - 0x1FF	고정값 0x55 0xAA

- BPB (Bios Parameter Block) 영역 구조를 자세히 살펴보면 아래와 같다.

Offset(h)	00	01	02	03	04	05	06	07	08	09	0A	0B	0C	0D	0E	0F	Decoded text
00000000	EB	58	90	4D	53	44	4F	53	35	2E	30	00	02	08	DE	12	ëX.MSDOS5.0...p.
00000010	02	00	00	00	00	F8	00	00	3F	00	FF	00	00	08	00	00ø...?.ÿ.....

자동차 보안 등장 배경

자동차 보안 등장 배경

- 배경 : 하드웨어를 중심으로 발전하던 자동차 → 내부 소프트웨어의 중요성 증가
 - 5G, 6G 기술과 함께 무선 인터넷 망과 클라우드를 통해 자동차는 데이터를 교환한다.
 - Example) OTA (무선 소프트웨어 업데이트), 주행 데이터 OEM 서버 저장, 자율 주행

- 자동차에는 스마트폰과 같이, 개인 정보와 운영 소프트웨어를 저장하게 되었다.

자동차 해킹 사례와 모의해킹

- 해킹 이슈는 회사에 큰 타격이 가해진다. → 뉴스에 퍼뜨리지 않고 회사측과 비밀리에 협상을 진행 (뉴스에 없는 이유)

사이버 보안 국제 기준

- 2022년 7월 이후 개발에 들어가는 모든 자동차에는 UNECE에서 제정한 R155, R156의 기준을 따라 사이버 보안 인증을 받아야 자동차 판매를 가능하게 하였다.
 - 155 : CSMS : Cyber Security Management System
 - 156 : SUMS : Software Update Management System
 - 사이버 보안 국제 정책 및 프로세스 표준은 ISO 21434에 정의되어 있다.

사이버 보안 인증을 받기 위한 주요 테스트

- 모의 해킹
- Key Management : 암호화 알고리즘에 사용되는 Key는 안전하게 관리되어야 한다.
- Fuzzing Test & Pentetration Test (침투테스트)
- TARA (Threat Analysis and Risk Assessment) : 자동차 사이버보안 위험 평가. 제품 수명 주기

자동차 보안 기능

대표적인 사이버 보안

- Software Download
 - 특정 세션 및 Secure Level에서 다운로드 → Secure Access
 - 업데이트 하고자 하는 어플리케이션 보안
 - 업데이트 후, 소프트웨어 인증

충전 프로토콜

- 자동차 ↔ 충전소 (사용자 인증서 교환)

통신 암호화

- 통신 데이터 유출 시, 방지하기 위한 통신 암호화
- 승인된 사용자의 데이터만을 받기 위한 사용자 인증 후 통신.

Smart Contract 취약점 - Arithmetic Issues

- Arithmetic Issues의 경우, Integer Overflow, Integer Underflow를 생각하면 된다.

- Smart Contract에서는 Unsigned가 물론 존재하지만, 많은 개발자들의 편의를 위해 int형을 많이 사용하곤 한다.
 - 만약, Overflow가 발생한다면, 이는 거의 돈을 탈취하는 공격이나 DOS 공격으로 이어질 수 있는 심각한 공격 벡터로 사용된다.

예시 코드 1

```
function withdraw(uint _amount) {
    require(balances[msg.sender] - _amount > 0);
    msg.sender.transfer(_amount);
    balances[msg.sender] -= _amount;
}
```

- 위 코드에서는 돈을 송금하는 withdraw() 함수가 구현되어 있는데, 돈을 전송하기 전에 balances[msg.sender] - _amount가 0보다 큰 값인지 우선 확인한다.
 - 이 때, Integer Underflow를 막아 검사하지 않기 때문에, 엄청난 양의 돈을 빼내는 것이 가능하 다.

예시 코드 2

```
function popArrayOfThings() {
    require(arrayOfThings.length >= 0);
    arrayOfThings.length--;
}
```

- 해당 함수의 경우, require문에 오류가 존재한다.
 - 만약, arrayOfThings.length == 0인 상황에 popArrayOfThings() 함수를 호출한다면, require문을 통과하고 1을 감소시키면서 arrayOfThings.length가 -1이 되고 Off By One 취약점으로 이어질 수 있다.

예시 코드 3

```
function votes(uint postId, uint upvote, uint downvotes) {
    if (upvote - downvote < 0) {
        deletePost(postId)
    }
}
```

- 여기서 핵심은 Unsigned와 Signed의 연산 결과는 Unsigned라는 것이다.



Portfolio?

포트폴리오 어떻게 준비하셨나요?

논문

1학년 때부터 인공지능 보안 논문으로 정보보호학회 호남지부 추계 학술대회 참가, 4학년 때 대한전자공학회 하계 학술대회 참가 (DBPIA 올라갔습니다.)

특허

4학년 때 정명희 교수님의 도움으로 특허 5개 출원, 거의 다 보안에 관련된 내용으로, 그 내용 덕분에 대학원 면접 때 좋은 이미지를 보여서 홍익대, 동국대, 건국대학교 대학원에 합격해 지금은 건국대학교 일반대학원 보안 학과 재학 중

개발 및 포트폴리오

보안 부분에서 1학년 때부터 논문을 작성하고, 2학년 때 국가에서 주관하는 버그바운티 토론회에 참여하여 동아일보 기사에 이름 및 사진이 올라감. 3학년 때 포트폴리오를 잃었으나 (깃허브 날아감), 4학년 때 논문 및 특허로 이를 다시 만들어 냈음....

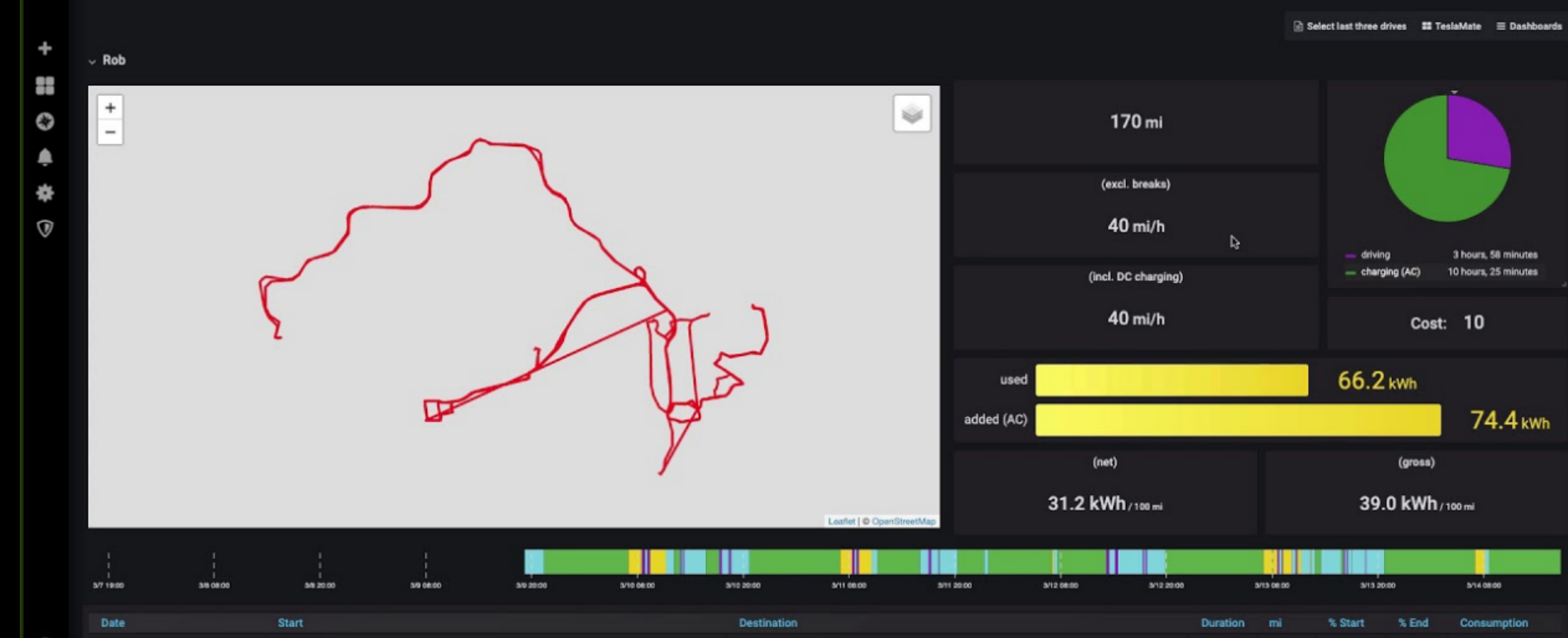
PORTFOLIO

대표적인 작업물 소개

```
> telnet localhost 9000
Trying 127.0.0.1...
Connected to localhost.
Escape character is '^]'.
YT]]^Connection closed by foreign host.
```

```
~
> █
```

```
untitled4 x
/Users/jeongjun-yeong/CLionProjects/untitled4/cmake-bu
hell^
Process finished with exit code 0
```



000001F0	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00000200	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00000210	08 83 11 00 60 00 00 00 00 00 00 00 00 00 00 00	.f.....
00000220	00 00 00 00 00 00 00 00 55 50 58 30 00 00 00 00UPX0..
00000230	00 B0 0B 00 00 10 00 00 00 00 00 00 00 04 00 00	.°.....
00000240	00 00 00 00 00 00 00 00 00 00 00 00 80 00 00 E0€..à
00000250	55 50 58 31 00 00 00 00 00 C0 07 00 00 C0 0B 00	UPX1.....À...À..
00000260	00 BA 07 00 00 04 00 00 00 00 00 00 00 00 00 00	.°.....

Offset (h)	00	01	02	03	04	05	06	07	08	09	0A	0B	0C	0D	0E	0F	Decoded text
000001B0	F0	BF	13	00	90	06	00	00	00	80	13	00	F0	3F	00	00	δ¿.....€..δ?..
000001C0	00	50	12	00	40	62	00	00	00	00	00	00	00	00	00	00	.P..@b.....
000001D0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
000001E0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
000001F0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00

보안 & 인공지능과 관련된 프로젝트들

통신 중 텍스트를 암호화 시키고 복호화 시키는 솔루션, 인공지능을 이
용한 전력 사용 및 그래프 솔루션, 마지막으로 제 주 연구분야인 파일 시
그니처 즉, 파일 내부 시스템에 대한 연구를 주로 포트폴리오로 해서 작
성을 했습니다.

VISION OF THE FUTURE

미래에 대한 비전? 및 해주고 싶은 말

현재의 비전

아마 여러분들은 현재 실력에 대해서 고민이 많고, 분야에 대해서도 고민이 많으실 것입니다. 저도 그랬었고, 저도 지금도 이 자료를 만들 때도 좌절을 했습니다. 수없이 좌절을 해도 하나만 생각한다면 이겨낼 수 있습니다. 내가 온 길을 생각하면 이겨낼 수 있고, 정 이겨내기 힘들다면 주변 친구들의 도움을 받으세요 그렇게 현재의 비전을 만들어가고 그 꿈을 이루기 위해 노력하세요.

미래의 비전

미래에도 똑같은 좌절이 없을 것이라고 생각할 순 없습니다. 그러나 미래에는 조금이나마 실력이 늘었을 것이고, 자신이 왔던 분야가 있을 것입니다. 그럼 그 분야를 믿고 다시 배운다는 마음가짐으로 나아가면 부담을 줄일 수 있을 것입니다. 이것이 저의 방식이고 미래의 비전을 만들어가는 방식입니다.

CONNECT WITH US

언제든지 편하게 연락주세요 ~

Q & A

문의사항이 있으시면 아래로 연락주세요!

Email	dsph9245@naver.com
Phone	010-2167-7246
Instagram	KaztoRay