

실사례로 말해주는 게임 해킹 대응스토리

v.1.0

강민수 / NHN

2019년 11월 15일



© 2019 NHN Corp.

ABOUT

이 름	강민수
입 사	2018년 12월
업 무	모바일 보호 솔루션 개발, 앱 보안 검수
이 메 일	ms.kang@nhn.com



CAREER

- BOB (대한민국 최고의 차세대 보안리더를 양성하는 「Best of the Best(BoB)」 프로그램)
2012/07/01 ~ 2013/12/14
- [수상] 정보보호 올림피아드 금상
2013
- [발표] 해킹캠프 발표(보호된 안드로이드 어플리케이션 분석방법 feat. 소녀전선)
2017/08
- [발표] 코드엔진 발표 (게임핵과 보안솔루션의 전쟁)
2018/07/07



목차

1. 소개

1.1 자기소개

2. 1부. 안드로이드 리퍼블릭

2.1 해킹 커뮤니티란?

2.2 해킹 커뮤니티의 대상

2.3 해킹 커뮤니티 결제 대상

2.4 해킹된 변조앱 분석

2.5 새로운 보호기법 추가

2.6 지속적인 모니터링

2.7 결론

3. 2부. 크리티컬 옵스 CBT

3.1 배경

3.2 전체 로그

3.3 변조 로그 분석

3.4 중간 결론

----- iOS -----

3.5 트윅

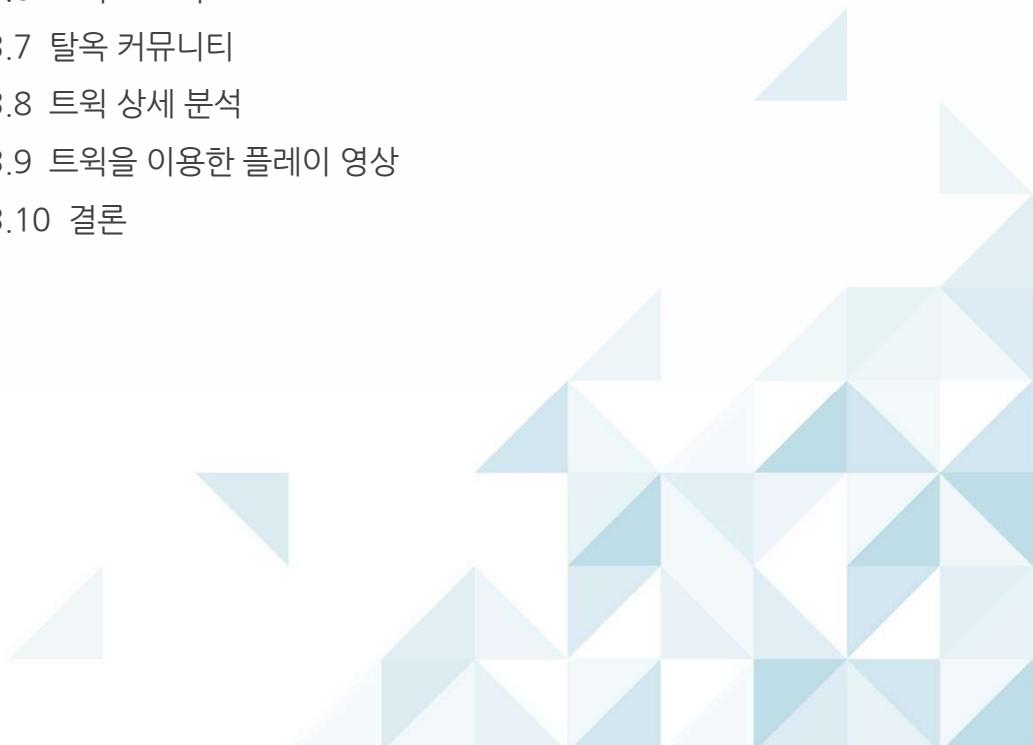
3.6 트윅 스토어

3.7 탈옥 커뮤니티

3.8 트윅 상세 분석

3.9 트윅을 이용한 플레이 영상

3.10 결론



게임핵을 공유하는 커뮤니티가 문제

- 커뮤니티마다 광고 수익, 결제, 취미 방향이 조금은 다른데
- (하지만 모두 VIP 결제는 유료)
- 커뮤니티에 공개될 경우에 빠르게 '핵' 사용자 급증

안드로이드 리퍼블릭 이 놈..

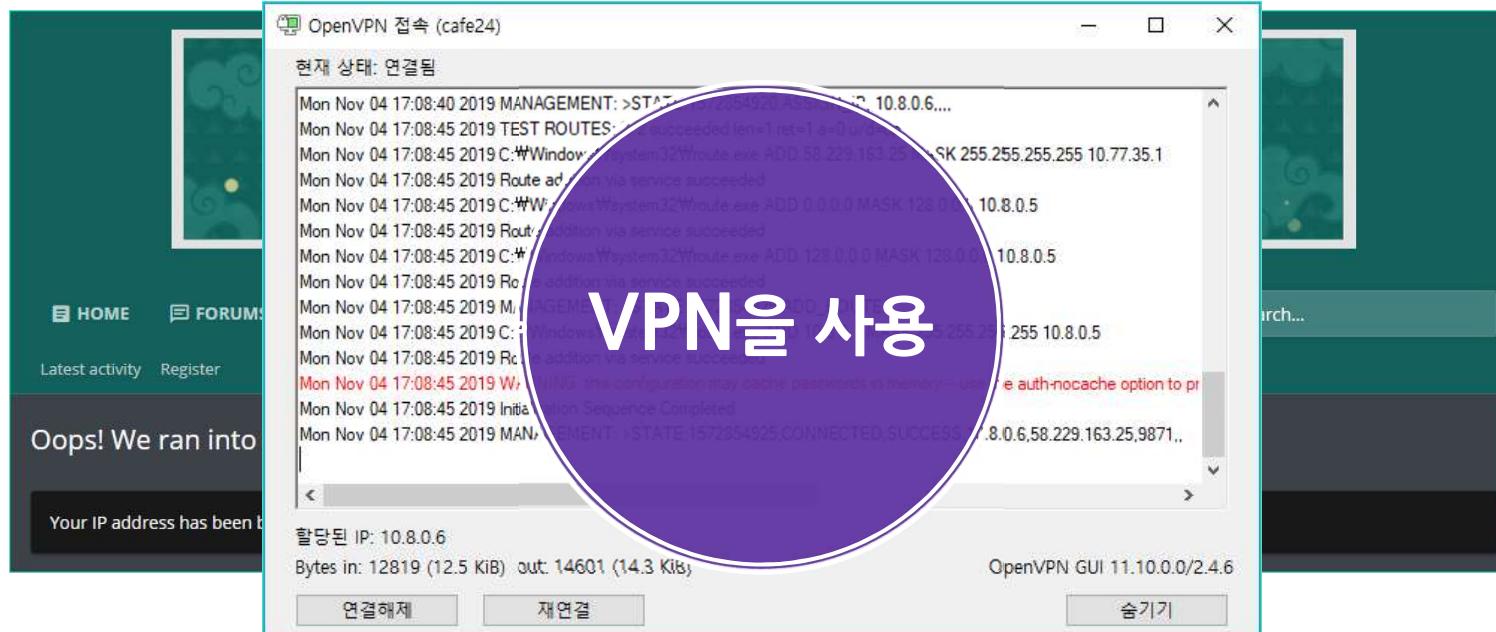


2-1. 해킹 커뮤니티란?

TOAST

안드로이드 리퍼블릭

- 게임회사야? 분석회사야? 너 컴퓨터 잘해? 그럼 사이트 접속 “안돼!”
- 게임회사의 IP는 접속 불가한 문제로 VPN은 필수..



2-2. 해킹 커뮤니티의 대상

TOAST

Greetings!

This is a list of all the games we have in our VIP section. They are sorted out in alphabetical order to hopefully make it easier to search what games you are looking for. All games are kept up to date, any game that gets added or removed will be updated on this thread.

VIP game list:

SPOILER: AVAILABLE GAMES

Age of Wushu Dynasty
Age of Wushu Dynasty (KR) / 구음진경
Arena of Valor: 5v5 Arena Game (EU)
Astral Chronicles
AVABEL LUPINUS
Avabel Online
Azur Lane
AxE: Alliance vs Empire
Battle of Souls
BEASTS VS MONSTERS - Idle RPG
Blade Knights HD - Another World
Blade Reborn - Forge Your Destiny
Blank City
BLEACH Mobile 3D
Boxing Star
Brave Cross
Brown Dust
Call of Duty®: Mobile - Garena
Call of Duty®: Mobile
Chain Strike
Clash of Knights
Chiến Hòn Mobile / Battle Of Soul (VN)
Crazy Dragon
Crusaders Quest
Kingdom Story: Brave Legion
KOF ALLSTAR
Kritika: The White Knights
TALION
League of Masters
Legend Hunter-Devil Unleashed
Light In Chaos: Sangoku Heroes
LINE BLEACH -PARADISE LOST-
LINE: GUNDAM WARS / 鋼彈大戦鬥
Lord of Dice
Lost Kingdom-末日終戦



2-2. 해킹 커뮤니티의 대상

TOAST

핵과의 전쟁을 했던 게임 [크루세이더 쿼스트, 킹덤스토리]



킹스TV 구독자 3,96천명

뉴스 | 동영상 | 재생목록 | 커뮤니티 | 채널 | 정보 | Q

[킹덤스토리] 킴릭 뉴스 (feat. 덫글 이벤트) #킹덤스토리 #킹...
조회수 1,166회 • 9주 전
미묘와 지성의 새 MC 광가령 TV :
<https://www.youtube.com/channel/UCHct...>
새 MC가 여러분과 친해지고 살고 게임도 배우고 싶다고 다음 주
필요한 저녁!! 개인 방송을 한다고 하네요!! 구독과 좋아요 부탁드
려요~

새 MC 등장 & 광가령' 3행시 댓글 이벤트!!
자세히 알아보기

킹덤후랜드 시즌1 ▶ 모두 재생

[Kingdom Story] 킹덤스토리 라이브 방송 [킹덤후랜드 1...]
킹스TV 조회수 3.1천회 • 스트리밍 시간: 4개월 전

[Kingdom Story] 킹덤스토리 라이브 방송 [킹덤후랜드 2...]
킹스TV 조회수 2.1천회 • 스트리밍 시간: 4개월 전

[Kingdom Story] 킹덤스토리 라이브 방송 [킹덤후랜드 3...]
킹스TV 조회수 2.1천회 • 스트리밍 시간: 4개월 전

[Kingdom Story] 킹덤스토리 라이브 방송 [킹덤후랜드 4...]
킹스TV 조회수 2.9천회 • 스트리밍 시간: 4개월 전

[Kingdom Story] 킹덤스토리 라이브 방송 [킹덤후랜드 5...]
킹스TV 조회수 2.2천회 • 스트리밍 시간: 3개월 전

Crusaders Quest

카페정보 | 나의활동 | 전체글보기 | 448,908개의 글 | 15개씩 | 공지 슬기기 | 편집 | 확장 | 카페 채팅

매니저: 류희 since 2014.09.18. 카페소개

나무2단계 | 84,666 명 | 조대하기 | ★ 즐겨찾는 업비 4,385명 | ☰ 게시판 구독수 67회 | ☆ 우리카페 수 413회

카페 가입하기 | 카페 채팅

제목	작성자	작성일	조회
[공지] 카페 유저분들을 위해 디스코드 방을 개설하였습니다. [10]	씨앗은행	2019.03.08.	3,178
[공지] [필독] 카페 공식 규정 (수정) [8]	류희	2018.04.16.	4,326
[공지] [공지] 카페 내 오픈 / 단독방 홍보글 금지 [6]	별꽃두유	2016.09.15.	3,866
[공지] [필독] 등급에 대한 설명 [37]	씨앗은행	2016.05.02.	1.3만
같은 게시판 확장	알티우스	11:52	34
같은 게시판 평소에 저희 안모아놓으면 [1]	다시시작해요	11:51	57

|-|

2-3. 해킹 커뮤니티 결제 과정



Receipt for your account upgrade at And
Android Republic - Android Game Mods <support@androidrepublic.org>
나에게 ▾
영어 ▾ 한국어 ▾ 메일 번역

Sager Technologies 님이 2019년 3월 27일에 진행한 구매에 대해 \$20.00 USD의 금액을 환불했습니다.

금액이 VISA x-0016(으)로 환불되었습니다. 명세서에 표시되면 몇 일 정도 걸릴 수 있습니다. 시간이 더 소요되는 경우 카드 발급기관에 직접 문의해 주세요.

환불 요약

거래 ID: 8RJ31827H0811183G	2019년 3월 27일 09:11:27 PDT
총 구매 금액	\$20.00 USD
환불된 금액	\$20.00 USD

환불 결제수단

Sager Technologies
Support@androidpublic.org

환불 대상 “빠른 환불”
민수 강
dladbru@gmail.com

3월 27일 (수) 오후 4:31 ☆ ↗ :

영어 번역 안함 ×



2-3. 해킹 커뮤니티 결제 과정



Jun 1, 2017 265

안녕하세요, AR 회원님들, 한국스텝입니다.
홈페이지의 개편으로 인해 간단한 질문답변을 먼저 작성하시고, 저의 인터뷰메세지를 받으신뒤 그것에 답변하시면 제가 승인처리를 하게되는방식으로 바뀌었습니다. 보다 빠른 진행을 위해 결제를하시고나서, 제가 인터뷰 메세지를 회원님께 보내기전에 미리 아래 제출사항을 읽어보시고, 저에게 제출사항을 업로드한 메세지를 주시면 승인처리가 훨씬 빨라질수있습니다.

제출사항은 타 vip회원님들도 이미 제출하셨던것으로, 악의적으로 사용되지않으며 거부하실시 거절처리하고 환불받으실수있습니다. 단 한번이라도 vip거절처리된 계정은 다시 vip에 신청하실수없습니다.

아래는 제출사항입니다. 회원님의 상황에맞게 제출을 해주시면됩니다.(메세지에서 사진을 업로드하시면됩니다). 또한 가급적이면 컴퓨터 모니터화면, 종이서류 등 모두 휴대폰 직접촬영사진으로 업로드해주시면 감사하겠습니다. 웃이 스캔이나 압축해서올린다던지 하지않으셔도됩니다.
@Mattdol

해당사항중 하나라도 제출이 불가능하신경우 인터뷰가 길어지거나, 또는 거절처리됩니다. 주의하셔서 빠르게 VIP로 승격하실수있기를 바랍니다.

- Interviewee께서 직장인이실경우
i. 주민번호 뒷자리를 가린 신분증 (운전면허증도 해당)
ii. 직장의 월급명세서 또는 재직증명서 또는 사원증 (3종 택1)
iii. 직장의 연금보험 관련서류
= 총 두개의 자료,* 직장의 이름과 성명, 주민번호 앞자리는 가리시면 안됩니다.

- Interviewee께서 학생이실경우
i. 주민번호 뒷자리를 가린 신분증 (운전면허증도 해당)
ii. 학생증
을 제출하시기바랍니다. 참고로 학생증 기간은 표기되어있어야하며, 이미지
= 총 두개의 자료,* 성명과 주민번호 앞자리는 가리시면 안됩니다.

- Interviewee께서 이미 퇴직하셨을경우
i. 주민번호 뒷자리를 가린 신분증 (운전면허증도 해당)
ii. 원천징수영수증 또는 고용보험 가입확인서 (2종 택1)을 제출해주십시오
= 총 두개의 자료,* 직장의 이름과 성명, 주민번호 앞자리는 가리시면 안됩니다.

퇴직의 경우 퇴직후 너무 오랜기간(6달이상)은 인정되지 않습니다.

무직의경우 승인처리가 어렵습니다.

마지막으로, 새벽 늦은시간에 결제하시고 승인처리가 언제되는지에대한
인터뷰는 수작업으로 처리되며 모든 AR 스텝들에게는 사이트활동외의
감사합니다.

Please select your preferred language, by pressing one of the listed languages:

- English
- Chinese
- French
- German
- Indonesian
- Italian
- Japanese
- Korean
- Malaysian
- Portuguese
- Russian
- Spanish
- Tagalog
- Thai
- Turkish
- Vietnamese



2-3. 해킹 커뮤니티 결제 과정

TOAST

퇴직의 경우 퇴직후 너무 오랜기간(6달이상)은 인정되지 않습니다.

무직의 경우 승인처리가 어렵습니다.

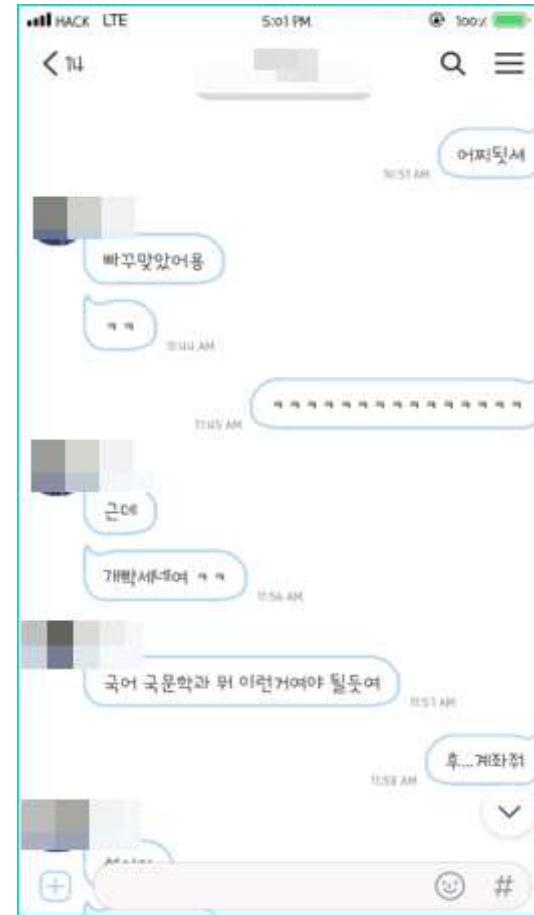
 gps19931999 New User  Oct 23, 2018  1	Oct 23, 2018 대출 알바생은 어떻게 하나요?.. 급여명세서 사원증 연금보험 이런것도 없는데.. 형.. 결제 완료한 후에 이걸 봐 버렸네..	#9
 dogdogdogdog New User  Jun 10, 2019  1	Jun 17, 2019 환불해주세요 결제하기 전에 저런 내용은 한번도 고지되지 않았는데. 너무 번거롭네요	
 jusal New User  Oct 7, 2018  5	Oct 7, 2018 이 정도면 은행 대출급 문서제출인데, 악의적으로 사용되지 않는다는 말로는 납득이 안가는 수준이네요. 어디에 사용되는지 꼭 설명이 필요합니다.	#7
 ★joseb18 VIP  Feb 28, 2015	Oct 22, 2018 간단하게 말해서 위에 서류들을 제출하는 까닭은. 안드로이드 리퍼블릭 사이트에 게임 회사 관계자들이 잠입하는것을 막기위한 보안상의 이유입니다. 새로하시는 VIP 회원님들 중에 착각하시는게 있는데, VIP는 특권이 아닙니다. 사이트를 운영하기위해 최소한의 비용만 받고 모드 업데이트를 관리하는 시스템이지. 한달에 2만원 남짓한 돈주면서 모드 찍어내라고 명령할수있는 그런게 아닙니다.	#8



2-3. 해킹 커뮤니티 결제 과정

TOAST

- SNS, 메신저, 통화
- 지인에게 대리 결제 요청
- 할 수 있는 모든 수단 진행



“
학생증으로 시도했으나 인증실패”



2-3. 해킹 커뮤니티 결제 과정



2-4. 해킹된 변조앱 분석

Forums > VIP Preview > VIP Game List

Not open for further replies.

Jun 2, 2017



Mod:
1.) Damage up to 6x using BGM slider (BGM OFF == original dmg)
2.) Defense up to 10x using SFX slider (SFX OFF == original defense)

Latest Modded Version: 2.43.3.KG
Playstore Link: Kingdom Story: Brave Legion - Apps on Google Play
VIP Download: <https://androidrepublic.org/downloads/kingdom-story-brave-legion.290/>

- 데미지 6배(배경음악 ON/OFF)
- 방어력 10배(효과 ON/OFF)

SPOILER: DESCRIPTION

Note:
- To login with google you must be rooted
- If you're VIP go to VIP Section to download

Interested in this mod as well as a great selection of exclusive releases?
----->[BUY VIP](#)<-----

Forums > VIP Preview > VIP Game List

Not open for further replies.

May 18, 2017



Mod:
1.) Player HP increase x5
2.) Enemy HP decrease x5

Latest Modded Version: 4.19.2.KG
Playstore Link: Crusaders Quest - Apps on Google Play
VIP Download: <https://androidrepublic.org/downloads/crusaders-quest.283/>

SPOILER: DESCRIPTION

Note:
- To login with google you must be rooted
- If you're VIP go to VIP Section to download

Interested in this mod as well as a great selection of exclusive releases?
----->[BUY VIP](#)<-----



2-4. 해킹된 변조앱 분석

TOAST

```
        ...
        v31 = -966630094;
        if ( v150 != 662252647 )
        {
            if ( v150 == 689227559 )
            {
                v125 = *(void (_fastcall **)(char *, _DWORD, _DWORD, _DWORD))(*(_DWORD *)dword_DD3362C4 + 336);
                v126 = lrand48();
                v125(&v238, 0, off_DD32D004[v126 % 5], 0);
                sub_DD0E96C8(v239); // verify?
                v31 = 1204037684;
                if ( *(_DWORD *)(*(_DWORD [5]{0xDD11C469,0xDD11F74D,0xDD1223AD,0xDD1257FD,0xDD127DB1})
                    v31 = -536078437;
            }
        else
        {
```

“ 보호 기법이 많이 적용되었음 ”



“ 변조된 실행화면 ”



2-4. 해킹된 변조앱 분석

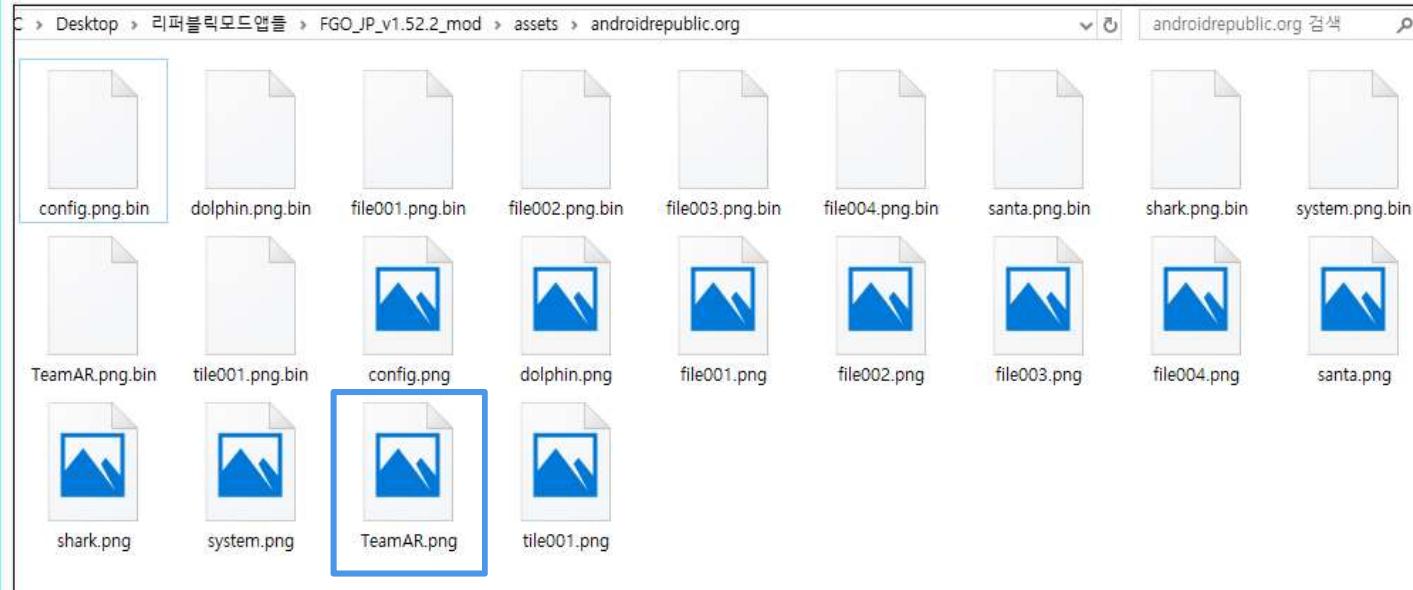
TOAST



〈Figure 0. GUI 복호화 프로그램〉

- [libandroidrepublic.so](#) 파일에서 암호화된 png파일들을 복호화하는 루틴을 분석해 동일한 동작을 하는 프로그램을 구현

“변조 앱이 언제 나타날지 모르니
바로 대응 할 수 있도록 최대한 자동화”



〈Figure 1. 복호화 된 png 파일들〉

- 최신 샘플 5건(mono,2cpp) 모두 잘 동작하며 해당 프로그램은 첨부파일로 올려두었음

2-4. 해킹된 변조앱 분석

```
C:\Users\HNEnt\Downloads\UPX-Visual-Studio-master\x64\Debug>upx --file-info C:\Users\HNEnt\Desktop\PicPick\iOS모의해킹\C_Quest_v4.1B.0.KG_mod_fixed\assets\androidrep
Ultimate Packer for executables
Copyright (C) 1996 - 2018
IPX 3.95w Markus Oberhumer, Laszlo Molnar & John Reiser Aug 26th 2018
Built with Visual Studio 2017 compiled by James34602 Build date: Sep 9 2019
C:\Users\HNEnt\Desktop\PicPick\iOS모의해킹\C_Quest_v4.1B.0.KG_mod_fixed\assets\androidrepublic.org\FILE\TeamAR.so [arm-linux.elf, linux/arm]
64d bytes, compressed by UPX 13, method 9, level 7, filter 0x00/0x00

C:\Users\HNEnt\Downloads\UPX-Visual-Studio-master\x64\Debug>upx -l C:\Users\HNEnt\Desktop\PicPick\iOS모의해킹\C_Quest_v4.1B.0.KG_mod_fixed\assets\androidrepublic.org
Ultimate Packer for executables
Copyright (C) 1996 - 2018
IPX 3.95w Markus Oberhumer, Laszlo Molnar & John Reiser Aug 26th 2018
Built with Visual Studio 2017 compiled by James34602 Build date: Sep 9 2019

File size      Ratio      Format      Name
792372 ->    516248   65.15%  linux/arm  C:\Users\HNEnt\Desktop\PicPick\iOS모의해킹\C_Quest_v4.1B.0.KG_mod_fixed\assets\androidrepublic.org\FILE\TeamAR.so

C:\Users\HNEnt\Downloads\UPX-Visual-Studio-master\x64\Debug>_



| Offset(h) | 00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F 10 | Decoded text          |
|-----------|----------------------------------------------------|-----------------------|
| 0002D9CE  | 65 72 73 69 6F 6E 00 2E 67 6E 75 2E 76 65 72 73 69 | ersion..gnu.versi     |
| 0002D9DF  | 6F 6E 5F 64 00 3F 67 6F 75 3F 76 65 72 73 69 6F 6E | on_d..gnu.version     |
| 0002D9F0  | 5F 72 00 2E                                        | _r..rel.dyn..rel.     |
| 0002DA01  | 70 6C 74 00                                        | 78 plt..text..ARM.ex  |
| 0002DA12  | 74 61 62 00                                        | 72 tab..ARM.exidx..r  |
| 0002DA23  | 6F 68 61 74                                        | 79 odata..fini_array  |
| 0002DA34  | 00 2E 64 61                                        | 79 ..data.rel.ro..dy  |
| 0002DA45  | 68 61 6D 69                                        | 00 namic..got..data.  |
| 0002DA56  | 2E 62 73 73                                        | 6F .bss..comment..no  |
| 0002DA67  | 74 68 2E 67 6E 75 2E 67 6F 6C 64 2D 76 65 72 73 69 | te..gnu.gold-versi    |
| 0002DA78  | 6F 6E 00 2E 41 52 4D 2E 61 74 72 69 62 75 74 65    | on..ARM.attribute     |
| 0002DA89  | 73 00 00 89 6D F6 F1 41 52 45 50 CC 03 0D 17 00 00 | s..tmd5[REDACTED].... |
| 0002DA9A  | 00 00 34 17 0C 00 34 17 0C 00 54 D5 02 00 38 B6 00 | ..4...4...IO..8%      |
| 0002DAA0  | 00 09 00 00 00 F8 7F 45 4C 46 01 A4 00 1F 03 00 28 | ..@ELF.E....(         |
| 0002DABC  | 00 61 1B BF 34 06 24 13 0C 6E 08 02 00 05 DD 1E 20 | .a_4.S..n....Y.       |
| 0002DADC  | 00 08 FE 36 1A 00 19 09 06 4D 87 07 00 01 23 09 91 | ..p6....M#....#..     |
| 0002DADE  | 00 0E 01 00 01 9E 00 07 08 FB 07 05 19 AC 10 3F ED | .0...ED...6....?i     |
| 0002DAEF  | B0 DA 1E B0 B3 EA 07 C4 B7 35 1E 54 49 00 DB 00 06 | 0U..*A 5.TI.0..       |
| 0002DB00  | 3F BE 02 0C A0 FC DD 2E A0 0C FC 07 18 01 00 BD    | ?4... QY...Q....4     |
| 0002DB11  | 06 00 A7 C7 34 01 69 07 C8 BC 00 B0 37 FD 51 E5 74 | ..\$C4.1.B4..79@t     |
| 0002DB22  | 64 00 AB 01 B2 06 BD EE FF 70 C0 61 CC BE 07 3C B0 | d.w...MyipAin4.<*     |
| 0002DB33  | 33 00 B6 7F 19 52 C1 3F 03 50 3E 50 35 D3 7F 08 78 | 3.I..RA?.P>P50..x     |
| 0002DB44  | 06 84 2F CF 41 6E F6 64 72 6F 69 DC BF 13 16 72 31 | ..IAm0droiUi..rl      |


| Offset(h) | 00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F 10                    | Decoded text                                                                   |
|-----------|-----------------------------------------------------------------------|--------------------------------------------------------------------------------|
| 00000F24  | E0 55 00 00 16 23 00 00 E4 55 00 00 16 24 00 00 E8                    | aU...\$.AU...\$.e                                                              |
| 00000F35  | 55 00 00 16 25 00 00 EC 55 00 00 16 26 00 00 F0 55                    | U...%..IU...%.8U                                                               |
| 00000F46  | 00 00 16 1                                                            | 3 55 00 .....8U....\$U.                                                        |
| 00000F57  | 00 16 1D 1                                                            | 5 00 00 ....8U...)....V..                                                      |
| 00000F68  | 16 2F 00 1                                                            | 3 00 16 ./...V...0...V...                                                      |
| 00000F79  | 32 00 00 0                                                            | 3 16 34 2...V...3...V...4                                                      |
| 00000F8A  | 00 00 14 1                                                            | 5 38 00 ...V...7...V...8.                                                      |
| 00000F9B  | 00 1C 56 1                                                            | 1 00 00 ..V...9.. V.....                                                       |
| 00000FAC  | 24 56 00 1                                                            | 3 00 2C \$V....;(V....+,                                                       |
| 00000FB3  | 56 00 00 1                                                            | V....,..0V....*,.4V                                                            |
| 00000FBD  | 00 00 16 31 00 00 38 56 00 00 16 36 00 00 D4 7B 78                    | ..1..BV...6..0ix                                                               |
| 00000FCE  | 00 00 16 31 00 00 38 56 00 00 16 36 00 00 D4 7B 78                    | 00000FDF 1F 55 50 58 21 04 04 0D 17 00 00 00 00 CC 4B 00 00 .DEX.....IK..      |
| 00000FDF  | 1F 55 50 58 21 04 04 0D 17 00 00 00 00 CC 4B 00 00 .DEX.....IK..      | 00000FF0 CC 4B 00 00 DC 0F 00 00 56 06 00 00 03 00 00 00 F9 IK..U...V.....6    |
| 00000FF0  | CC 4B 00 00 DC 0F 00 00 56 06 00 00 03 00 00 00 F9                    | 00001001 7F 45 4C 46 01 64 00 3F 03 00 28 00 61 0D DD 34 03 .ELF.d.?...(s.Y4.  |
| 00001001  | 7F 45 4C 46 01 64 00 3F 03 00 28 00 61 0D DD 34 03 .ELF.d.?...(s.Y4.  | 00001012 E4 B1 47 0A B7 05 0B 20 00 BB 08 1B 19 00 E4 18 00 @@G... .w...8..    |
| 00001012  | E4 B1 47 0A B7 05 0B 20 00 BB 08 1B 19 00 E4 18 00 @@G... .w...8..    | 00001023 06 16 03 1E 00 01 4F 04 00 27 03 7D 17 01 97 03 13 .....O.')...~.     |
| 00001023  | 06 16 03 1E 00 01 4F 04 00 27 03 7D 17 01 97 03 13 .....O.')...~.     | 00001034 93 00 B2 04 2A D8 00 4E 20 44 CE 03 05 FB 0C 10 1F ".,*0.N Df..6..    |
| 00001034  | 93 00 B2 04 2A D8 00 4E 20 44 CE 03 05 FB 0C 10 1F ".,*0.N Df..6..    | 00001045 36 13 36 54 03 79 1C 02 66 40 B0 06 1F 64 02 87 F0 6.6T.y..E@...d..#8 |
| 00001045  | 36 13 36 54 03 79 1C 02 66 40 B0 06 1F 64 02 87 F0 6.6T.y..E@...d..#8 | 00001056 00 67 03 06 B2 00 83 F6 48 01 03 SE 24 00 4D 87 1B .g...*.fCH..%Mt.   |
| 00001056  | 00 67 03 06 B2 00 83 F6 48 01 03 SE 24 00 4D 87 1B .g...*.fCH..%Mt.   | 00001067 51 F6 E5 74 69 00 00 00 E4 08 00 0D 32 70 DA 04 40 Qo@td...a..YzP06@  |
| 00001067  | 51 F6 E5 74 69 00 00 00 E4 08 00 0D 32 70 DA 04 40 Qo@td...a..YzP06@  | 00001078 04 C3 03 C9 38 01 B0 3F FF 2F 73 79 73 74 65 FE 6D .A.És..?/systembm  |
| 00001078  | 04 C3 03 C9 38 01 B0 3F FF 2F 73 79 73 74 65 FE 6D .A.És..?/systembm  | 00001089 2F 62 69 6E 2F 6C DE 03 6B 65 72 CE 17 14 C1 FB FF /bin/1D.kerI..Aqy  |
| 00001089  | 2F 62 69 6E 2F 6C DE 03 6B 65 72 CE 17 14 C1 FB FF /bin/1D.kerI..Aqy  | 0000109A 47 4E 55 00 8A 0A FC 17 FF DB 9F 74 58 C7 C0 26 AF GNU.S.ü.YÜtXÇA4    |
| 0000109A  | 47 4E 55 00 8A 0A FC 17 FF DB 9F 74 58 C7 C0 26 AF GNU.S.ü.YÜtXÇA4    |                                                                                |


```



2-4. 해킹된 변조앱 분석



- UPX는 실행 압축 유ти리티
 - 보호가 목적이 아님
(실행중에는 압축이 풀림)
 - 오픈 소스라 수정이 가능
 - 사용 가능한 플랫폼이 많음

UPX

위키백과, 우리 모두의 백과사전.

UPX(Ultimate Packer for eXecutables)는 여러 운영체제에서 수많은 파일 포맷을 지원하는 오픈 소스 실행 파일 압축 프로그램이다. GNU 일반 라이브러리를 통해 품가된 자유 소프트웨어이다. 압축, 압축 해제의 기능을 모두 담당한다.

목차 [숨기기]

- 1 압축
- 2 압축 해제
- 3 지원 포맷
- 4 각주
- 5 외부 링크

```
4776     for(int i = sz_dynsym / sizeof(Elf32_Sym); --i>0; ++sym) {
4777         unsigned syval = get_te32(&sym->st_value);
4778         unsigned sysec = get_te16(&sym->st_shndx);
4779         if (Elf32_Sym::SHN_UNDEF != sysec)
4780             && Elf32_Sym::SHN_LABS != sysec
4781             && xct_off <= syval)) {
4782                 set_te32(&sym->st_value, syval - asl_delta);
4783             }
4784
4785     }
4786
4787     /* write the file header */
4788     /* write the program headers */
4789     /* write the section headers */
4790     /* write the dynamic symbols */
4791     /* write the note entries */
4792     /* write the relocation entries */
4793
4794     /* write the file footer */
4795     /* write the program footer */
4796     /* write the section footer */
4797
4798     /* write the file size */
4799     /* write the program size */
4800     /* write the section size */
4801
4802     /* write the file offset */
4803     /* write the program offset */
4804     /* write the section offset */
4805
4806     /* write the file alignment */
4807     /* write the program alignment */
4808     /* write the section alignment */
4809
4810     /* write the file entry point */
4811     /* write the program entry point */
4812     /* write the section entry point */
4813
4814     /* write the file flags */
4815     /* write the program flags */
4816     /* write the section flags */
4817
4818     /* write the file version */
4819     /* write the program version */
4820     /* write the section version */
4821
4822     /* write the file flags */
4823     /* write the program flags */
4824     /* write the section flags */
4825
4826     if (fo) {
4827         fprintf(stderr, "Ix %x\n", sz_und, (get_te32(&phdr->p_filesz) - xct_off));
4828         xct_off -= (sz_und - (get_te32(&phdr->p_filesz) - xct_off));
4829         fi->seek(-(upx_int64_t)szb_info, SEEK_CUR);
4830     }
4831 }
```



2-4. 해킹된 변조앱 분석



```
C:\#Users#\[REDACTED] -d TeamAR.so
          Ultimate Packer for eXecutables
          Copyright (C) 1996 - 2018
JPX 3.95w      Markus Oberhumer, Laszlo Molnar & John Reiser   Aug 26th 2018
Built with Visual Studio 2017 compiled by James34602   Build date: Sep 16 2019

      File size       Ratio       Format       Name
-----  -----
2d554 2d5549027c 8fd44
> bd7d0 - 2d554 = 9027c (9027c)<
9027c 9027c2e0 2e06c0 6c0    792372 <-  516248   65.15%   linux/arm   TeamAR.so

Unpacked 1 file.

C:\#Users#\NHNEnt\Downloads\UPX-Visual-Studio-master\x64\Debug>
```

[AREP_Unpacker2.exe] -d [파킹된파일]



2-4. 해킹된 변조앱 분석

TOAST

```
public void UpdateMaxHPAura(); // RVA: 0xDEE3B8 Offset: 0xDEE3B8
public int get_HPEExtend(); // RVA: 0xDEC268 Offset: 0xDEC268
public void set_HPEExtend(int value); // RVA: 0xDEE5C0 Offset: 0xDEE5C0
public float get_BARRIER(); // RVA: 0xDEE5C8 Offset: 0xDEE5C8
public virtual float get_CurrentHp(); // RVA: 0xDEE764 Offset: 0xDEE764
public virtual void set_CurrentHp(float value); // RVA: 0xDEE830 Offset: 0xDEE830
public int get_CurrentHpInt(); // RVA: 0xDEEE9C Offset: 0xDEEE9C
public virtual float get_ActionRange(); // RVA: 0xDEF8C Offset: 0xDEF8C
public float GetStat(StatType statType); // RVA: 0xDEF000 Offset: 0xDEF000
public string get_UIHpBarPath(); // RVA: 0xDEF2D4 Offset: 0xDEF2D4
public float get_UIOverheadY(); // RVA: 0xDE9DB0 Offset: 0xDE9DB0
public void add_OnMeterChanged(Action value); // RVA: 0xDEF2F8 Offset: 0xDEF2F8
```

```
v22 = byte_BB77C;
v0 = 417172395;
}
else if ( v0 == 126333527 )
{
    x_342 = (int (_fastcall *(_DWORD))(v17 + 0xDEA2C8); // get_IsMonster
    (*(void (_fastcall **)(int, int (_fastcall )(int), int (_fastcall **)(_DWORD)))(x_346 + 8))( // get_CurrentHp
        v17 + 0xDEE764,
        sub_333E4,
        &y_15);
    v0 = 202977793;
    if ( !(((BYTE)dword_885FB * ((BYTE)dword_885FB - 1)) & 1) )
        v0 = 2038671105;
    v1 = 0;
    if ( dword_887DD < 10 )
        v1 = 1;
    else
        v0 = 202977793;
    if ( v1 != (((BYTE)dword_885FB * ((BYTE)dword_885FB - 1)) & 1) == 0 )
        v0 = 2038671105;
}
else
{
```

“ TeamAR.so 코드 ”



2-4. 해킹된 변조앱 분석

TOAST

```
v2 = a1;
v11 = COERCE_FLOAT(y_15(a1));
v12 = x_342(v2); // IsMonster
v3 = 0;
v4 = 146806589;
v5 = 146806589;
WORD(v6) = -168;
if ( (~(_DWORD *)((char *)std::__ndk1::basic_string<char, std::__ndk1::char_traits<char>, std::allocator<char> *) + 1)
    * (~(_DWORD *)((char *)std::__ndk1::basic_string<char, std::__ndk1::char_traits<char>, std::allocator<char> *) + 1)
    - 1) | 0xFFFFFFFF ) != -1 )
    v3 = 1;
HIWORD(v6) = -32454;
v7 = ((v3 | (~(_DWORD *)((char *)std::__ndk1::basic_string<char, std::__ndk1::char_traits<char>, std::allocator<char> *) + 1) > 9)) ^ 1 | (~(_DWORD *)((char *)std::__ndk1::basic_string<char, std::__ndk1::char_traits<char>, std::allocator<char> *) + 1) > 9) ^ v3) == 0;
LOWORD(v8) = 12838;
LOWORD(v3) = 26685;
if ( !v7 )
{
    v4 = -875680824;
    v5 = 1995810106;
}
HIWORD(v8) = -3287;
HIWORD(v3) = 3416;
v9 = v6;
while ( 1 )
{
    while ( v9 > v8 )
    {
        if ( v9 > v3 )
        {
            if ( v9 == 223897662 )
            {
                v9 = v5;
            }
            else
            {
                v9 = v4;
                v13 = v11 / 5.0;
            }
        }
        else if ( v9 == -215403993 )
```

“ 몬스터일 경우 체력을 5로
나눈 값 적용 ”



2-5. 새로운 보호기법 추가(Stolen-Byte)



- 함수의 이름만 남고 보이지 않는 코드(mono)
- 보이지 않는 코드는 다른 곳에서 복호화가 진행되고 동작

```
18 // Token: 0x06003E85 RID: 16005 RVA: 0x00135F14 File Offset: 0x00134314
19 public void initPortal(NSDouble hp, bool allyPortal)
20 {
21     this.m_hitEffectRemainCount = 0;
22     if (this.cachedSpriteRenderer != null)
23     {
24         this.cachedSpriteRenderer.color = Color.white;
25     }
26     this.m_dxHP = hp;
27     this.currentHP = hp;
28     this.isAlly = allyPortal;
29     base.cachedGameObject.SetActive(true);
30     this.setState(State.Idle);
31     this.spawnCount = Int.MaxValue;
32     if (!this.isAllyPortal)
33     {
34         if (GameManager.currentBaseMode == GameManager.GameMode.StoryMode || GameManager.currentBaseMode == GameManager.GameMode.PvP)
35         {
36             this.spawnCount = ManagerSingleton<EnemyManager>.instance.getEnemySpawnCount();
37         }
38     }
39 }
40
41 // Token: 0x06003E86 RID: 16006 RVA: 0x00135FB4 File Offset: 0x001343B4
42 protected override IEnumerator Idle()
43 {
44     yield return null;
45     yield break;
46 }
47
48 // Token: 0x06003E87 RID: 16007 RVA: 0x00135FC8 File Offset: 0x001343C8
49 protected override void dieInit()
50 {
51     if (GameManager.currentGameMode != GameManager.GameMode.PvP && this.isAllyPortal)
52     {
53         return;
54     }
55     if (GameManager.currentGameMode == GameManager.GameMode.StoryMode)
56     {
57         NSDouble nsdouble = LabManager.getFlaskValueForClearStage();
58         int num = 20;
59         nsdouble /= (double)num;
60         for (int i = 0; i < num; i++)
61         {
62             ManagerSingleton<DropItemManager>.instance.spawnDropitem(DropItemManager.DropItemType.Upgrade);
63         }
64     }
65     else if (GameManager.currentGameMode == GameManager.GameMode.MachaCity)
66     {
67         NSDouble nsdouble2 = LabManager.getGearValueForClearStage();
68         int num2 = 20;
69         nsdouble2 /= (double)num2;
70         for (int i = 0; i < num2; i++)
71         {
72     }
```

기존

```
14     return this.cachedSpriteRenderer.cachedTransform.position + new Vector3(0f, 0.73f, 0f);
15 }
16
17 // Token: 0x06003E85 RID: 16005 RVA: 0x00135F14 File Offset: 0x00134314
18 public void initPortal(NSDouble hp, bool allyPortal)
19 {
20 }
21
22 // Token: 0x06003E86 RID: 16006 RVA: 0x00135FB4 File Offset: 0x001343B4
23 [DebuggerHidden]
24 protected override IEnumerator Idle()
25 {
26 }
27
28 // Token: 0x06003E87 RID: 16007 RVA: 0x00135FC8 File Offset: 0x001343C8
29 protected override void dieInit()
30 {
31 }
32
33 // Token: 0x06003E88 RID: 16008 RVA: 0x00136114 File Offset: 0x00134514
34 public override void decreaseHP(UnitObject attacker, NSDouble value, UnitManager.AttackDamageType damageType, bool true)
35 {
36 }
37
38 // Token: 0x06003E89 RID: 16009 RVA: 0x00136238 File Offset: 0x00134638
39 protected override void Update()
40 {
41 }
42
43 // Token: 0x04002C28 RID: 11307
44 public SpriteRenderer cachedSpriteRenderer;
45
46 // Token: 0x04002C20 RID: 11308
47 public bool isAllyPortal;
48
49 // Token: 0x04002C2D RID: 11309
50 private int m_hitEffectRemainCount;
51
52 // Token: 0x04002C2E RID: 11310
53 private float m_timerForHitEffect;
54
55 // Token: 0x04002C2F RID: 11311
56 private bool m_isSwitchColor;
57
58 // Token: 0x04002C30 RID: 11312
59 private int spawnCount;
60
61
62 }
```

암호화



2-5. 새로운 보호기법 추가(가상화)

TOAST

- 기존 코드를 가상화해 Virtual CPU가 명령어를 해독해서 실행
- 국내 모바일 보호 솔루션에는 최초

```

1 int __fastcall sub_CD994()
2 {
3     unsigned int v4; // r4
4     unsigned __int8 *v5; // r5
5     unsigned __int8 *v6; // r6
6     int result; // r8
7     unsigned __int8 *i; // r1
8     int v9; // r2
9     int v10; // r2
10    int v11; // r2
11
12    v4 = a3;
13    v5 = a2;
14    v6 = this;
15    sub_CD708();
16    result = sub_CD39C();
17    if ( v5 )
18    {
19        result = v4 >> 8;
20        for ( i = 0; i != v5; ++i )
21        {
22            while ( 1 )
23            {
24                v9 = i[(_DWORD)v6];
25                if ( (unsigned __int8)i & 1 )
26                    break;
27                v10 = v9 ^ v4;
28                if ( (_DWORD)v6 ] = v10;
29                result ^= v10;
30                if ( v5 == ++i )
31                    return result;
32            }
33            v11 = v9 ^ result;
34            i[(_DWORD)v6] = v11;
35            v4 ^= v11;
36        }
37    }
38    return result;
39 }
```

NORMAL

```

21 sub_CD994();
22 {
23     v1 = *(__int8 *)(&loc_CC0A8 + dword_1BB0F4);
24     v2 = *(__int8 *)(&loc_CC114 + dword_1BB0F4);
25     v3 = *(__int8 *)(&loc_CC114 + dword_1BB0F8);
26     v4 = *(__int8 *)(&loc_CC114 + dword_1BB0F8);
27     v5 = *(__int8 *)(&loc_CC114 + dword_1BB0F8);
28     v6 = *(__int8 *)(&loc_CC114 + dword_1BB0F8);
29     v7 = *(__int8 *)(&loc_CC114 + dword_1BB0F8);
30     v8 = *(__int8 *)(&loc_CC114 + dword_1BB0F8);
31     v9 = *(__int8 *)(&loc_CC114 + dword_1BB0F8);
32     v10 = *(__int8 *)(&loc_CC114 + dword_1BB0F8);
33     v11 = *(__int8 *)(&loc_CC114 + dword_1BB0F8);
34     v12 = *(__int8 *)(&loc_CC114 + dword_1BB0F8);
35     v13 = *(__int8 *)(&loc_CC114 + dword_1BB0F8);
36     for ( i = 0; i < v15; ++i )
37     {
38         v17 = 28;
39         ((&loc_CC114 + dword_1BB0F4))(4, 0, &v10);
40         v17 = 32;
41         v10 = i;
42         ((&loc_CC114 + dword_1BB0F8))(1, 0, &v9);
43         v9 = *(v16 + v10);
44         if ( v10 % 2 )
45         {
46             v17 = 80;
47             *(v16 + v10) = v9 ^ v12;
48             v6 = *(v16 + v10);
49             v17 = 40;
50             v13 ^= v6;
51         }
52         else
53         {
54             v17 = 76;
55             *(v16 + v10) = v9 ^ v13;
56             v7 = *(v16 + v10);
57             v17 = 36;
58             v12 ^= v7;
59         }
59         v17 = 44;
60         ((&loc_CC0A8 + dword_1BB104))(1, 0, &v9);
61         v17 = 48;
62         ((&loc_CC0A8 + dword_1BB108))(4, 0, &v10);
63         v17 = 56;
64     }
65     v17 = 20;
66     ((&loc_CC20C + dword_1BB0EC))(4, 0, &v12);
67     v17 = 60;
68     ((&loc_CC23C + dword_1BB114))(1, 0, &v12);
69     v17 = 64;
70     return ((&loc_CC23C + dword_1BB118))(1, 0, &v13);
71 }
```

OBF



2-6. 지속적인 모니터링



- 로그수집을 이용한 해킹 시도 및 진척도 확인
- 지속적인 공격을 하는 해커 주시

package_info	action	platform	device_id	language	detail	detect_p
com.nhnent.SKQUEST	block	Android(NDK)	[REDACTED]	en	libil2cpp.so:text:dbceb70a;	NULL
com.nhnent.SKQUEST	block	Android(NDK)	[REDACTED]	ko	libil2cpp.so:text:c3319460;	NULL
com.nhnent.SKQUEST	block	Android(NDK)	[REDACTED]	ko	libil2cpp.so:file:882351ef;	NULL
com.nhnent.SKQUEST	block	Android(NDK)	[REDACTED]	ko	libil2cpp.so:file:882351ef;	NULL
com.nhnent.SKQUEST	block	Android(NDK)	[REDACTED]	ko	libil2cpp.so:file:882351ef;	NULL
com.nhnent.SKQUEST	block	Android(NDK)	[REDACTED]	ko	libunity.so:text:1aa2079d;	NULL
com.nhnent.SKQUEST	block	Android(NDK)	[REDACTED]	en	libil2cpp.so:text:67e45da1;	NULL
com.nhnent.SKQUEST	block	Android(NDK)	[REDACTED]	ko	libunity.so:text:2d04edee;	NULL

```
if (CST<AppGuardInfo>::GetInstance()->isAntiDebugging() == true)
{
```

안드로이드 리퍼블릭 분석가 정보

- 최초 번조 로그로 각종 번조시도 로그가 확인됨
 - 리퍼블릭 분석가로 추정됨
- 디바이스 아이디
 - 8[REDACTED]...[REDACTED]
- IP
 - 11[REDACTED].[REDACTED].[REDACTED].[REDACTED]
 - 모두 베트남 아이피
- 탈지 로그 정보
 - 루팅 탈지, 서명 번조 탈지, 메니페스트 번조, il2cpp번조, 301(xposed) 탈지

```
atible.so";
:Addr(-1, libCompatible.c_str());

::AndroidRepublic, PatternGroup::Modification, PatternName::Sigtrap,
'republic.so';
:Addr(-1, libAndRep.c_str());

::AndroidRepublic, PatternGroup::Modification, PatternName::Sigtrap,
```



안드로이드 리퍼블릭

1. 월 20달러를 결제하는 VIP 고객을 위해 게임 변조
2. 각국의 서포터즈가 멤버들을 관리해 소통 문제 해결
3. 보호 솔루션이 적용되어 있으면 분석해서 무력화하고 자신들이 사용하는 솔루션으로 보호
4. 변조 앱 샘플을 구하기도 힘들지만 분석도 힘들다.
5. 킹덤스토리 분석가의 IP를 따보니 베트남 IP. 부업으로 하는 듯
6. 이런 글로벌 서비스를 한다는 것은 입장에서는 대단한 조직

현재 NHN 게임의 변조 앱이 올라오지 않고 있음.

보호 수준이 높아짐에 따라 시간이 많이 소요되어
포기하고 다른 앱 변조하러 간 듯 ㅎ

“ ”
이겼다.





제 2부. 크리티컬 옵스 베타 테스트

기간

2019년 8월 30일 - 2019년 9월 01일



NHN 신작 '크리티컬옵스', 아시아 테스트 '돌입'

임영택 기자 | 입력 : 2019.08.30 10:06:44



NHN(대표 정우진)은 핀란드 개발사 크리티컬포스(대표 사미엠 툴로넨)와 공동 개발한 모바일 FPS '크리티컬옵스:리로디드'의 테스트를 오는 9월 1일까지 한국과 일본, 인도 지역에서 실시한다.

'크리티컬옵스:리로디드'는 슈팅 장르 본연의 재미를 살린 1인칭 슈팅(FPS)게임이다. 지난 2015년 출시해 글로벌 5000만 다운로드를 기록하며 인기를 끈 '크리티컬옵스'의 아시아 버전이다.



NHN은 사흘간의 테스트 기간 동안 매일 오후 8시부터 자정까지 하루 4시간씩 서버를 운영한다. 또 스포티비게임즈의 FPS게임 전문 MC 김수현 아나운서를 기용해 '특집 라이브 방송'도 마련한다. '크리티컬옵스:리로디드' 공식 유튜브 채널 및 트위치를 통해 테스트 기간 동안 매일 오후 9시부터 10시 사이 모바일 FPS 유튜버와 이용자간 경기를 생중계한다.



3.1 배경

TOAST

핵 신고 | 자유게시판

전체공개 2019.09.01. 21:21

IVAINGLORY(gur1****) 크옵대원 ★ 1:1

<https://cafe.naver.com/criticalopsreloaded/395> 주소복사

유저명 : ops-8793
p90으로 올 헤드에 샷건처럼 머리에 박하고 esp까지 있는거 같네요

패배

73 42

	KILLS	DEATHS	ASSISTS	PING
OPS-8793	49	9	0	274
LazyTurtle	21	12	0	30
	9	11	0	12
	12	15	1	14
	7	6	0	83
	6	13	1	350
	5	12	0	351
	2	17	0	42
	3	4	2	13
	0	5	0	25

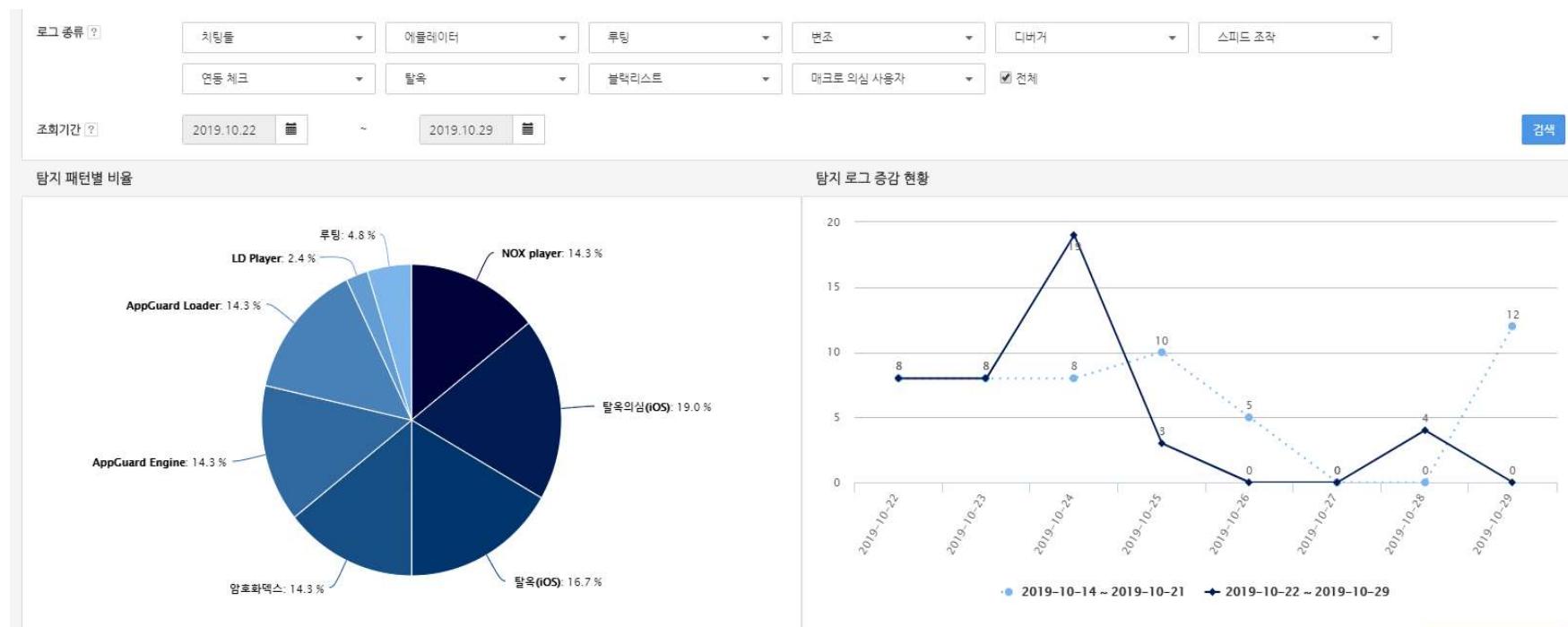
- 하루~이틀만에 게임해킹이 발생함
- 실제 테스트 과정 중에 핵 사용자를 발견



3.1 배경

TOAST

- 앱가드는 다양한 해킹 시도와 탐지/차단된 로그들을 확인할 수 있음

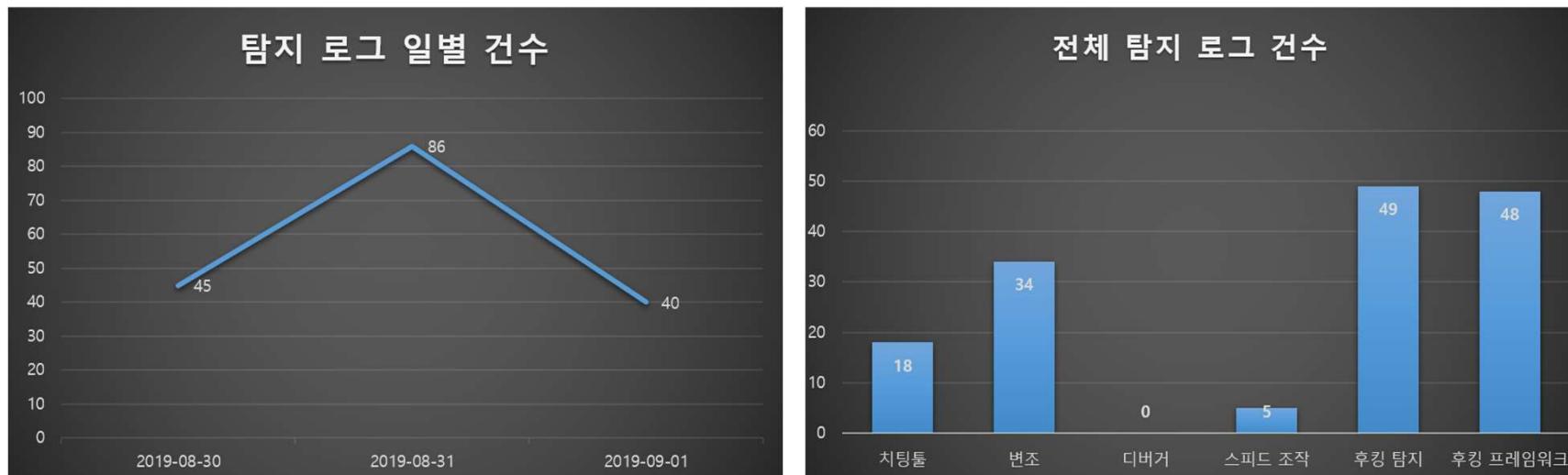


3.2 전체 로그



전체 탐지 로그 분석

- 루팅과 에뮬레이터를 제외한 일별로그
- 해킹 시도 탐지된 로그는 총 154건이며, 시스템 API 후킹이 49건 탐지



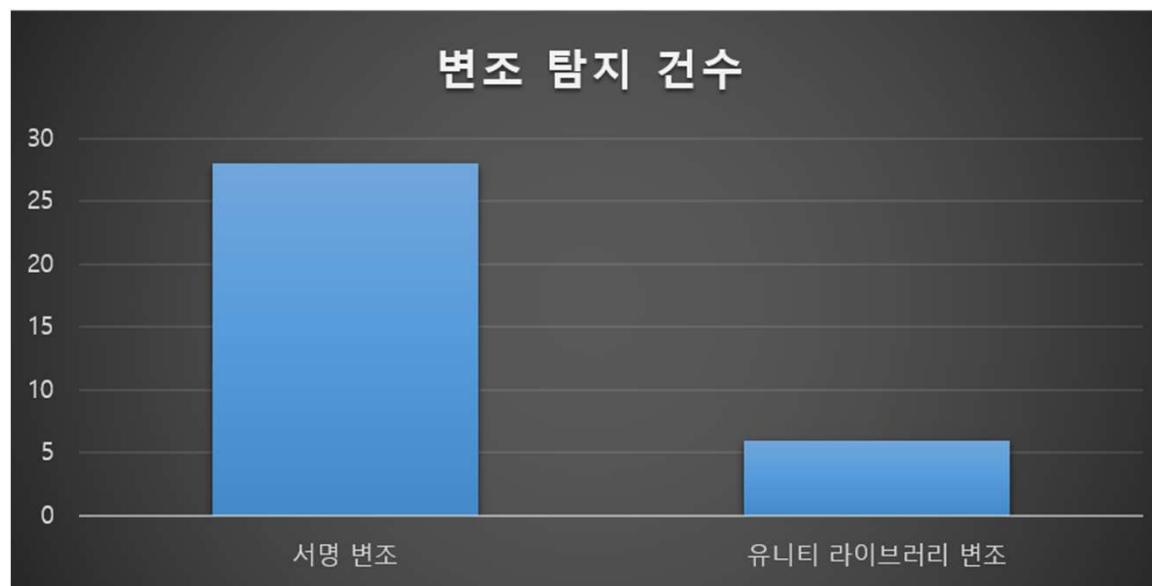
- 시스템 API 후킹?

게임 종료 함수를 우회하거나 프로세스 탐지, 파일 탐지 등에 사용되는 API들을 후킹함
앱 가드의 탐지 기능을 피하는 방법



변조로그분석

- 게임 내 실제 실행되는 코드들을 변조하여 게임에 직접적인 영향을 주게됨 (월핵, 데미지핵 등)
- 변조로그는 총 34건
 - 서명 변조 28건
 - 유니티 변조 6건
- 이중 유니티 변조는 파일 변조가 아닌 메모리 변조로 확인됨
 - 라이브러리 패킹 기능으로 인하여 암호화된 파일을 복호화를 하지 못하여, 메모리 내 코드 영역 변조 시도



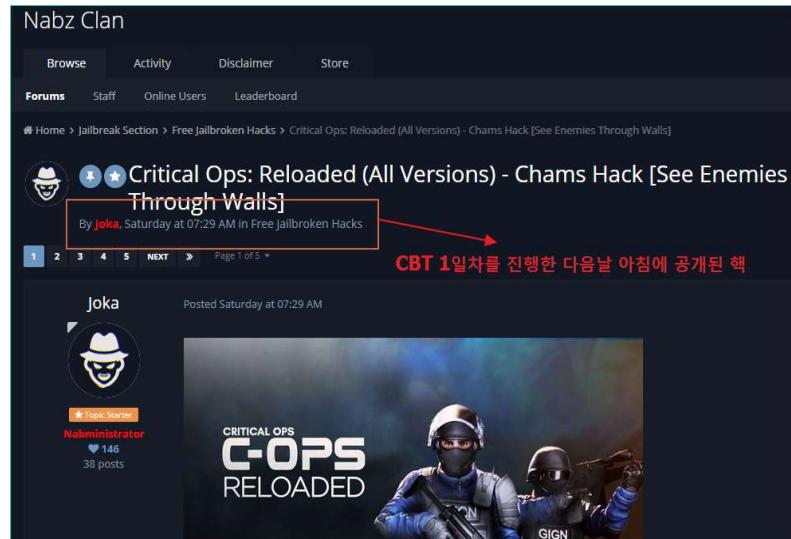
결론

- 해커들은 분석을 진행했지만 앱 가드가 정상적으로 차단하여 분석을 방지함



유,무료 버전으로 공개되어 있던 트윅

- 구글에 크리티컬 옵스 핵을 검색
- 17가지의 기능제공
- 무료버전은 월핵만제공



3. 트윅

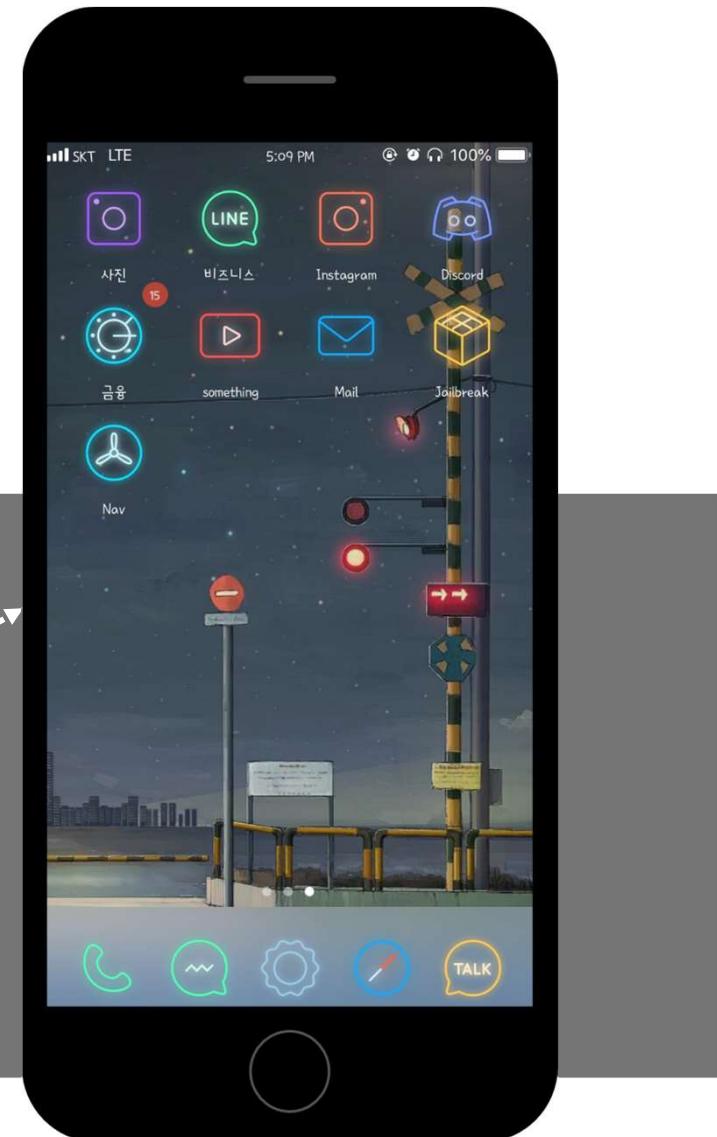
TOAST

Tweak 이란?

- 앱과 같지만, 일반 앱에서 할 수 없는 권한을 가진다.
- 메모리 변조, 후킹, 시스템 변경
- 탈옥된 사용자만 사용 가능

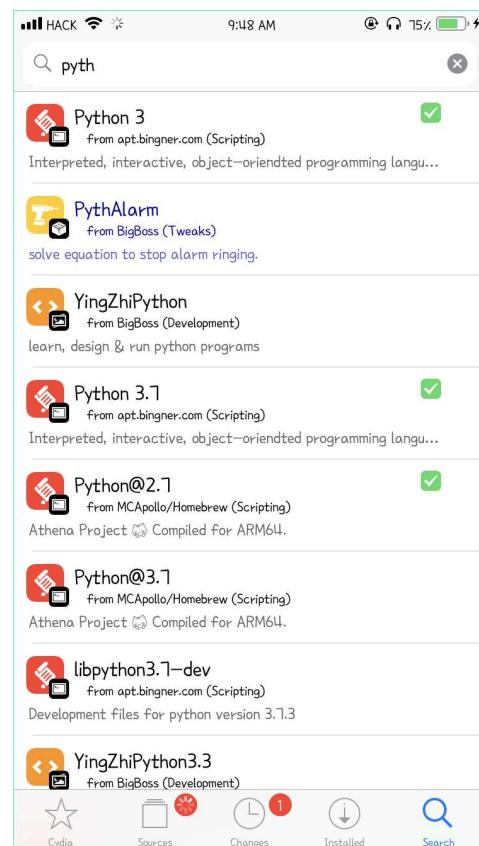
설치된 트윅

1. 통화가 끝나면 구글 드라이브 업로드
2. 떨어트리면 아프다고 소리지르기
3. 유튜브 백그라운드 재생 + 광고 제거
4. 탈옥 환경 탐지 우회
5. 네온 사인 테마

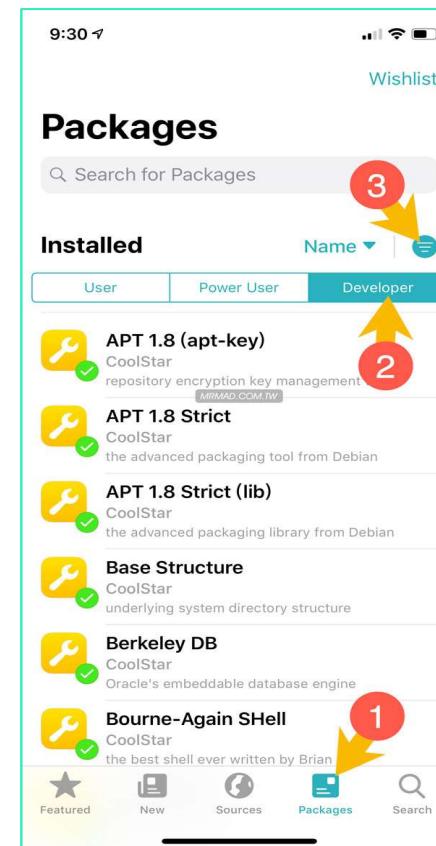


탈옥 유저들의 앱스토어

Cydia



Slieo



3.7 탈옥 커뮤니티



```
void setup(void)
{
    __int64 v0; // x0
    __int64 v1; // x0
    intptr_t v2; // x0
    intptr_t v3; // x0
    intptr_t v4; // x0
    intptr_t v5; // x0
    intptr_t v6; // x0
    intptr_t v7; // x0
    id v8; // x20
    id v9; // x19
    double v10; // d1

    v0 = MSFindSymbol(0LL, "_glDrawElements");
    MSHookFunction(v0, $glDrawElements, &_glDrawElements);
    v1 = MSFindSymbol(0LL, "_glGetUniformLocation");
    MSHookFunction(v1, $glGetUniformLocation, &_glGetUniformLocation);
    v2 = _dyld_get_image_vmaddr_slide(0);
    MSHookFunction(v2 + 0x101560260LL, _GameSystem_Update, &GameSystem_Update);
    v3 = _dyld_get_image_vmaddr_slide(0);
    MSHookFunction(v3 + 0x1015301FCLL, _Character_Gameplay_Update, &Character_Gameplay_Update);
    v4 = _dyld_get_image_vmaddr_slide(0);
    MSHookFunction(v4 + 0x1013A3E64LL, _NoRecoil, &NoRecoil);
    v5 = _dyld_get_image_vmaddr_slide(0);
    MSHookFunction(v5 + 0x1013A3F14LL, _NoSpread, &NoSpread);
    v6 = _dyld_get_image_vmaddr_slide(0);
    MSHookFunction(v6 + 0x1015AE850LL, _CrashLobby, &CrashLobby);
    v7 = _dyld_get_image_vmaddr_slide(0);
    MSHookFunction(v7 + 0x101414494LL, CustomSensitivity, &CustomSensitivity_Old);
    ...
}
```



global-metadata.dat

- 유니티를 이용해 개발된 게임은 해당 파일에 함수들의 정보가 저장! (iOS, AOS 모두)



Il2CppDumper

```
C:\Users\NHNEnt\Downloads\Il2CppDumper-v4.6.0\Il2CppDumper.exe  
Input Unity version:  
2019.1  
Initializing metadata...  
Select Mode: 1.Manual 2.Auto 3.Auto(Plus) 4.Auto(Symbol)  
Initializing il2cpp file...  
Searching...  
CodeRegistration : 102af9470  
MetadataRegistration : 102b9b9c0  
WARNING: Unable to get function pointers for System.Diagnostics.StackTrace.dll  
WARNING: Unable to get function pointers for System.Globalization.Extensions.dll  
WARNING: Unable to get function pointers for System.IO.Compression.dll  
WARNING: Unable to get function pointers for UnityEngine.dll  
WARNING: Unable to get function pointers for netstandard.dll  
Dumping...  
Done !  
Create DummyDLL...  
Done !  
Press any key to exit...
```

- Generates dummy DLLs that can be viewed in .NET decompilers



3.8 트윅 상세 분석

TOAST

```
private void UpdateCollider(Character c); // RVA: 0x10155C330 Offset: 0x155C330
public void KillCharacter(int id, int killerID, int shortTimeKillCount, int assistID, LiveWeaponData victimWeapon, BodyPart bodyPart, Vector3 deathForce); // RVA: 0x10155C46C Offset: 0x155C46C
public void DestroyCharacter(int id, optional bool teamflip); // RVA: 0x10155C798 Offset: 0x155C798
public void DestroyCharacter(Character character, optional bool teamflip); // RVA: 0x10155C5FC Offset: 0x155C5FC
public T GetCharacter(int id); // RVA: 0x101752080 Offset: 0x1752080
public Character GetCharacter(int id); // RVA: 0x10155C59C Offset: 0x155C59C
public int GetCharacterID(Character character); // RVA: 0x10155C8B0 Offset: 0x155C8B0
public bool CharacterExists(int id); // RVA: 0x10155B234 Offset: 0x155B234
public bool IsDead(Player player); // RVA: 0x10155CAD4 Offset: 0x155CAD4
public Team GetEnemyTeam(Team team); // RVA: 0x10155CB94 Offset: 0x155CB94
public List`1<Character> GetCharacters(Team ofTeam); // RVA: 0x10155CBA4 Offset: 0x155CBA4
public List`1<Character> GetEnemies(Team ofTeam); // RVA: 0x10155CBBC Offset: 0x155CBBC
public void SpotCharacter(Character target); // RVA: 0x10155CBD4 Offset: 0x155CBD4
public LiveWeaponData CreateWeapon(int weaponID, string ownerName, int weaponDefID, int weaponsOffset); // RVA: 0x10155CCCC Offset: 0x155CCCC
public bool WeaponExists(int weaponID); // RVA: 0x10155D27C Offset: 0x155D27C
public void AssertWeapon(int weaponID); // RVA: 0x10155D2EC Offset: 0x155D2EC
public LiveWeaponData GetWeapon(int weaponID); // RVA: 0x10155D354 Offset: 0x155D354
public void DestroyWeapon(int weaponID); // RVA: 0x10155D3D0 Offset: 0x155D3D0
public WeaponOnGround GetWeaponOnGround(int weaponID); // RVA: 0x10155D5C4 Offset: 0x155D5C4
public void DestroyWeaponOnGround(int weaponID); // RVA: 0x10155D51C Offset: 0x155D51C
public void DestroyWeaponOnGround(WeaponOnGround weapon); // RVA: 0x10155D6D0 Offset: 0x155D6D0
public MaterialDef GetMaterialForCollider(Collider c); // RVA: 0x10155D880 Offset: 0x155D880
public WeaponOnGround DropWeapon(Character character, LiveWeaponData weapon, Vector3 position, Vector3 rotation, Vector3 angularVelocity, bool thrown); // RVA: 0x10155D9B8 Offset: 0x155D9B8
```



월핵분석

- OpenGL 함수 glDrawElements, glGetUniformLocation을 후킹

```
id setup(void)
{
    __int64 v0; // x0
    __int64 v1; // x0

    v0 = MSFindSymbol(0LL, "_glDrawElements");
    MSHookFunction(v0, $glDrawElements, &_glDrawElements);
    v1 = MSFindSymbol(0LL, "_glGetUniformLocation");
    MSHookFunction(v1, $glGetUniformLocation, &_glGetUniformLocation);
    return objc_msgSend(
        qword_35D78,
        "addSwitch:description:",
        CFSTR("Chams"),
        CFSTR("Enemies will be visible through all walls."));
}
```



3.8 트윅 상세 분석

```

id __fastcall $glDrawElements(__int64 a1, __int64 a2, __int64 a3, const void* a4)
{
    __n128 v4; // q8
    __n128 v5; // q9
    const void *v6; // x19
    __int64 v7; // x20
    __int64 v8; // x21
    int v9; // w22
    id result; // x0
    unsigned int v11; // [xsp+Ch] [xbp-44h]

    v6 = a4;
    v7 = a3;
    v8 = a2;
    v9 = a1;
    result = (id)_glDrawElements(a1, a2, a3, a4); // glDrawElements 호출
    if ( v9 == 4 && (int)v8 >= 1000 )
    {
        glGetIntegerv(35725LL, &v11);
        result = (id)_glGetUniformLocation(v11, "_Color4");
        if ( (_DWORD)result != -1 )
        {
            result = objc_msgSend(flag_35D78, "isSwitchOn:", CFSTR("Chams")); // Menu Switch Chams
            if ( (_DWORD)result )
            {
                v4.n128_u32[0] = 1.0;
                v5.n128_u32[0] = 0.5;
                glDepthRangef(v4, v5); // R/G/B/Alpha - 초록색으로 그려주는 효과
                glEnable(3042LL); // GL_BLEND - GL_BLEND
                glBindFunc(770LL, 1LL);
                _glDrawElements(4LL, v8, v7, v6); // glDrawElements 재호출
                glDepthRangef(v5, v4);
                glColorMask(1LL, 1LL, 1LL, 1LL);
                result = (id)glDisable(3042LL);
            }
        }
    }
    return result;
}

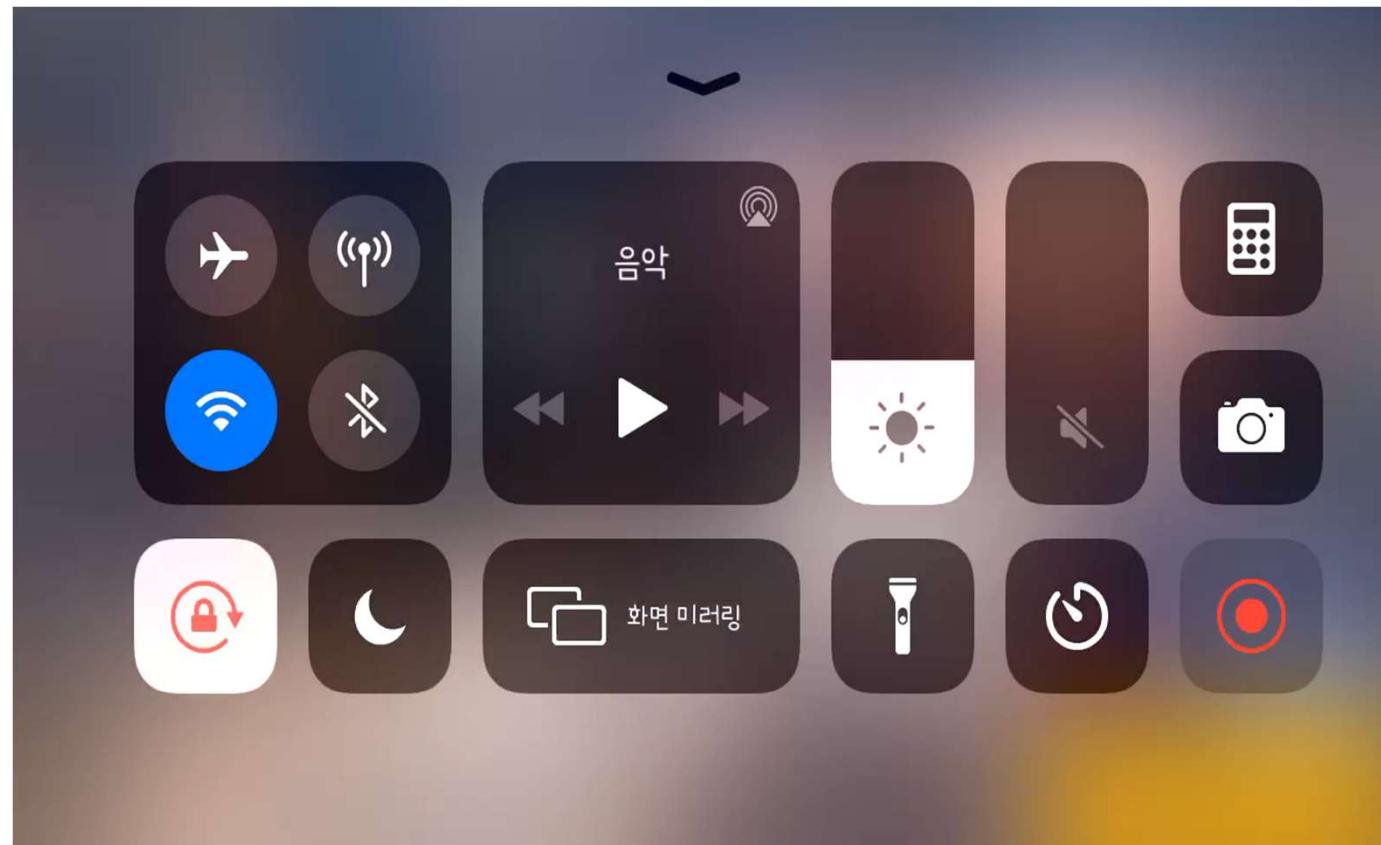
```

The screenshot shows a game menu for 'Critical Ops: Reloaded v0.0.3 Chams Mod Menu'. The 'Chams' button is highlighted with a red box. A red arrow points from the line of code `result = objc_msgSend(flag_35D78, "isSwitchOn:", CFSTR("Chams"));` to the 'Chams' button in the menu.



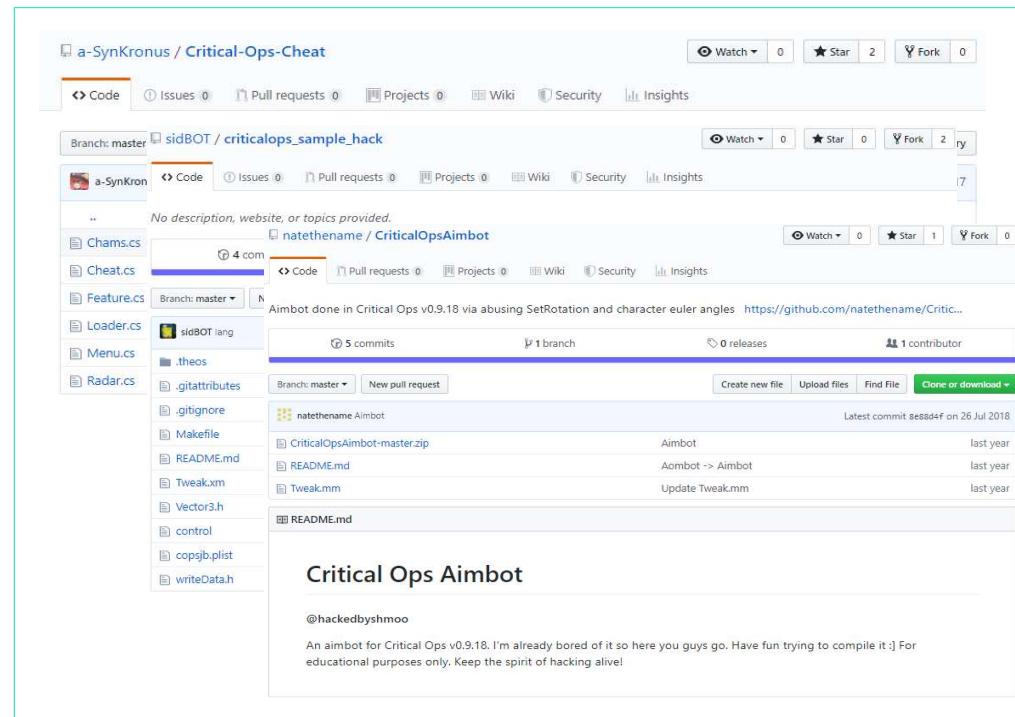
3.9 트윅을 이용한 플레이 영상

TOAST



빠르게 핵이 등장한 배경

- 1. iOS는 탈옥한 아이폰 기기를 막는 것이 쉽지가 않음. (탈옥한 사용자의 권한이 막강)
- 2. FPS 게임류의 특성상 핵을 사용하는 유저가 많음.
- 3. 크리티컬옵스 웨스턴 버전의 소스코드와 많이 유사함.
- 크리티컬옵스 iOS는 앱가드가 적용된다면 베타기간은 문제 없었을 것.
- [*] 안드로이드에서 그랬던 것처럼 뚫고 막히는 오랜싸움을 해야 한다.



Thank You.

