S2W

# 제1회
# S2W WITH 웨비나

2023년 2월 28일 (화) • LIVE
오후 2:00 - 3:30

**For February**
다크웹과 침해사고

**Agenda**

| | |
|---|---|
| 2:00 - 2:10 | 키노트 |
| 2:10 - 2:30 | 딥다크웹 동향 & 인사이트 |
| 2:30 - 3:00 | Account Take Over 시나리오 |
| 3:00 - 3:30 | QnA |

1. Keynote

# 데이터 인텔리전스 웨비나 S2W <with>는 무엇인가요?

서상덕, CEO

# S2W, 데이터 인텔리전스 R&D 회사

1.

**초 연결의 시대**: '디지털 전환' 으로 우리 일상생활은 '인터넷'이라는 온라인 공간으로 빠르게 이동하고 있습니다.

2.

**고도화된 기술의 대중화:** 최근 ChatGPT의 사례처럼, 기술은 특정 분야와 사람에게 국한되지 않고 빠르게 발전하고 있습니다.

3.

**연결? 노출!:** 기술의 발전 속도가 빨라질수록 우리에게 많은 편의를 제공하는 반면 새로운 위험에 노출시키기도 합니다.

# S2W, 데이터 인텔리전스 R&D 회사

1.

**초 연결의 시대**: '디지털 전환' 으로 우리 일상생활은 '인터넷'이라는 온라인 공간으로 빠르게 이동하고 있습니다.

2.

***"S2W <with>를 시작한 이유"***

**고도화된 기술의 대중화:** 최근 ChatGPT의 사례처럼, 기술은 특정 분야와 사람에게 국한되지 않고 빠르게 발전하고 있습니다.

***데이터 인텔리전스 기반 보안 지식과 인사이트를 나누는 장***

3.

**연결? 노출!:** 기술의 발전 속도가 빨라질수록 우리에게 많은 편의를 제공하는 반면 새로운 위험에 노출시키기도 합니다.

# S2W, Data Intelligence @ Cybersecurity Domain

## 1. (Big) Data Intelligence ?

Huge INFORMATION → ACTIONABLE INFORMATION

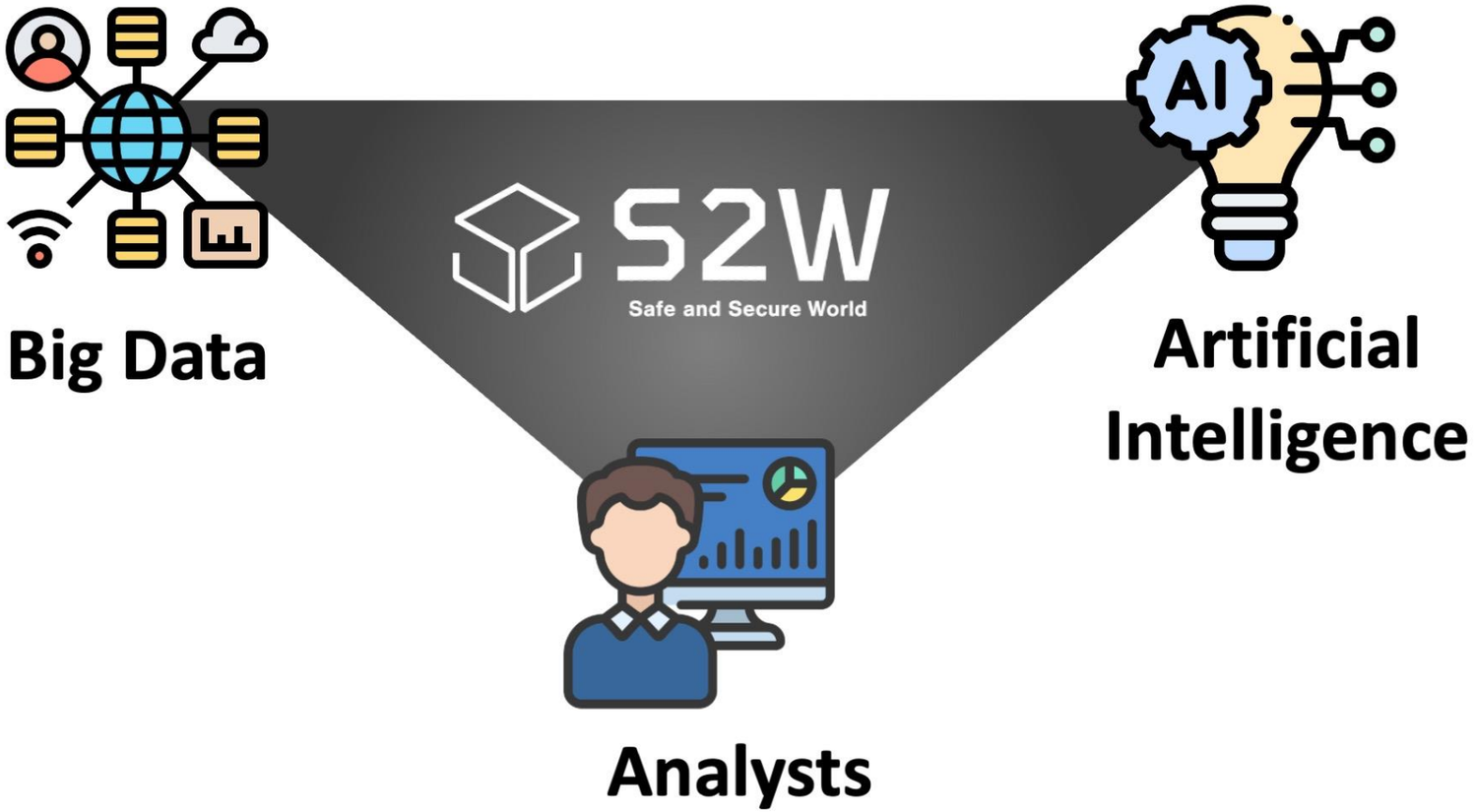
## 2. Cybersecurity Domain ?

ATTACK, LEAK, ABUSE, …

Monitor, Analyze, Defend Forward, Certify, Audit, Checkup, …

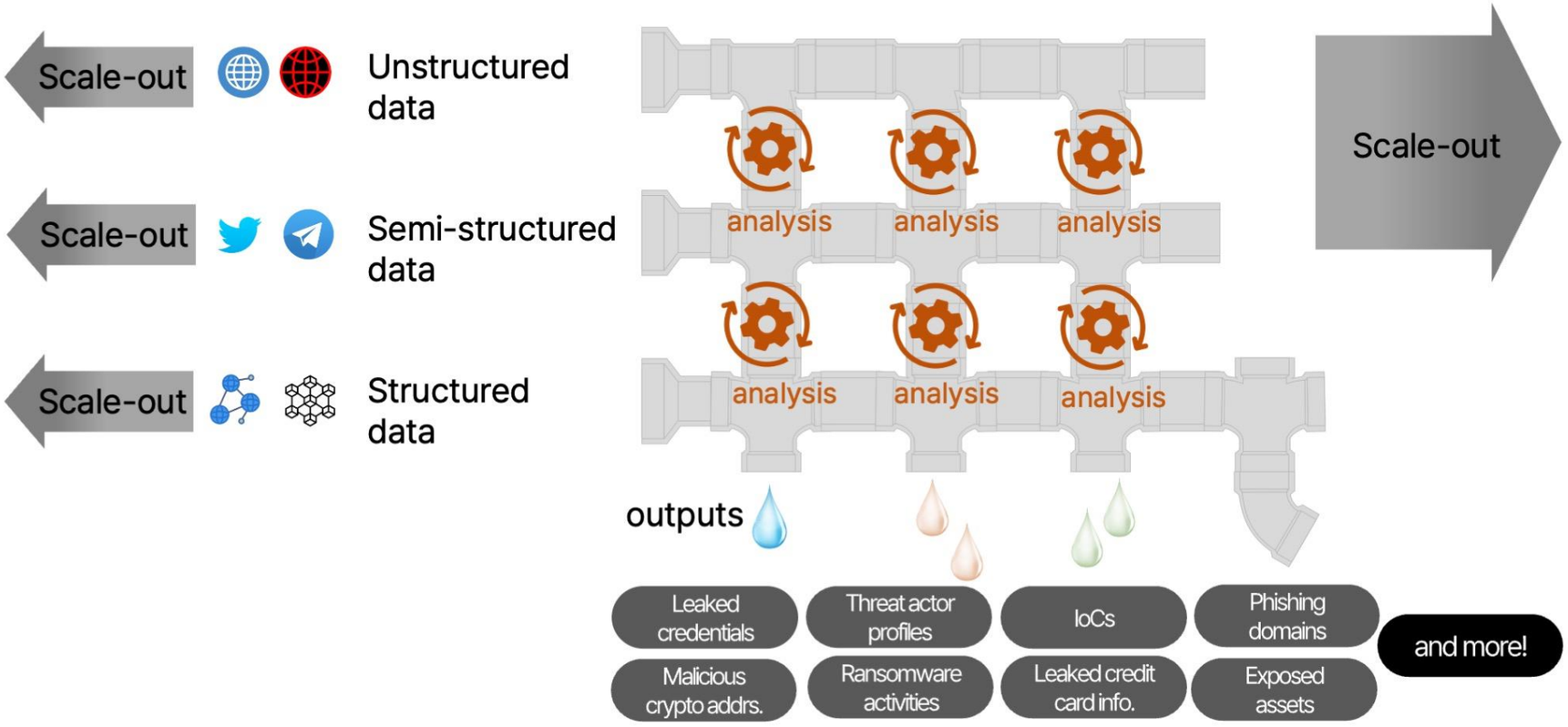
# S2W 데이터 인텔리전스 경쟁력의 기반

S2W fights against cybercrime with our specialists, big data and AI technologies



# 빅데이터 파이프라인 기반의 보안

It is scalable and efficient at processing and storage of various types of data.



# 빅데이터 파이프라인 기반의 보안

It is scalable and efficient at processing and storage of various types of data.


*다크웹, 딥웹..... 뭐가 나오긴 하나?*

*나온다면... 뭘 어떻게 할 수 있나?*

# 제1회 S2W <with>

2월 웨비나 주제는 급격히 성장하는 사이버 보안 문제의 가장 큰 허브, **다크웹 트렌드&침해사고(ATO)**에 대해 이야기합니다.

# 2023 아젠다

**Data Leak**
Credential(자격 증명), Confidential(기밀 정보), Personal Information(개인 정보) 등에 대한 데이터 유출

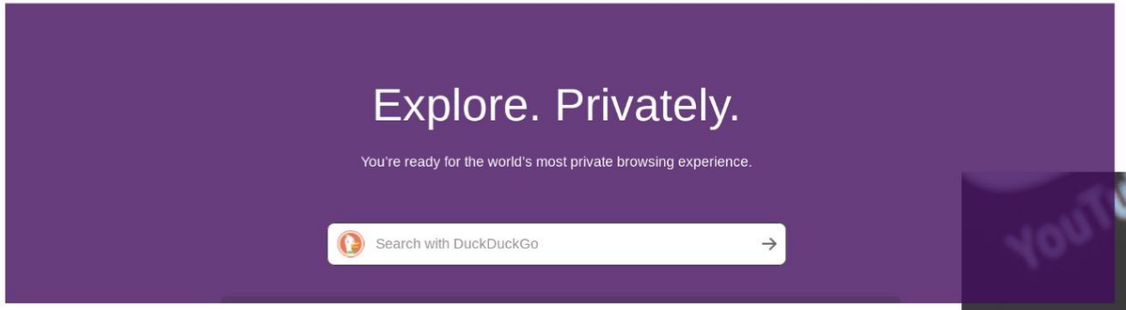
**Digital Abuse**
기업의 디지털 플랫폼 특성을 악의적으로 이용하여 금전적 이득을 취하는 행위

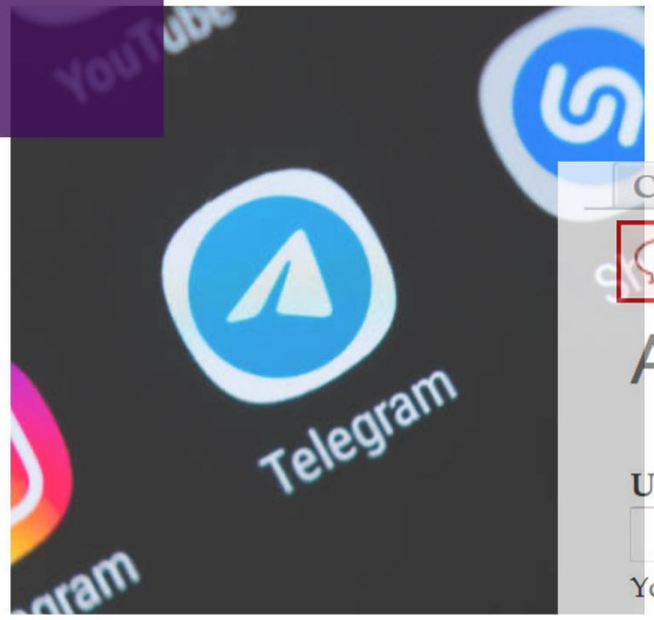
**Threat Actor**
기업과 개인을 대상으로 사이버 공격을 수행하는 공격 그룹에 대한 프로파일링

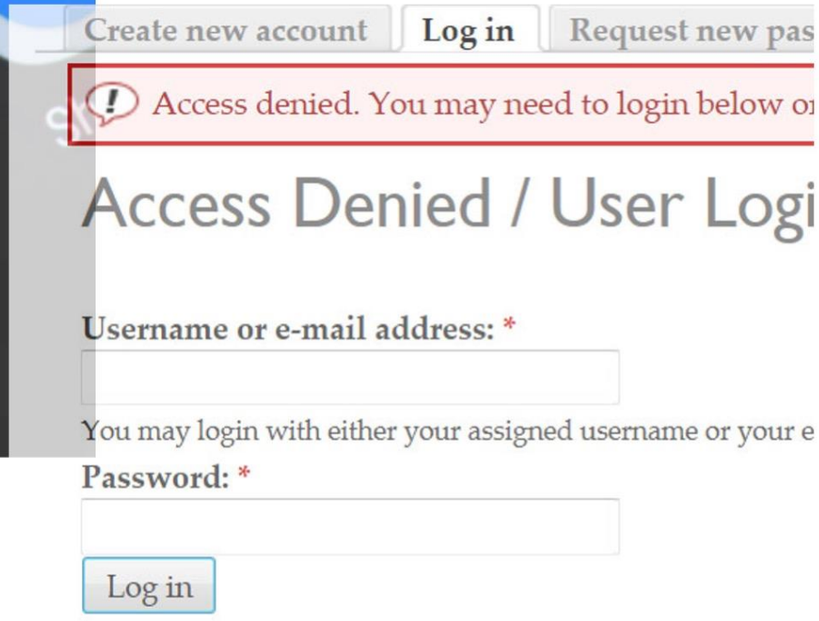
**Artificial Intelligence**
익명 채널 및 보안에 특화된 언어모델 개발 및 이를 통한 위협 콘텐츠 자동 탐지 및 분류

# 세상의 문제를, 기술로 이롭게

S2W가 집중해 온 다크웹, 딥웹, 텔레그램 등에 대한 데이터와 분석 기술에 대한 인사이트를 함께 나누는 장이 될 것입니다.



S2W

Safe and Secure World


## 심선형

**데이터 분석가**

딥/다크웹 데이터 인사이트 도출 및 분석

2. 딥다크웹 동향 및 인사이트

# 범죄의 목적, 다크웹 개요, 다크웹 최신 동향

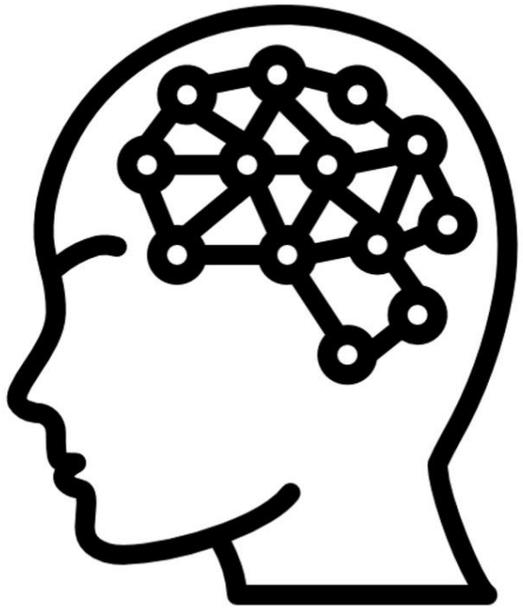
심선형, Data Analyst

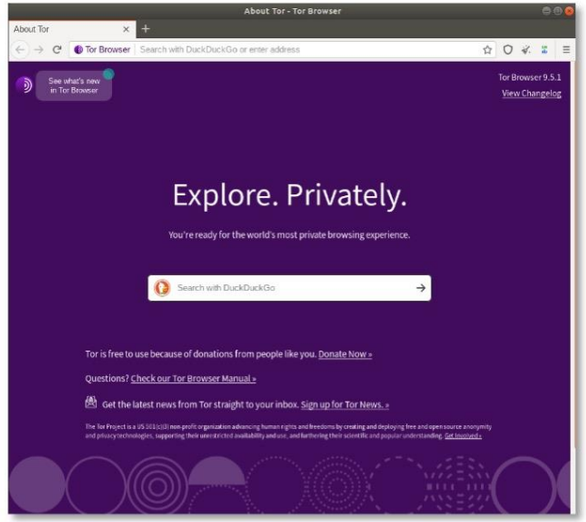
# (1) 발표자 소개

## AI를 통한 딥/다크웹 주요 이슈 발견

BF

~/ XSS.is




***사이버 범죄 생태계에도 범죄 트렌드가 있다!***

# (2) 해커들의 대전제: 왜 사이버 공격을 할까?

**범죄 자체가 일어나는 이유는 무엇일까?**

강도


불법 도박

탈세

유괴

# (2) 해커들의 대전제: 왜 사이버 공격을 할까?

**범죄는 금전 탈취라는 하나의 목적 아래서 실행됨**

강도


불법 도박

탈세

유괴

# (2) 해커들의 대전제: 왜 사이버 공격을 할까?

## 그렇다면 해커들의 목적은?

***해킹 기술 자랑을 통한***
***유명 해킹 그룹의 주목?***

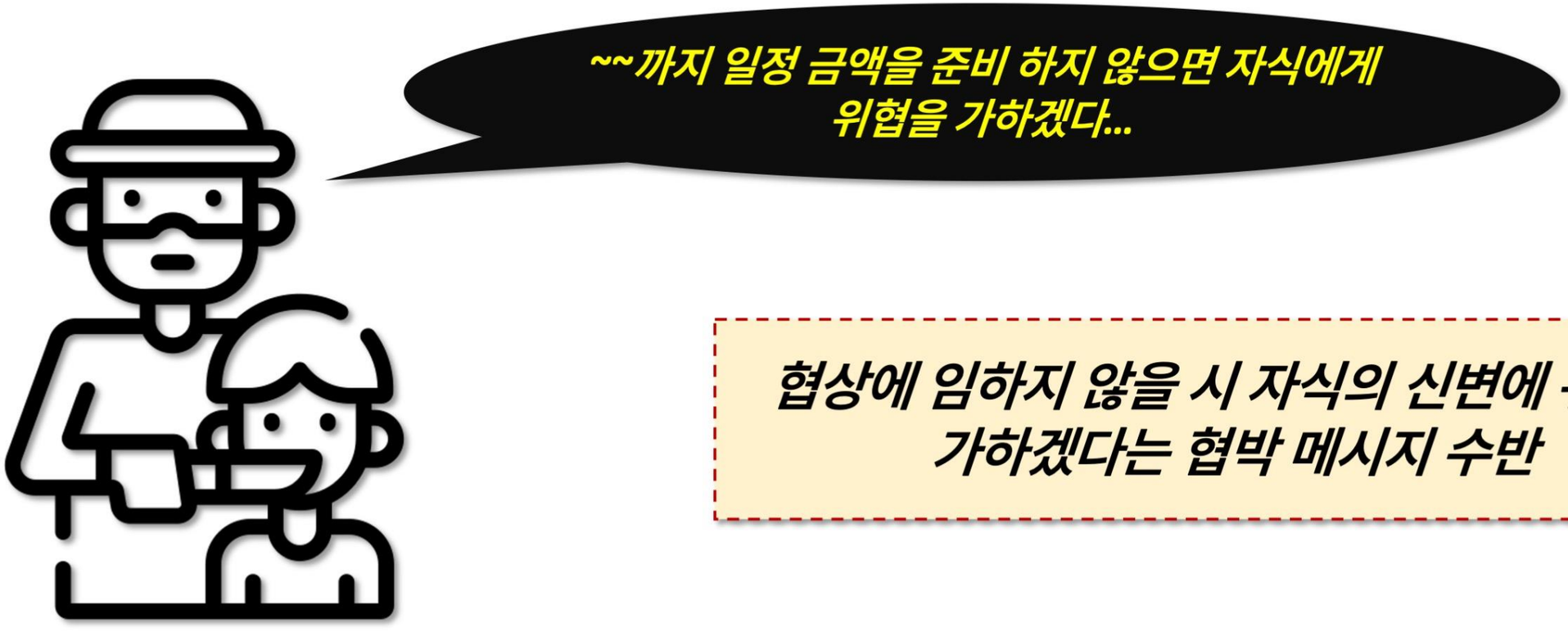
# (2) 해커들의 대전제: 왜 사이버 공격을 할까?

그렇다면 해커들의 목적은?

***금전 및 자산 탈취***

# (2) 해커들의 대전제: 왜 사이버 공격을 할까?

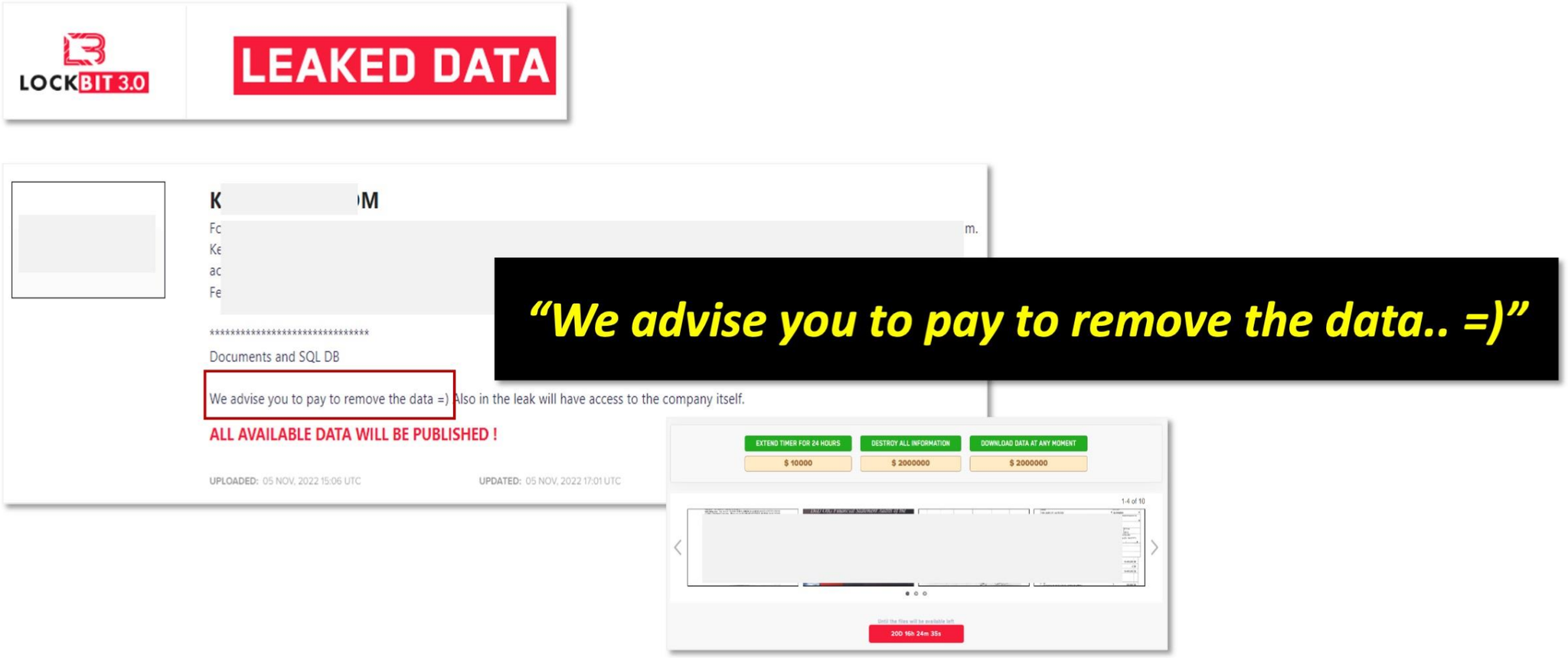
**유괴: 부모로부터 소중한 자식을 납치하여 협박하는 행위**




*협상에 임하지 않을 시 자식의 신변에 위협을 가하겠다는 협박 메시지 수반*

# (2) 해커들의 대전제: 왜 사이버 공격을 할까?

## 랜섬웨어: 유괴와 동일한 수법, 행해지는 방식과 주체가 다를 뿐




***"We advise you to pay to remove the data.. =)"***

# (2) 해커들의 대전제: 왜 사이버 공격을 할까?

## 오프라인 범죄에는 실행하기 어려운 온라인 범죄의 최대 장점

*집에서 편하게 원격으로 범죄에 가담 가능*

*24/7 범죄 가담 가능*

*범죄 유형의 다양화*

***익명성이 보장됨***

***과 동시에, 금전과 자산을 갈취!***

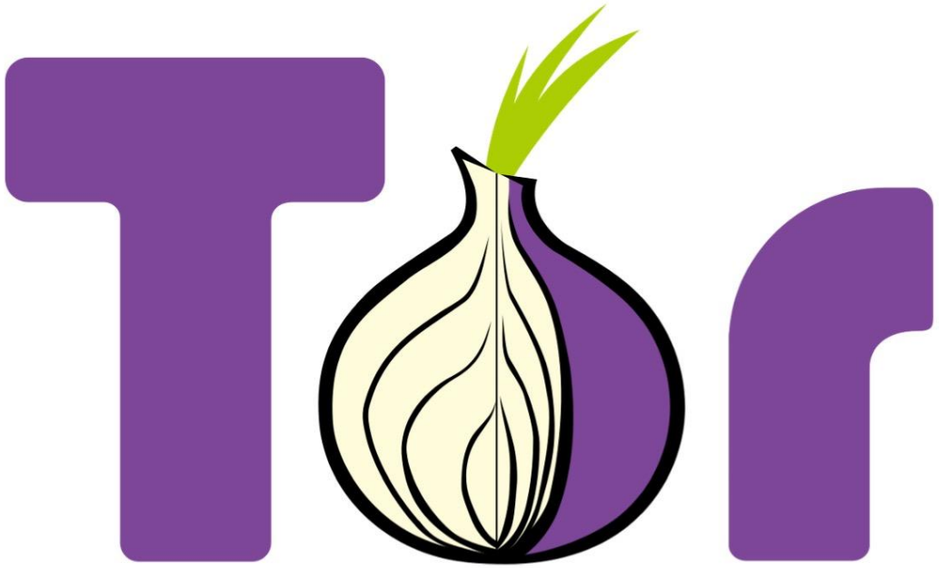
# (2) 해커들의 대전제: 왜 사이버 공격을 할까?

***익명성이 보장되며, 금전과 자산 갈취가 가능한 공간은 어디일까..?***

# (3) 해커들의 무대. 딥/다크웹 공간이란?

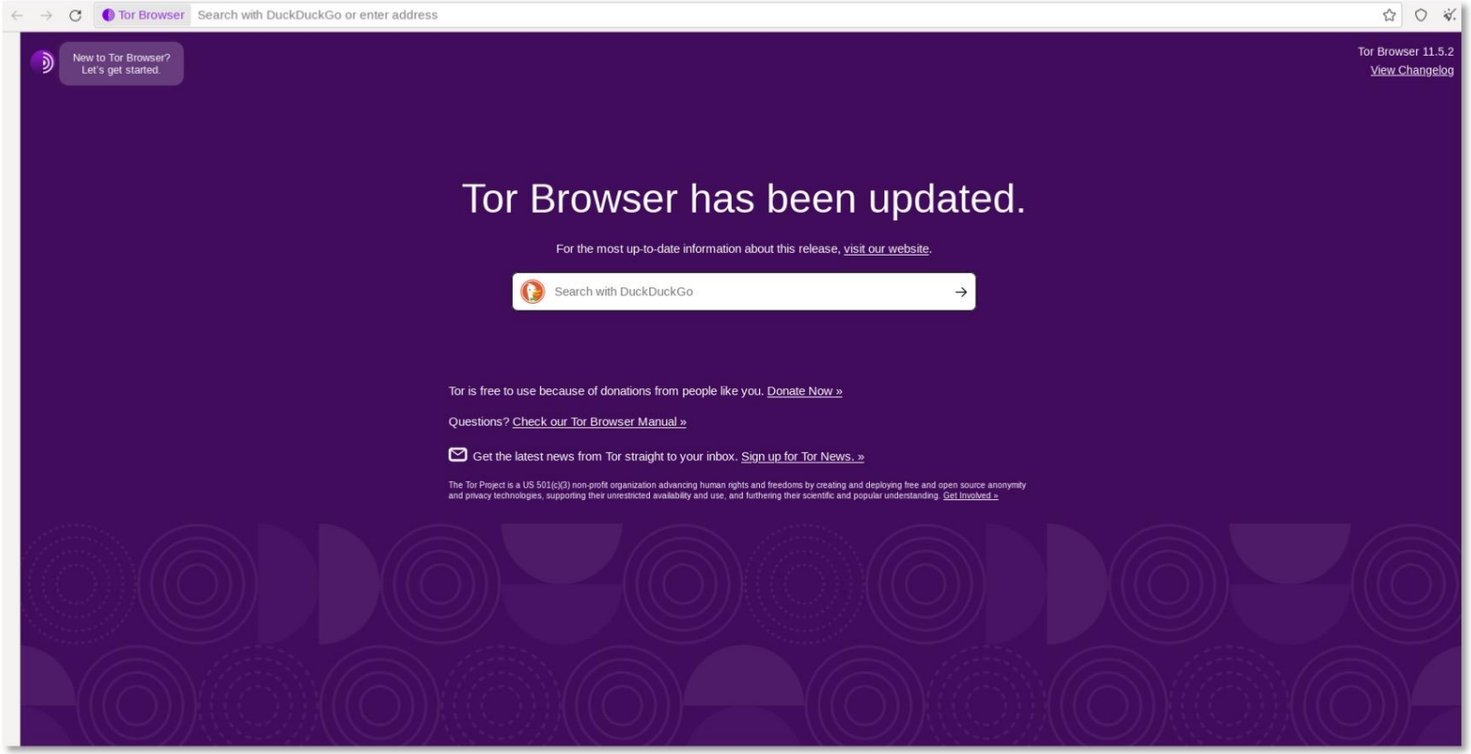
**다크웹은 특수한 브라우저 ‘Tor Browser’을 통해서만 접근 가능**

Firefox



# (3) 해커들의 무대. 딥/다크웹 공간이란?

## ‘Tor Browser’ 메인 화면




**n3rnu4upio2b64g6gyw4dwboajmuyqarvlan4r3tgcemzy6ccjgveuad.onion**

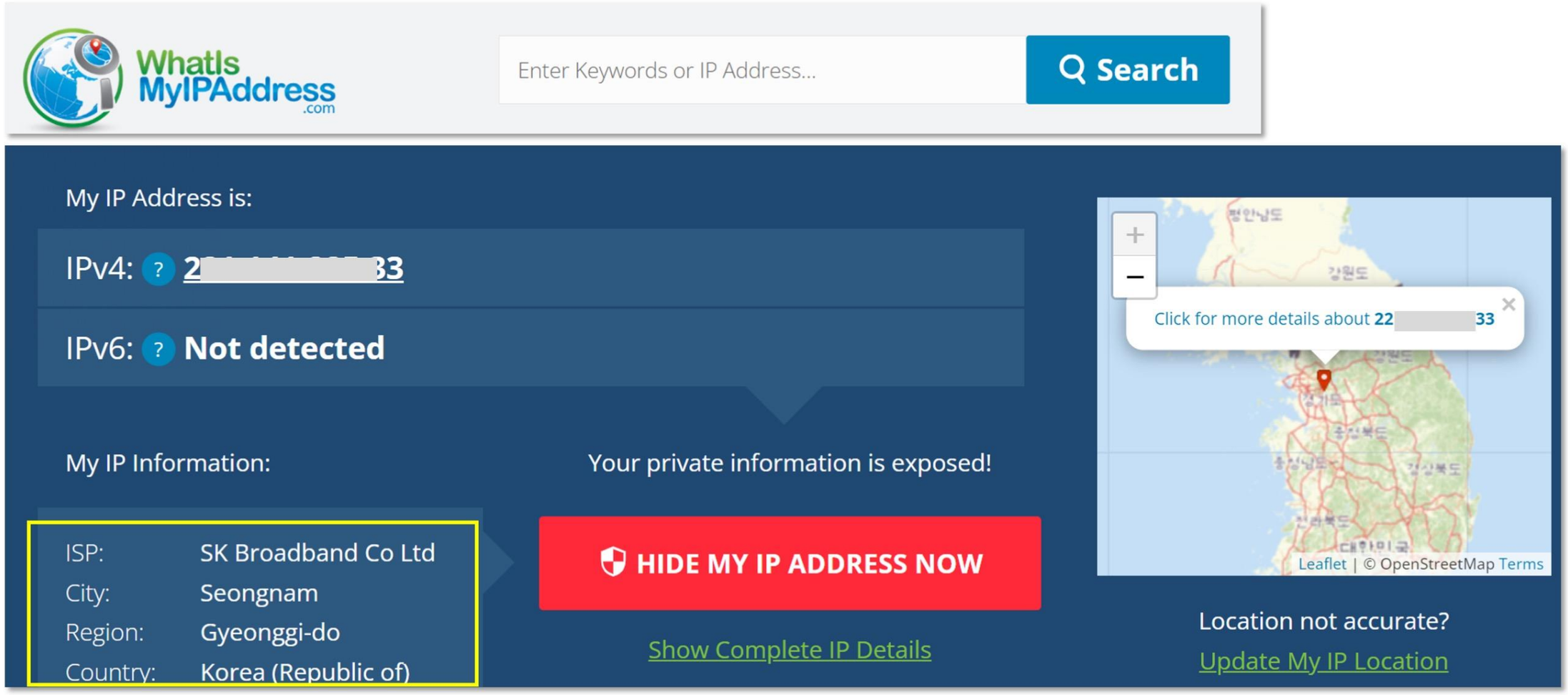
**fdh6mpolzifswuemp3pz67fwvre5t2kmyhr63htymcjh5e5murnfcmqd.onion**

**다크웹 접속에 사용되는 TOR 브라우저**

**일반적인 사이트와는 달리 다크웹 사이트들은 56개의 알파벳과 숫자의 조합으로 이루어진 사이트 주소를 가지고 있음**

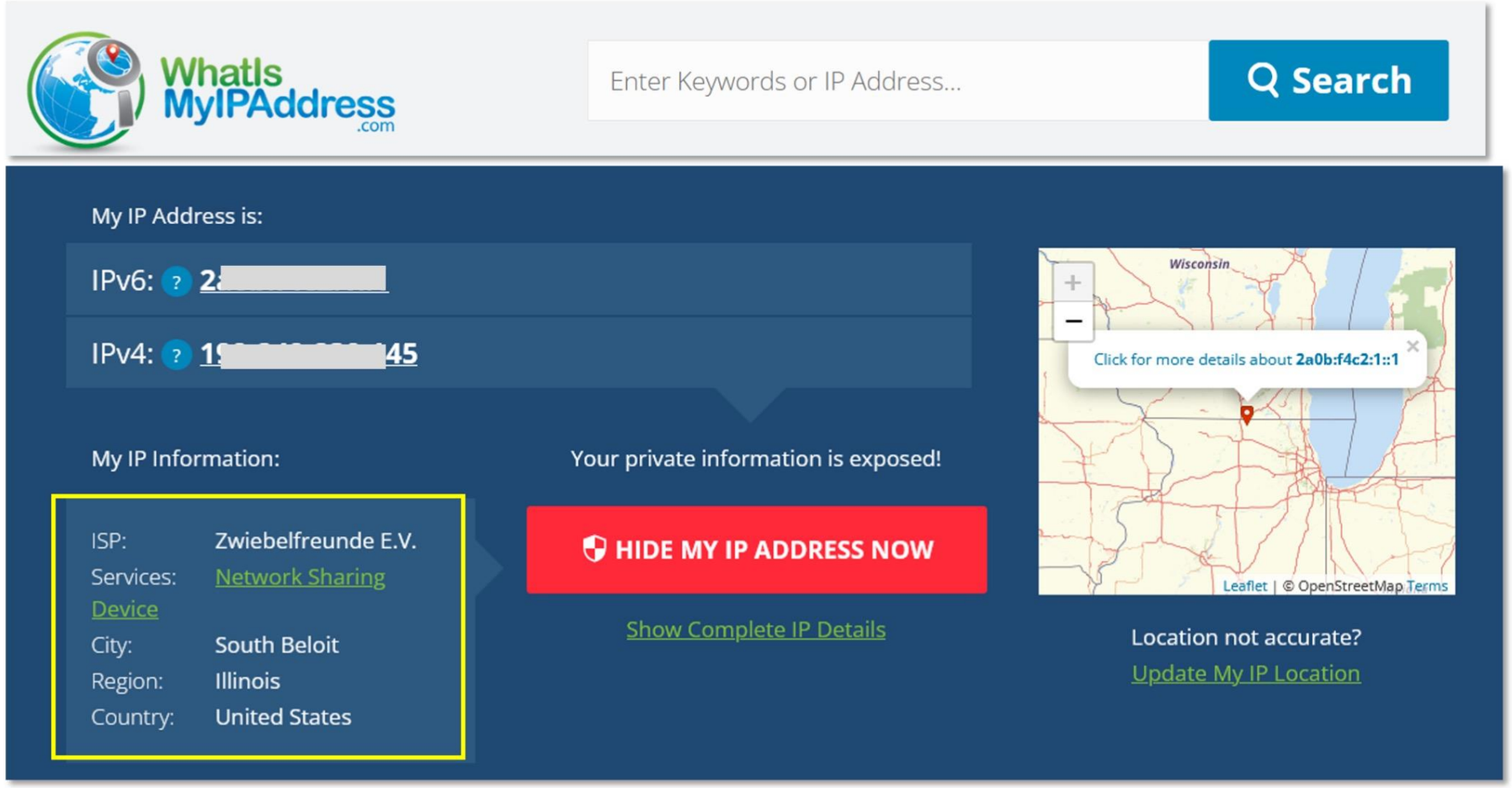
# (3) 해커들의 무대. 딥/다크웹 공간이란?

## 일반 웹 브라우저에서 확인한 IP 주소



# (3) 해커들의 무대. 딥/다크웹 공간이란?

## Tor 브라우저에서 확인한 IP 주소



# (3) 해커들의 무대. 딥/다크웹 공간이란?

## 블랙 마켓 형성을 위한 사이버 범죄 에코 시스템 형성

1.코인보유

미미샵은 대마초를 현금으로 매매하지 않습니다
비트코인이라는 것과 교환하는 시스템입니다 따라서 대마초를 나눔 받으려면 비트코인을 준비하셔야 합니다
코인보유는 국내거래소 및 해외거래소에서 구매 가능합니다

Have PayPal account. Even WU & prepaid cards

Payment upfront in Bitcoin only.
Buy an account according to your budget

익명성 보장

암호 화폐 결제


블랙 마켓

**Paypal Transfer! BIG DEAL!!!**

AnonyMiss
January 21 edited August 2016 in Money Transfers

Using hacked and verified paypal accounts to transfer paypal account to account transfer if you are SMART then you can easily dodge paypal and enjoy big free online money from it.

$1200 Transfer = $200 Charges (Payment Only BTC) // [AUTOMATIC PAYMENTS - CLICK HERE to pay $200]

Everything is sent within Finland so no worry about the customs. Payment only BTC
Free shipping!!!!! Orders over 5000€ get a 15% discount.

#26147

떨 12 액상 15 아이스 35 케이 35 캔디 9 비트코인만 받고

# (3) 해커들의 무대. 딥/다크웹 공간이란?

## 불법 컨텐츠는 매일 쏟아져 나오고 있음

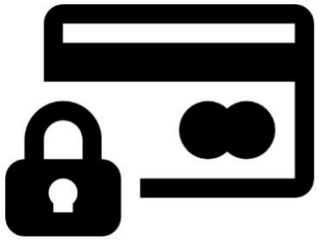
마약

해킹

암호화폐 세탁

***불법 컨텐츠는 그 유형이 매우 다양함***

총기 & 장물



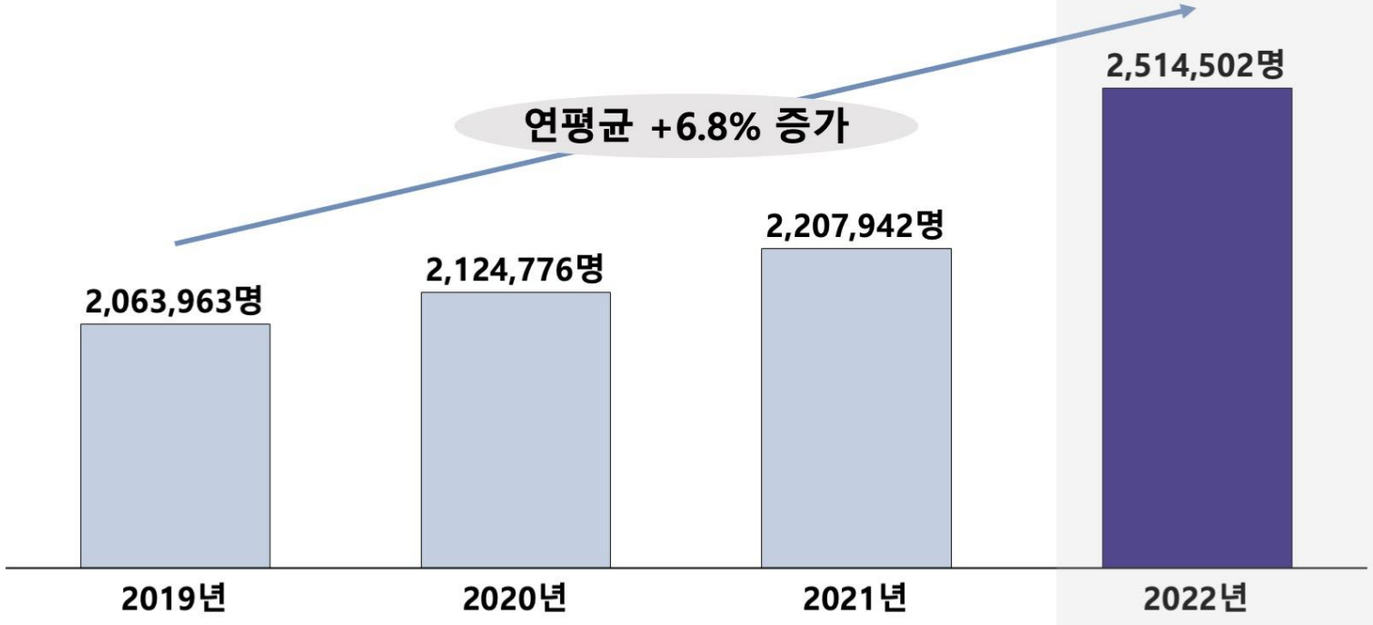
금융 범죄

카지노 & 불법도박

# (3) 해커들의 무대. 딥/다크웹 공간이란?

## 글로벌 다크웹 유저: 다크웹 접속자 수는 꾸준한 상승 추세

**2019 – 2022 전세계 일평균 다크웹 접속자**

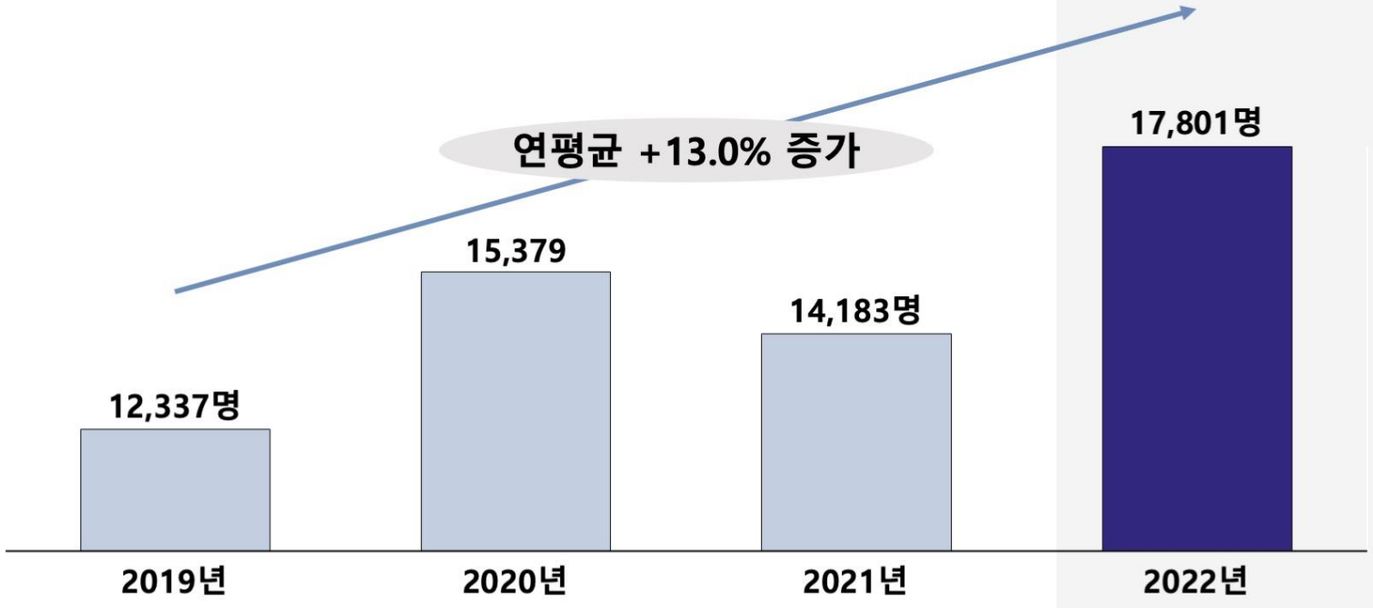



***일평균 접속자***
***250만명 돌파***

# (3) 해커들의 무대. 딥/다크웹 공간이란?

## 국내 다크웹 유저: 다크웹 접속자 수도 글로벌과 유사한 추이

**2019 – 2022 국내 일평균 다크웹 접속자**




***일평균 접속자***
***1.78만명 돌파***

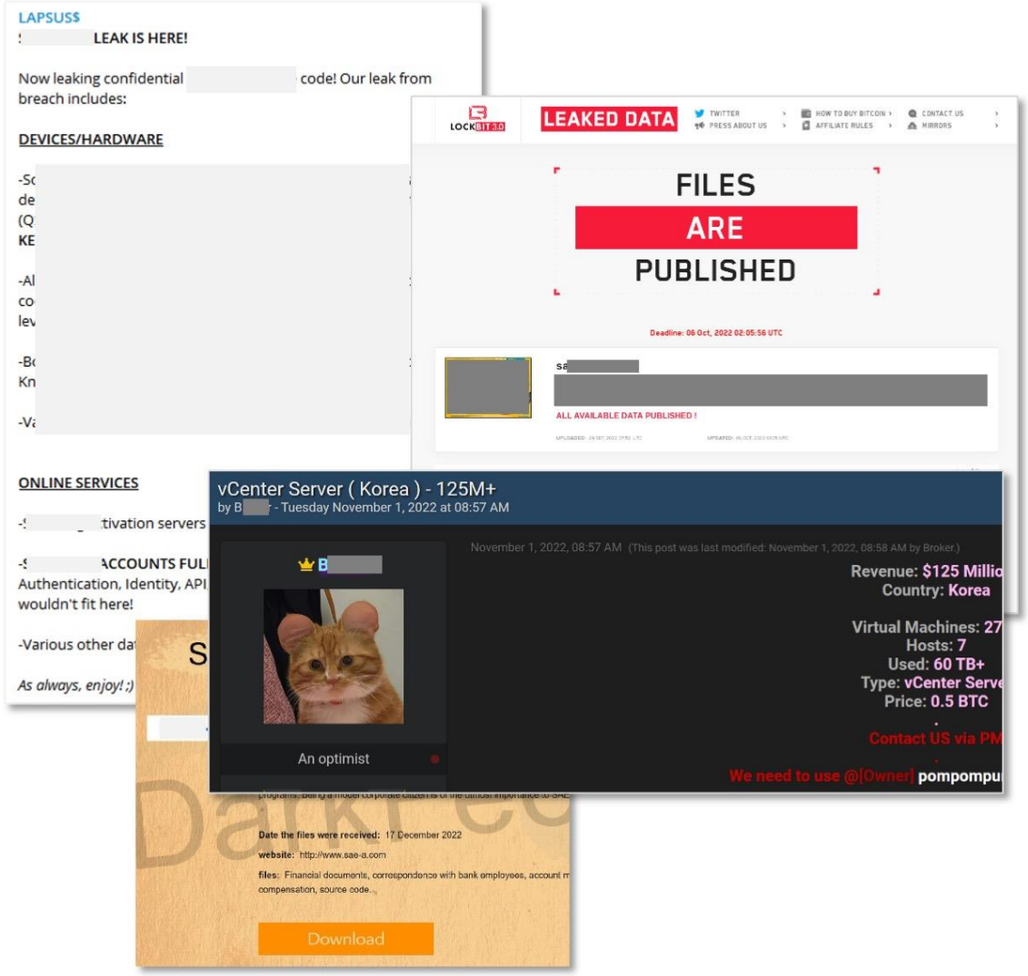
# (3) 해커들의 무대. 딥/다크웹 공간이란?

## 딥&다크웹 내 국내 관련 사건/사고는 과거와 비교해 현격히 증가

**다크웹 내 국내 데이터 유출 사고**

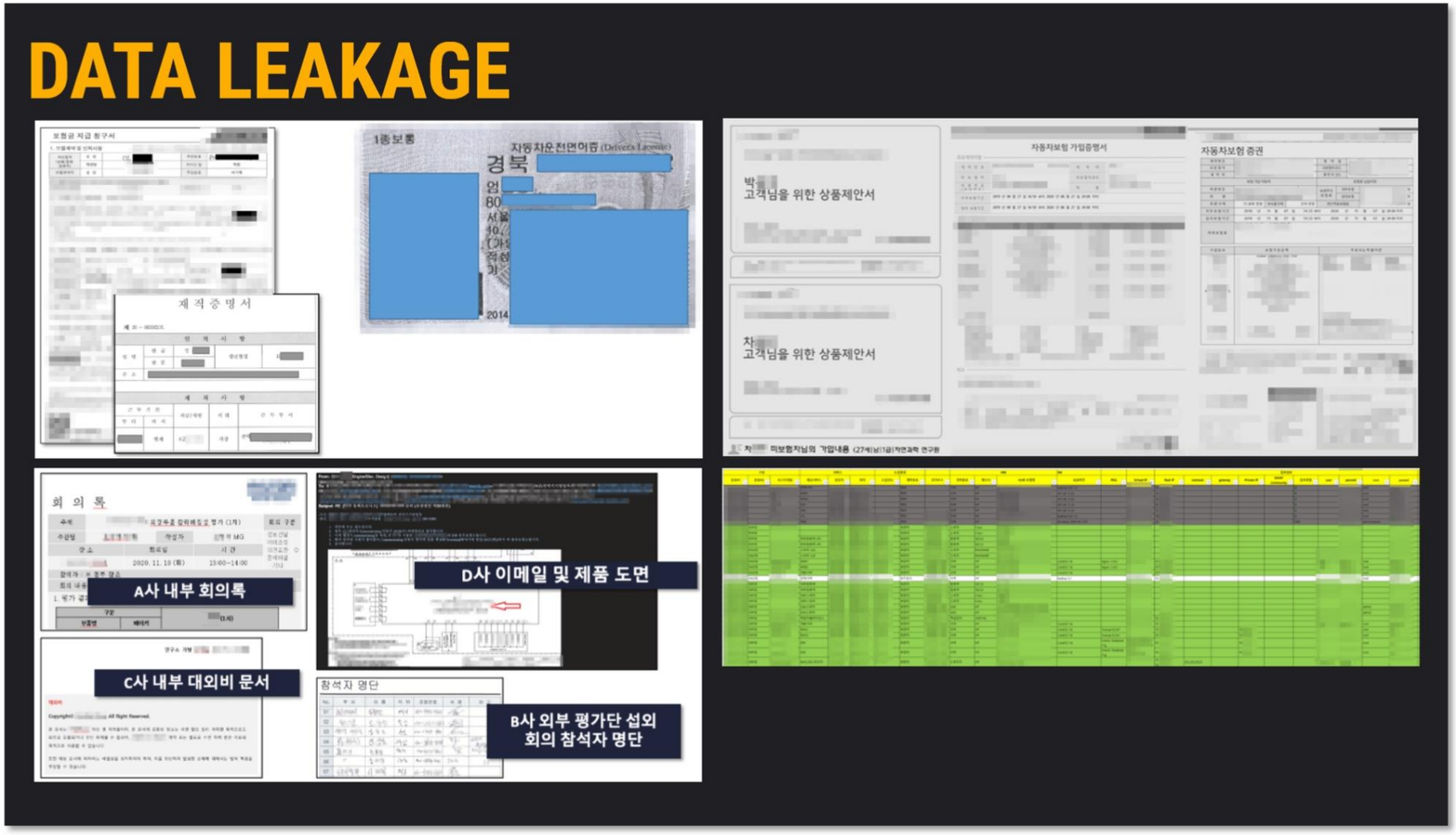
| 2020년 | | 2022년 |
|---|---|---|
| 매주<br>1~2개 | *Vs.* | 매주<br>**7~8개** |

**평균적으로 매일 1~2건 이상**
**국내 관련 사건/사고가 발생 중**



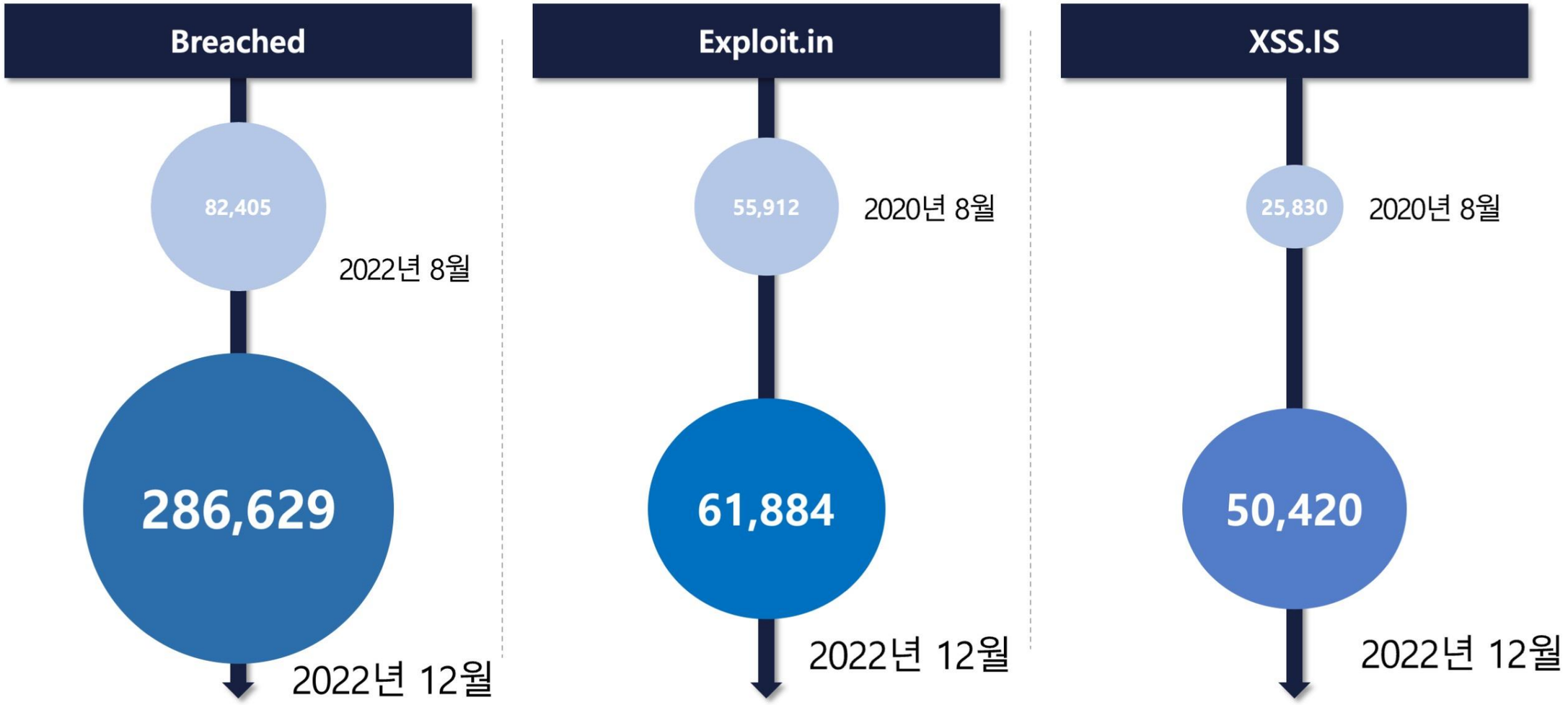
# (3) 해커들의 무대. 딥/다크웹 공간이란?

## 유출된 파일에는 기업 기밀 자료, 민감 개인 정보, 소스코드, 도면 등 매우 다양함



# (4) 다크웹 최신 동향_사이버 범죄 공간 확대

## 딥/다크웹 3대 해킹 포럼의 유저 수 급증

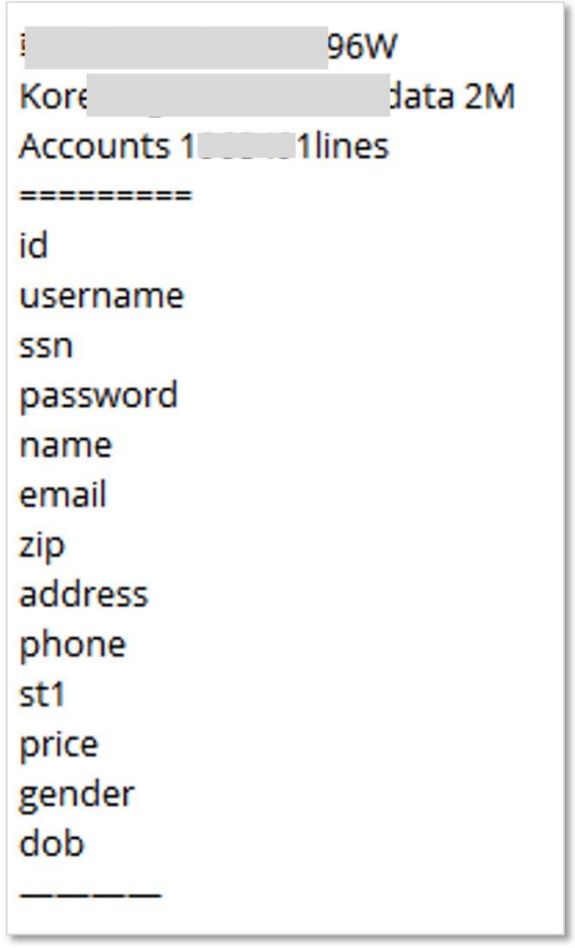


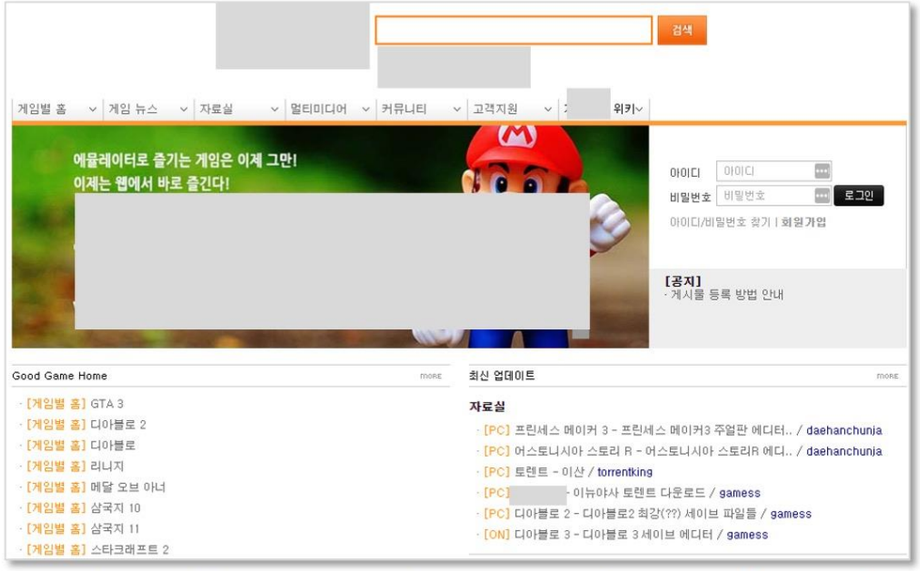
# (4) 다크웹 최신 동향_사이버 범죄 공간 확대

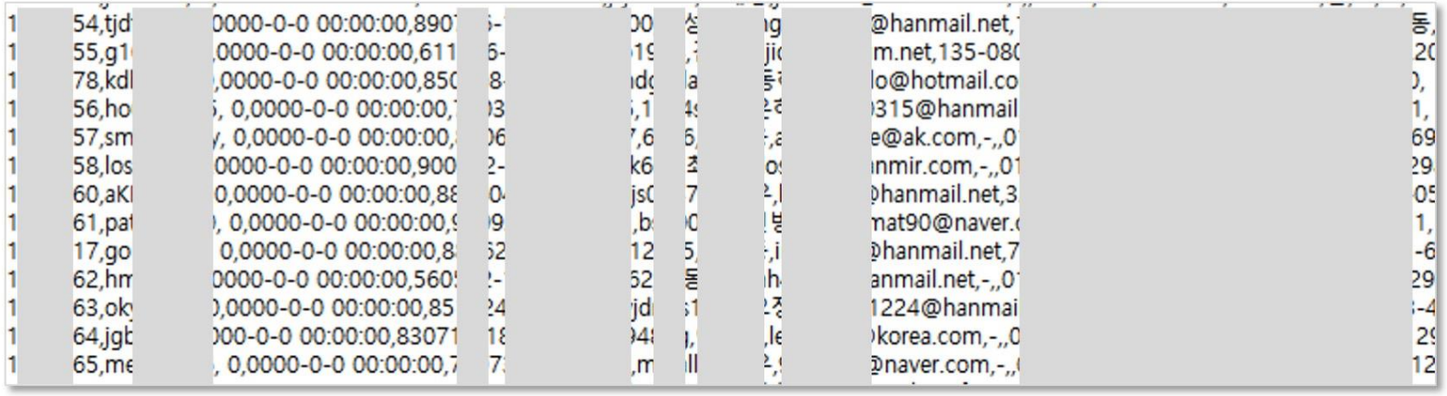
## 다크웹 + 텔레그램 채널로 사이버 범죄 공간 확대

# (4) 다크웹 최신 동향_사이버 범죄 공간 확대

## 사건 1) 국내 웹사이트 '게***'에 가입한 200만 명 회원 개인 정보 유출



# (4) 다크웹 최신 동향_사이버 범죄 공간 확대

## 사건 2) 해킹 그룹 'LAPSUS$', 국내 대기업의 내부 자료 유출

LAPSUS$

**LEAK IS HERE!**

Now leaking confidential S source code! Our leak from breach includes:

**DEVICES/HARDWARE**

-Source code for every Trusted Applet (TA) installed on all sa g device's Tr TEE) with specific code for every type of TEE OS (Q c) **THIS INCLUDES DRM MODULES AND KEYMASTER/GATEKEEPER!**

-Algorithms for all biometric unlock operations, including source code that communicates directly with sensor (down to the lowest level, we're talking individual RX/TX bitstreams here)

-B source code for all recent Sa g devices, including Knox data and code for authentication.

-Various other data, confidential source code from Q m.

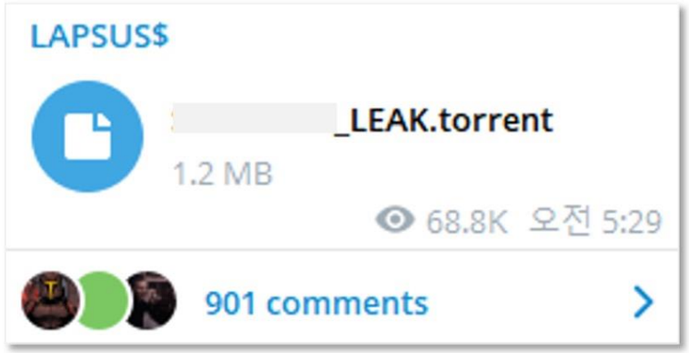
**ONLINE SERVICES**

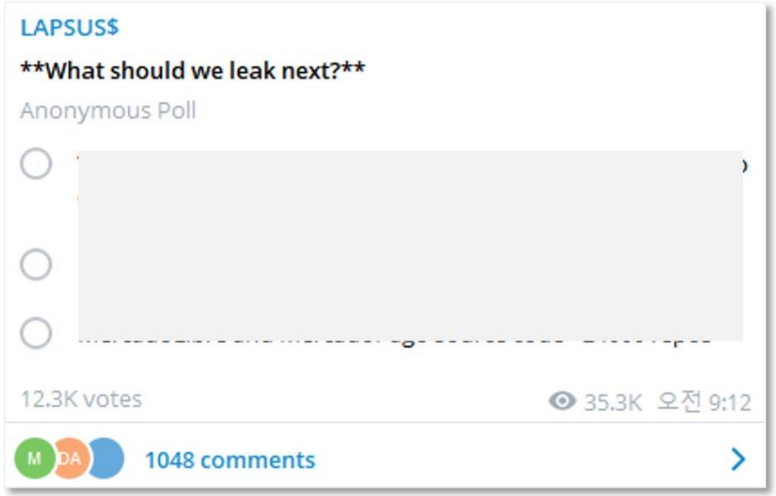
-S ctivation servers source code (for first-time setup)

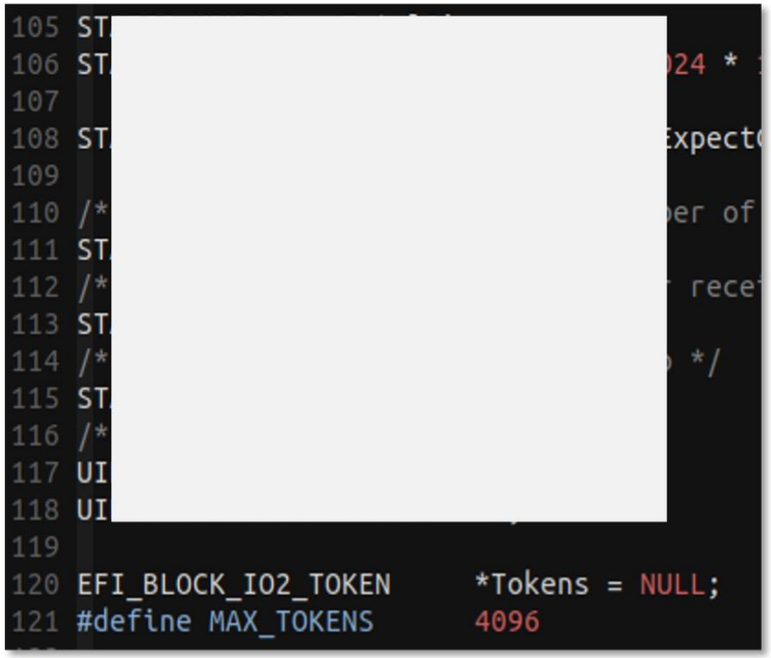
-S **ACCOUNTS FULL SOURCE CODE!** Including Authentication, Identity, API, Services, and many more that wouldn't fit here!

-Various other data.

*As always, enjoy! ;)*



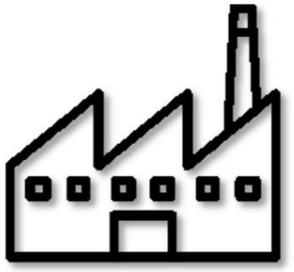



# (4) 다크웹 최신 동향_특정 산업이나 국가를 공격하는 유저/집단

## 특정 산업이나 특정 국가를 집중적으로 공격하는 해킹 그룹 및 유저 등장

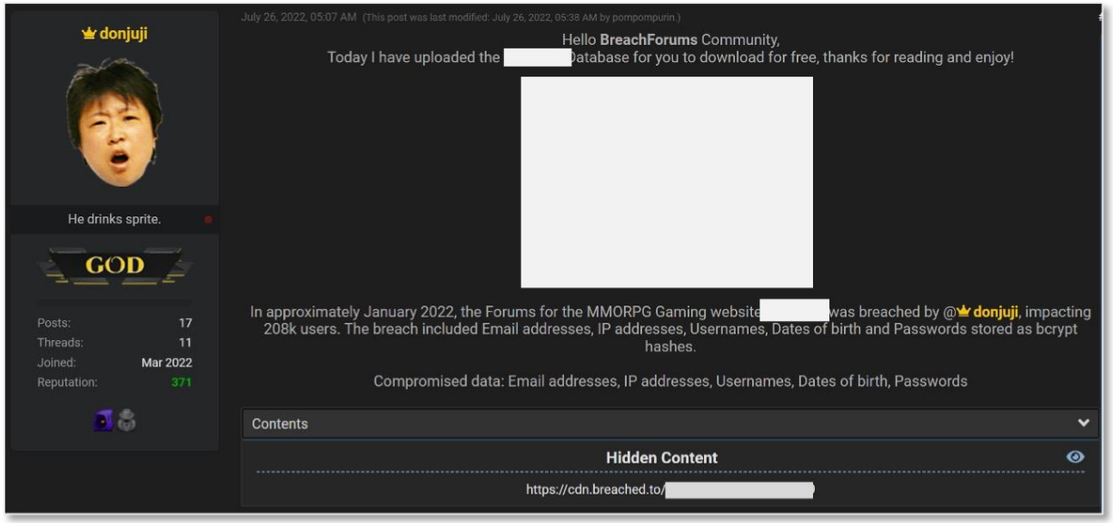
Set target
and Attack



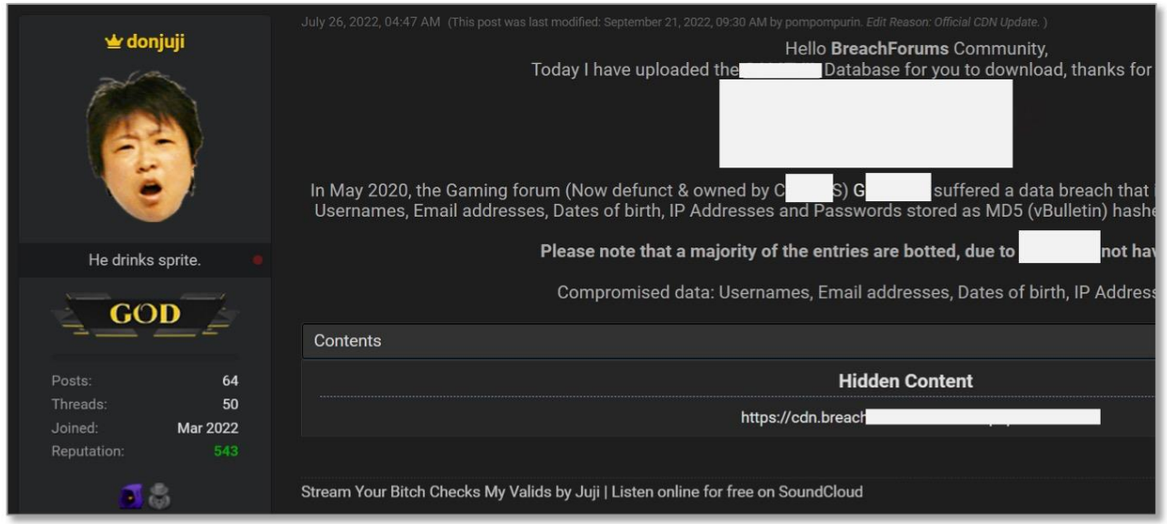
# (4) 다크웹 최신 동향_특정 산업이나 국가를 공격하는 유저/집단

## 사건 1) 유명 해킹 포럼 내에서 국내 게임사를 타겟하여 공격하던 유저 포착

[redacted] Database - Leaked, Download!
by donjuji - Tuesday July 26, 2022 at 05:07 AM

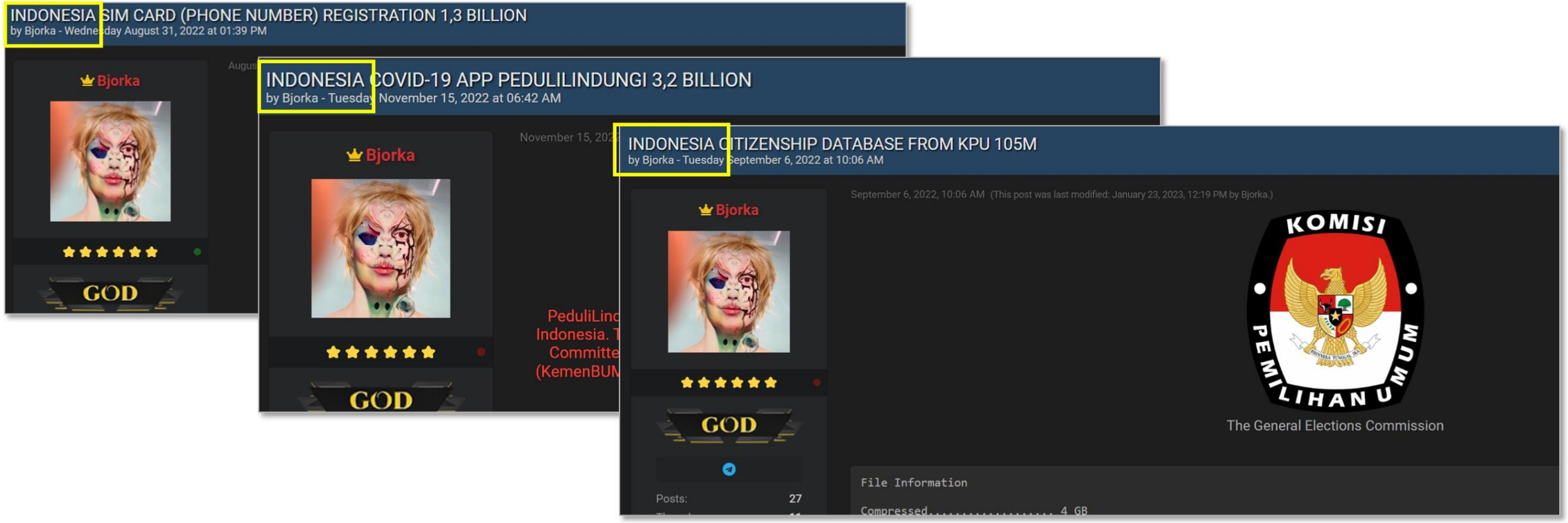


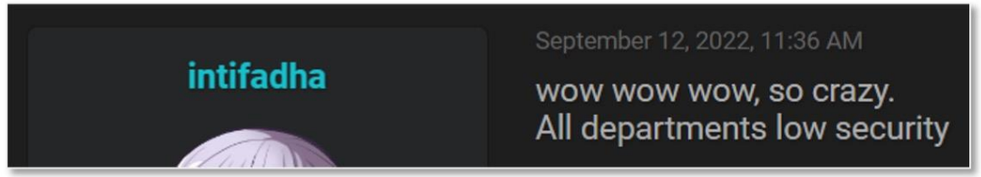

[redacted] Database - Leaked, Download!
by donjuji - Tuesday July 26, 2022 at 04:47 AM

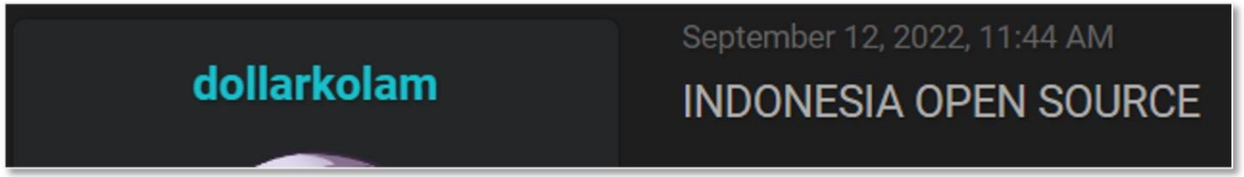


# (4) 다크웹 최신 동향_특정 산업이나 국가를 공격하는 유저/집단

## 사건 2) 인도네시아를 집중 타격하는 유저 등장

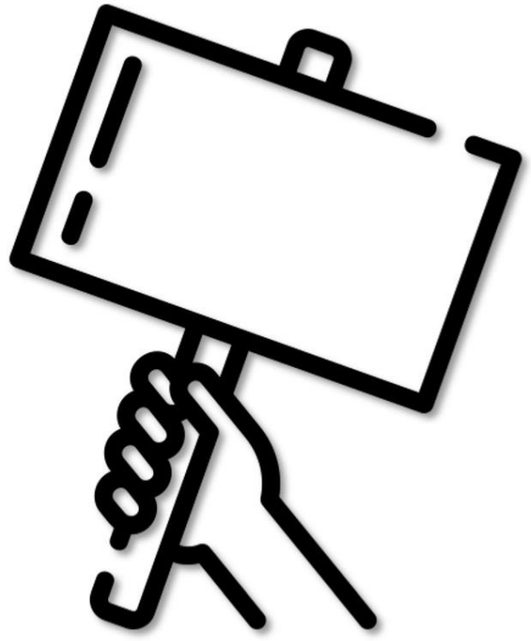


# (4) 다크웹 최신 동향_핵티비즘 활동 증가

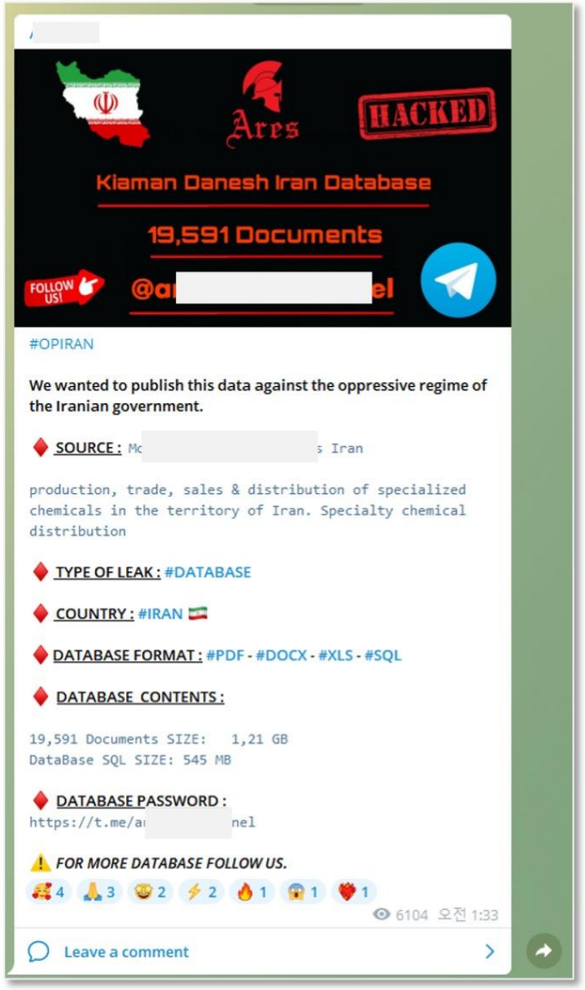
## 반정부 성향을 사이버 공격을 통해 표출

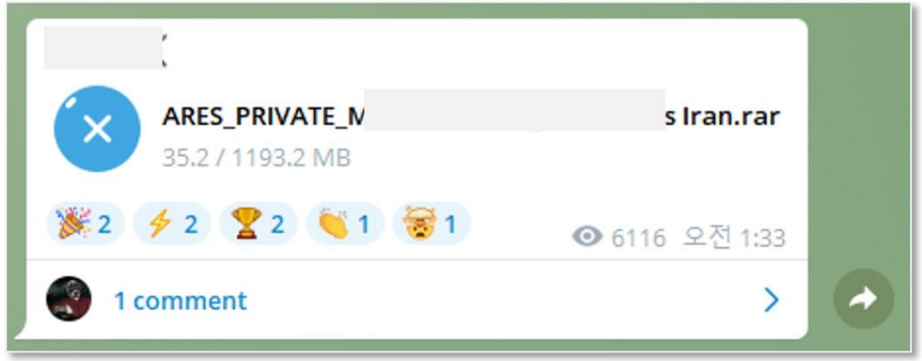


***Hacking (해킹) + Activism (정치행동주의) = Hacktivism***

# (4) 다크웹 최신 동향_핵티비즘 활동 증가

## 사건 1) 히잡 시위를 지지하며 이란 정부를 비판하기 위한 사이버 활동 개시

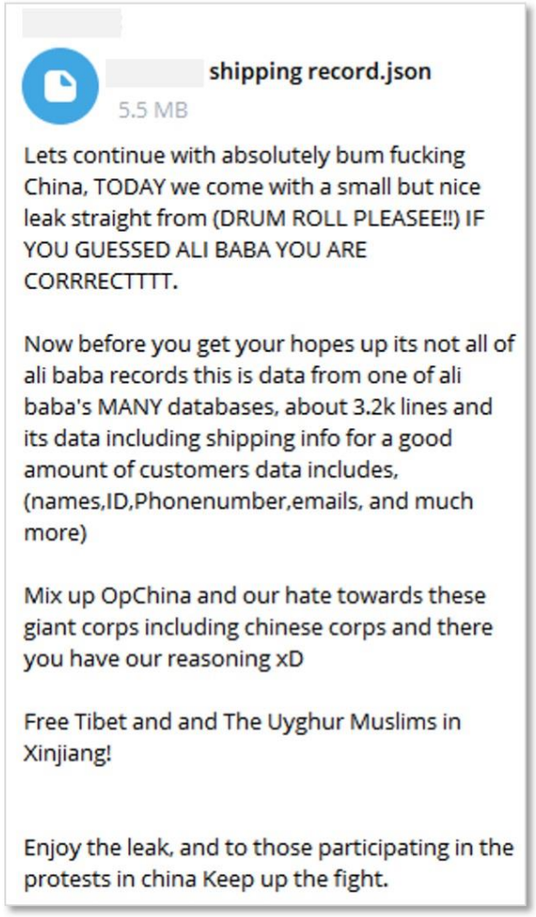




# (4) 다크웹 최신 동향_핵티비즘 활동 증가

## 사건 2) 中 특정 지역 인권의 해방을 촉구하는 명목 하에 '알리바바' DB 유출



shipping record.json
5.5 MB

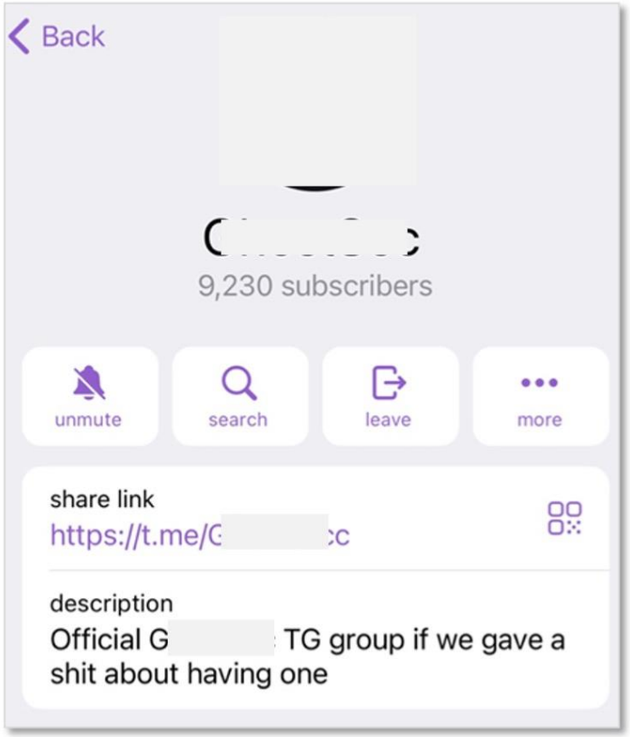
Lets continue with absolutely bum fucking China, TODAY we come with a small but nice leak straight from (DRUM ROLL PLEASEE!!) IF YOU GUESSED ALI BABA YOU ARE CORRRECTTTT.

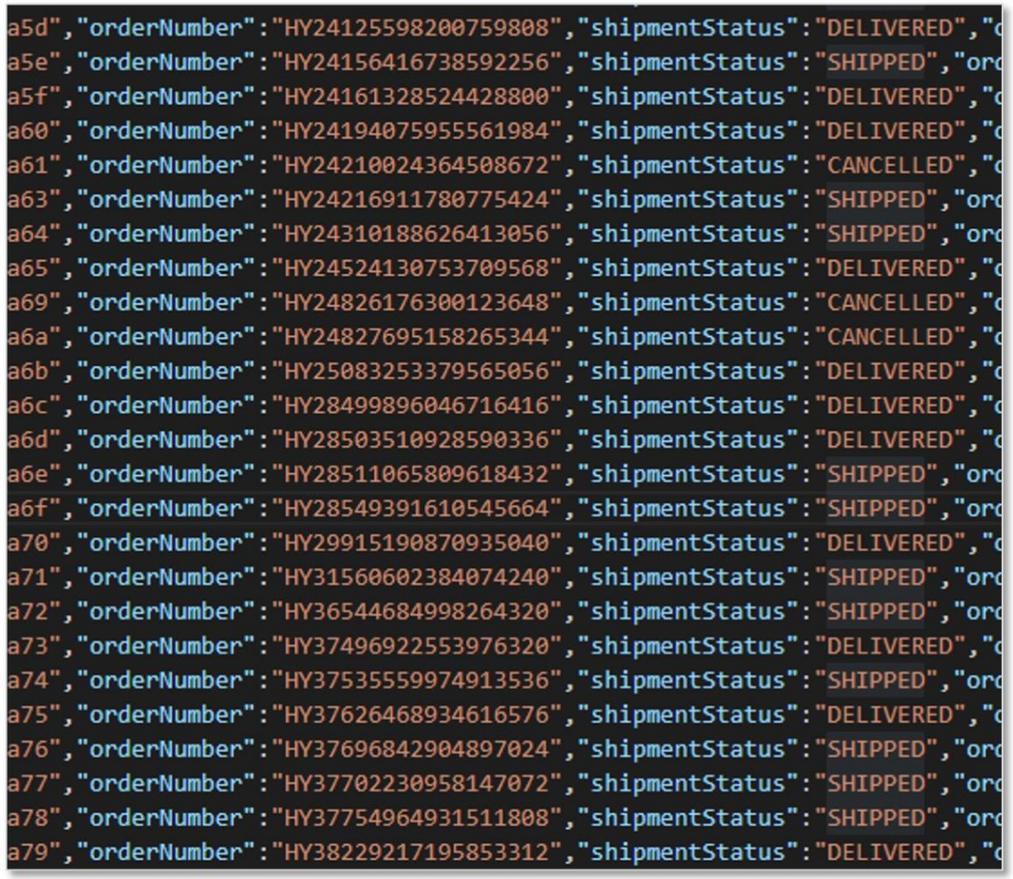
Now before you get your hopes up its not all of ali baba records this is data from one of ali baba's MANY databases, about 3.2k lines and its data including shipping info for a good amount of customers data includes, (names,ID,Phonenumber,emails, and much more)

Mix up OpChina and our hate towards these giant corps including chinese corps and there you have our reasoning xD

Free Tibet and and The Uyghur Muslims in Xinjiang!

Enjoy the leak, and to those participating in the protests in china Keep up the fight.



# (4) 다크웹 최신 동향_정부 및 군사

**정부 및 군사 유출 사건 관련 사고가 지속적으로 가장 많은 비중을 차지하고 있음**

# (4) 다크웹 최신 동향_정부 및 군사

## 사건 1) 중국 상하이 공안 데이터베이스 유출, 약 10 BTC (2.6억원)에 판매

**2022 - SHGA Shanghai Gov National Police database**
by ChinaDan - Thursday June 30, 2022 at 08:55 AM

ChinaDan

BreachForums User

MEMBER

| | |
|---|---|
| Posts: | 1 |
| Threads: | 1 |
| Joined: | Jun 2022 |
| Reputation: | 0 |

39 minutes ago (This post was last modified: 39 minutes ago by ChinaDan.)

In 2022, the Shanghai National Police (SHGA) database was leaked. This database contains many TB of data and information on Billions of Chinese citizens.

Sell: Shanghai GOV (SHGA.gov.cn) National Police Database

Host: http://d[redacted].sh/
Data leaked from these tables:

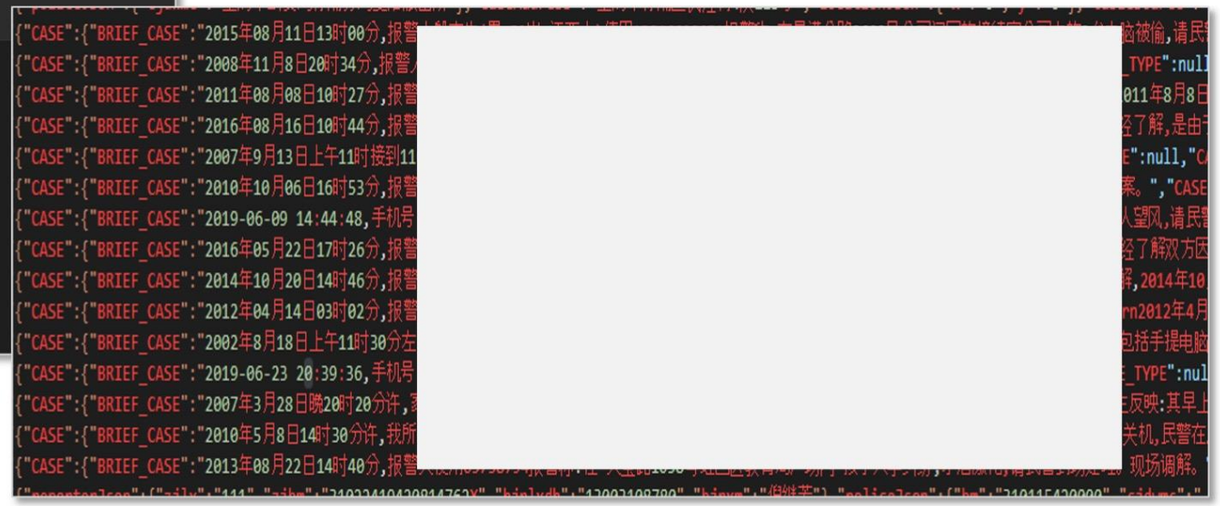
```
----TABLES----
person_address_label_info_slave QFpD25bKTJ2eQBxcbe2Aaw 90 0 546148916 0 172.2gb 172.2gb
nb_theme_address_merge_tracks_slave -bUMVB1uRRusUbbqZepEpA 300 0 37483779369 4 22.4tb 22.4tb
nb_theme_address_case_dwd_test 7COIWTt7QU-YPwWub8z_SQ 150 0 22375506 1749307 25.2gb 25.2gb
nb_theme_address_company_dwd-total fpnmEYB9SI6WevHnZIEwIA 150 0 1842856 0 2.8gb 2.8gb
nb_theme_address_case_dwd-total 7X8oNqULQnWFLpzHDaUTbg 150 0 1214119253 0 1tb 1tb
nb_theme_address_company_dwd_test g5f6l4LGQcGL3oQ6ON2Bbw 150 0 2017931 0 4.3gb 4.3gb
person_address_label_info_master t64pp9WnS3maY9jBjzTtiw 90 0 969830088 0 282.8gb 282.8gb
```

**Data Details:**

Databases contain information on 1 Billion Chinese national residents and several billion case records, including:
- Name
- Address
- Birthplace
- National ID Number
- Mobile number
- All Crime / Case details

Sample of 3 main databases: https://gofile.io/d/WIFNj0

PRICE: I am selling all of this data for 10BTC ($200k USD)



# (4) 다크웹 최신 동향_정부 및 군사

## 사건 2) 미국 주요 정부 기관 (FBI, 해군, 공군 등)의 내부 문서 탈취 후 판매

[SOLD] US GOVERNMENT RANSOMWARE BREACH
by IntelBroker - Tuesday November 15, 2022 at 04:13 PM

IntelBroker

the racist

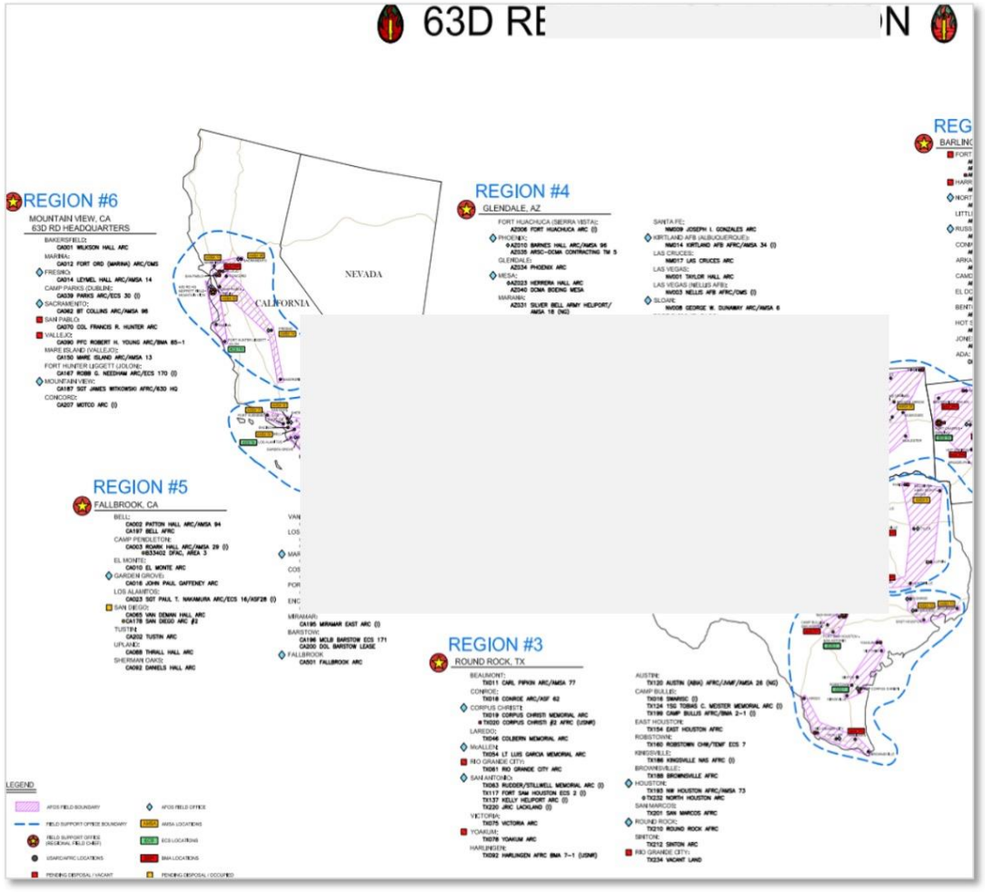
GOD

| | |
|---|---|
| Posts: | 482 |
| Threads: | 118 |
| Joined: | Oct 2022 |
| Reputation: | 2,033 |

November 15, 2022, 04:13 PM (This post was last modified: November 20, 2022, 03:30 PM by IntelBroker.)

Today, the Federal government of the United States fell victim to the Endurance Ransomw
it.
So I am posting this thread in an attem
(My ransomware has already been found

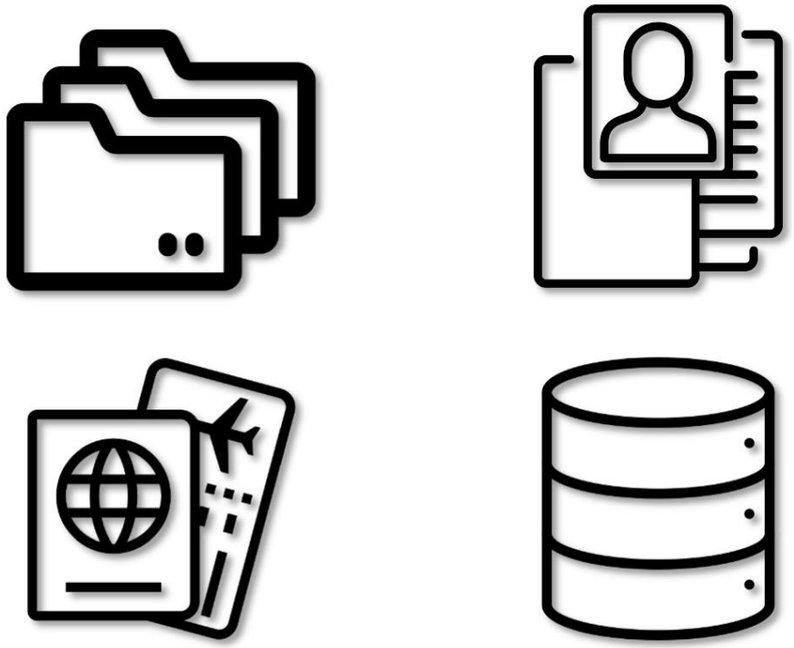
BREACH SAMPLES
353 page PDF
https://[redacted]df

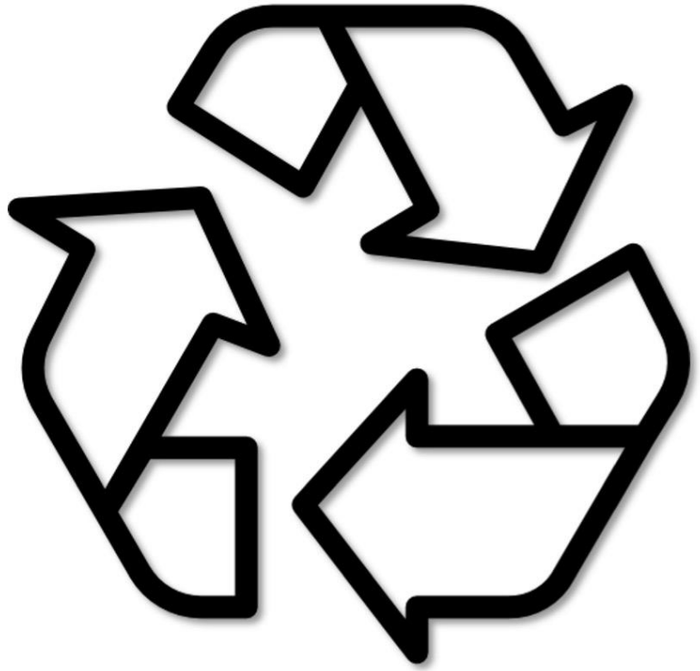


# (4) 다크웹 최신 동향_데이터의 끊임없는 재유출

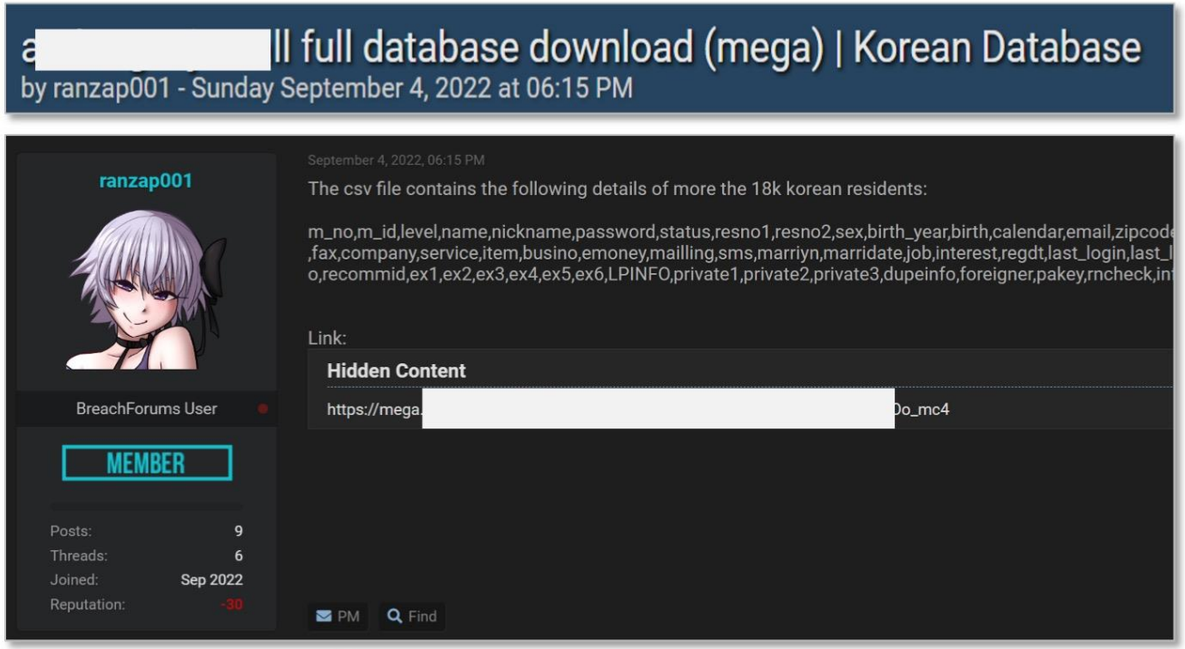
**1차 데이터 유출 이후 2차, 3차 재공유되는 데이터**

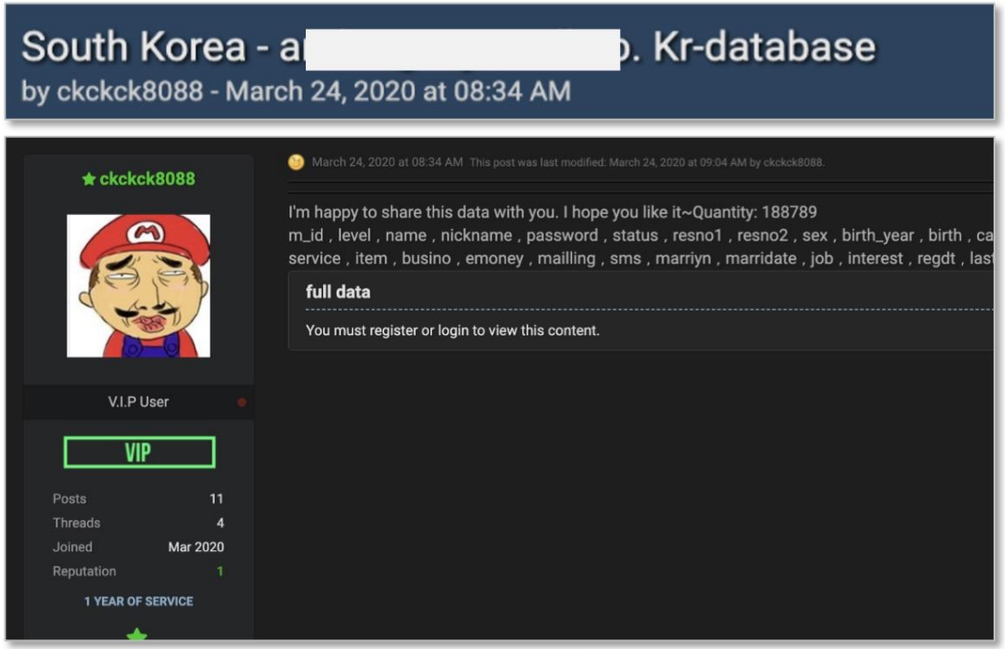


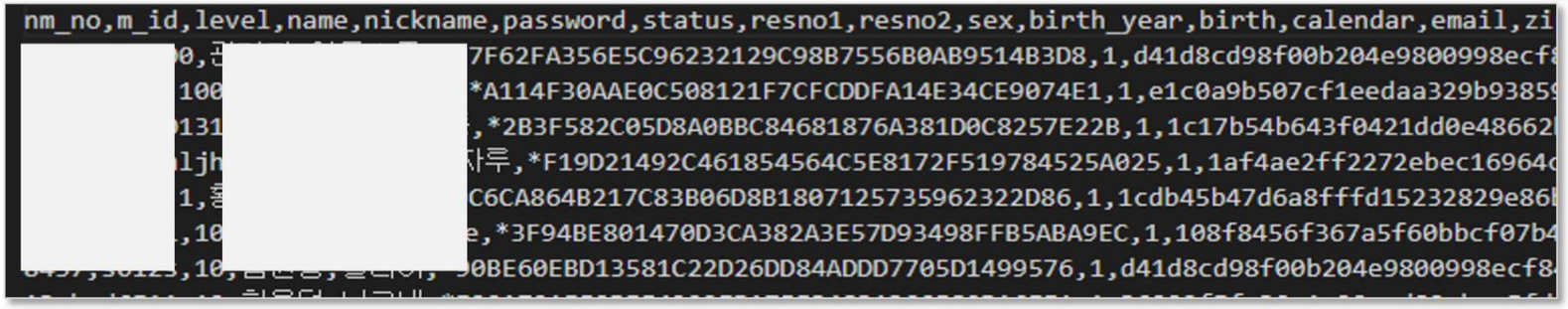


# (4) 다크웹 최신 동향_데이터의 끊임없는 재유출

## 국내 온라인 주류 쇼핑몰 데이터, 과거 유출된 데이터의 재공유

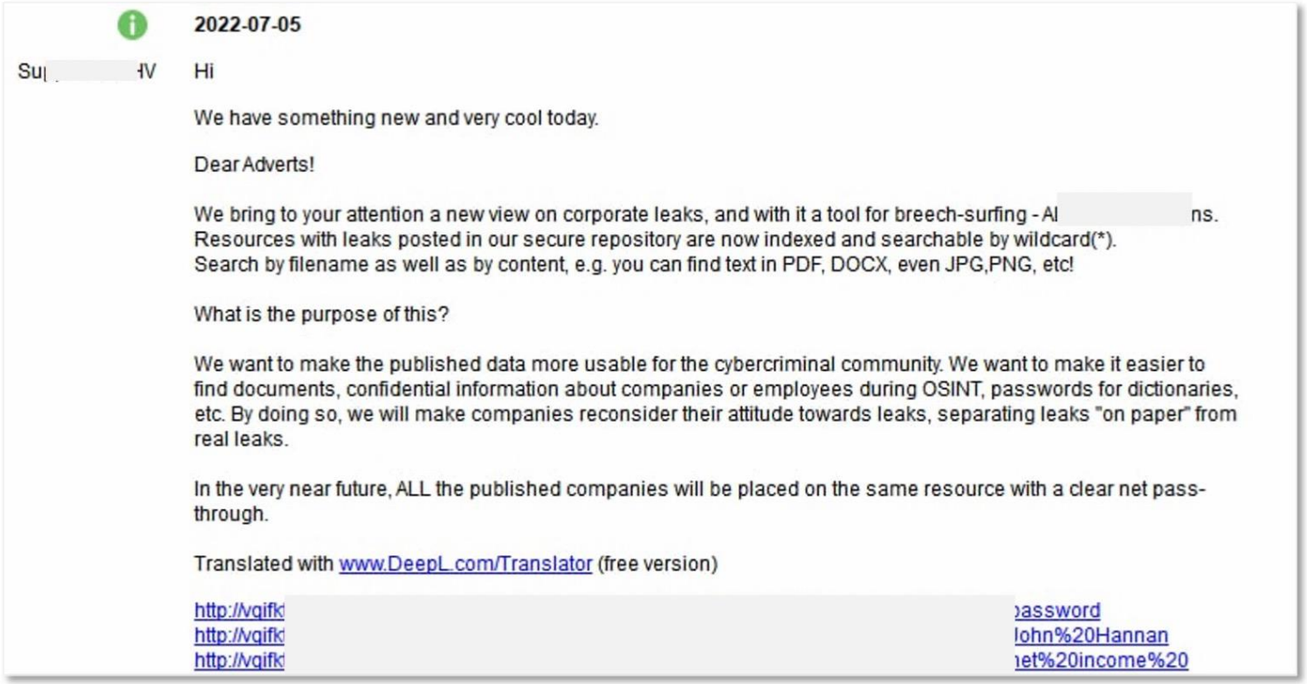


# (4) 다크웹 최신 동향_데이터의 끊임없는 재유출

## ALPHV(BlackCat) 랜섬웨어 onion 사이트



2022-07-05

Su[ ]V Hi

We have something new and very cool today.

Dear Adverts!

We bring to your attention a new view on corporate leaks, and with it a tool for breech-surfing - Al ns.
Resources with leaks posted in our secure repository are now indexed and searchable by wildcard(*).
Search by filename as well as by content, e.g. you can find text in PDF, DOCX, even JPG,PNG, etc!

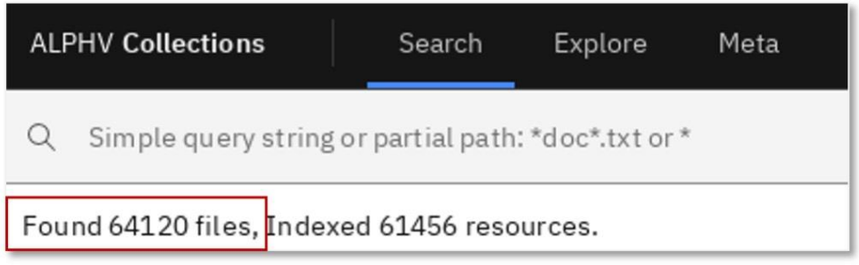
What is the purpose of this?

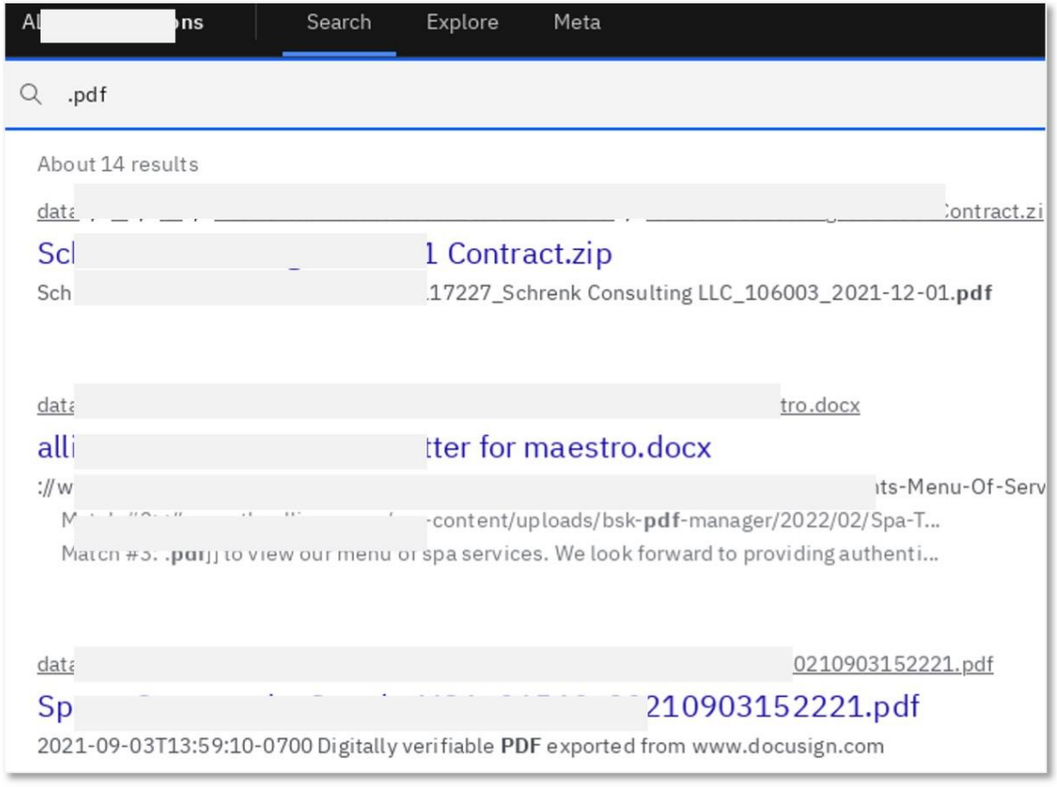
We want to make the published data more usable for the cybercriminal community. We want to make it easier to find documents, confidential information about companies or employees during OSINT, passwords for dictionaries, etc. By doing so, we will make companies reconsider their attitude towards leaks, separating leaks "on paper" from real leaks.

In the very near future, ALL the published companies will be placed on the same resource with a clear net pass-through.

Translated with www.DeepL.com/Translator (free version)

http://vqifk[ ]assword
http://vqifk[ ]lohn%20Hannan
http://vqifk[ ]et%20income%20



# (5) 정리

해킹 포럼 회원 수, 다크웹 페이지 수, 일평균 다크웹 유저 수 모두 증가세

대응도 중요하지만, 사건 사고에 대한 예방도 중요함

S2W

Safe and Secure World


## 김다솜

**위협 분석가**

사이버 위협 탐지 및 대응 관련 연구개발

3. Account Take Over Scenario

# 임직원 및 협력사 계정 유출 주요 시나리오 및 대응 방법

김다솜, Threat Detection

# 목차

- S2W 위협분석센터 위협탐지팀 소개
- 전세계 계정 유출 현황
- 주요 계정 유출 시나리오
- 계정 유출 대응 방안

# Talon

## Center for
## Threat Research & Intelligence

# 위협탐지팀 | Threat Detection Team (a.k.a HOTSAUCE)

위협탐지팀은 다크웹, 텔레그램 등에서 일어나는 사이버 범죄 시도와 수법, 데이터 유출 등을 분석해 정부/기업 고객에게 필요한 인사이트를 제공합니다.
팀의 목표는 다양한 소스에서 수집한 대량의 비정형 데이터에서 필요한 정보를 빠르게 찾아내는 작업의 기술적 자동화를 통해 효과적인 위협 대응 솔루션을 만드는 것입니다.

# 계정 유출 현황

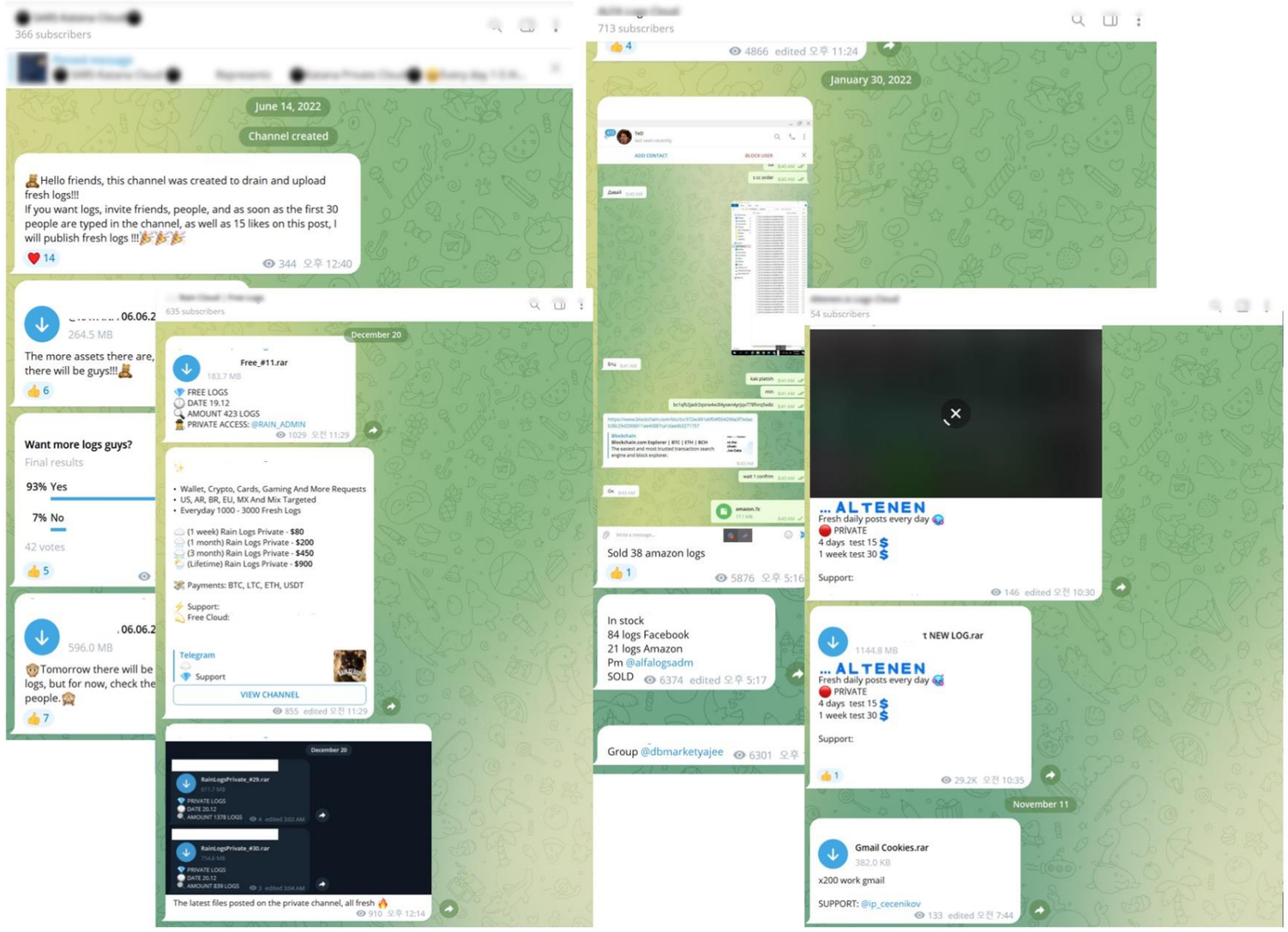
## 스틸러 로그

**2022년 11월 ~ 2023년 2월 (지난 3개월 기준)**

**전체 유출 계정 수**
**10,690,846**

**한국 관련 유출 계정 수**
**감염 IP 국가 Korea 기준
**440,799**

**한국 정부 기관 관련 유출 계정 수**
**감염 IP 국가 Korea 및 gov 관련 키워드 포함
**165,402**



# 계정 유출 현황

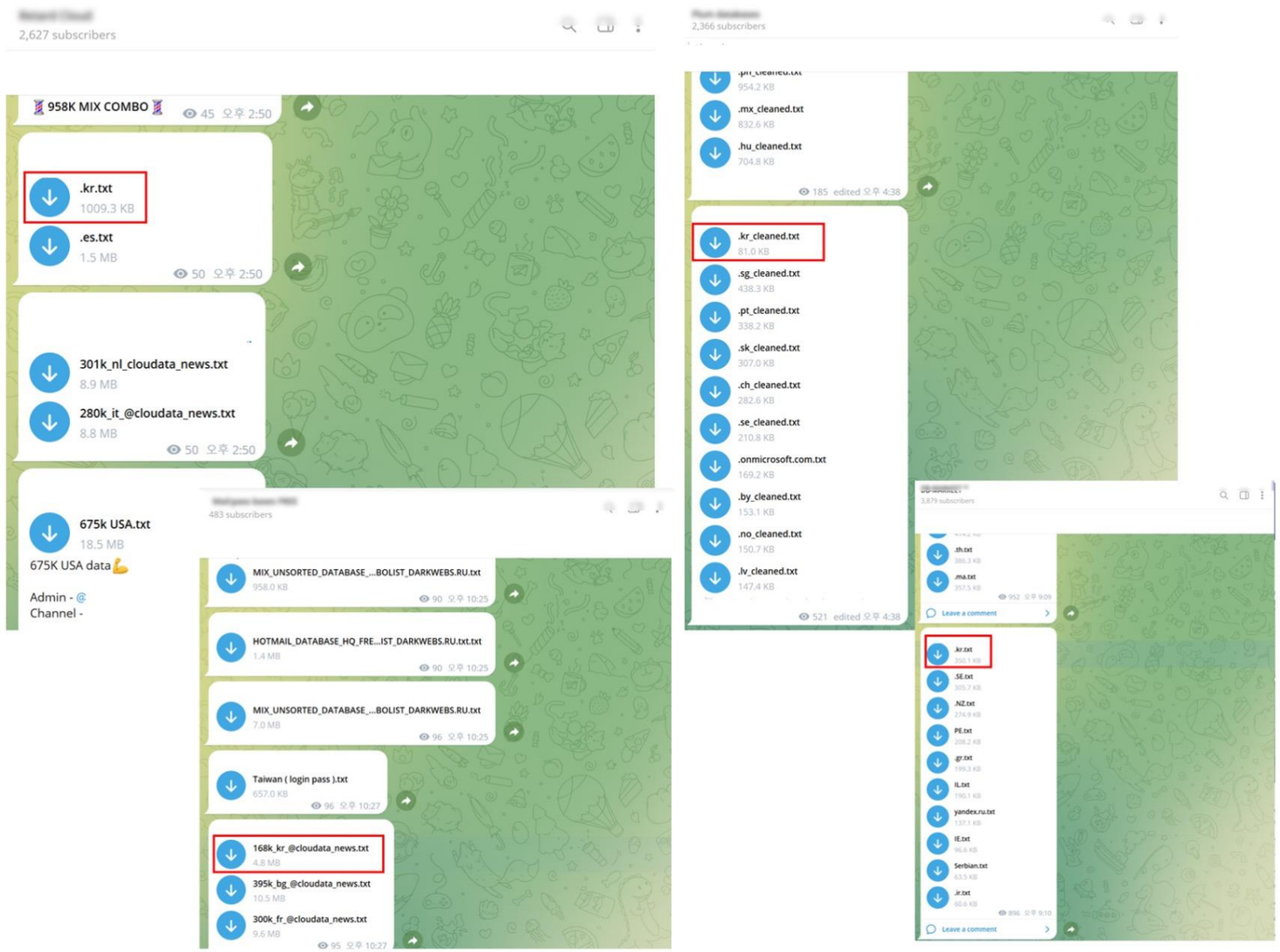
## 데이터베이스 및 계정 덤프 유출

**2022년 11월 ~ 2023년 2월 (지난 3개월 기준)**

**전체 유출 계정 수**
**409,956,208**

**한국 관련 유출 계정 수**
**파일명 kr, korea 관련 키워드 포함
**3,751,341**

**한국 정부 기관 관련 유출 계정 수**
**파일명 kr, korea 및 gov 관련 키워드 포함
**194,235**



# 주요 시나리오

**시나리오 1. GitHub 상에서 임직원 MySQL 계정 정보 유출**

**시나리오 2. GitHub 상에서 마라톤클럽 웹 사이트 유저 개인 정보 유출 (기업 임직원 계정 정보 포함)**

**시나리오 3. 국내 IT 인프라 운영 및 유지보수 업체 임직원의 스틸러 감염으로 인해 기업 민감 정보 유출**

**탐지 케이스. 협력사 임직원의 스틸러 감염으로 인해 기업 민감 정보 유출**

# 배경 및 요약

- 2020년 9월 14일 Github 상에 M 사용자가 “프로젝트 개발시 사용한 React/TS/Nextjs/Nestjs/GraphQL SSR 설정” 라는 내용의 커밋 메세지와 함께 GraphQL 설정값을 업로드함.
- 해당 사용자에 대해서 조사한 결과, LinkedIn 프로필에서 2021년 5월까지 A사에 재직했던 직원임을 확인함.
- 커밋 메시지에서 “프로젝트 개발시 사용한 React/TS/Nextjs/Nestjs/GraphQL SSR 설정”과 코드 내에서 “https://***-mysql-writer.dev.***.**/” 를 언급한 사실을 바탕으로 A사 관련 프로젝트로 판단하였음.

# 시나리오 1. GitHub 상에서 임직원 MySQL 계정 정보 유출

29 lines (27 sloc) | 810 Bytes

Raw Blame

```
import {SequelizeModuleOptions} from "@nestjs/sequelize";
import {Log} from "./logs/log.model";
require('dotenv').config()

const dbConfig = (env: string): SequelizeModuleOptions => {
    switch(env) {
        case 'development':
            return {};
        case 'production':
            return {};
        // default -> dev db
        default:
            return {
                dialect: 'mysql',
                [redacted]
                username [redacted]
                password [redacted]
                database: 'latency_log',
                models: [Log],
                timezone: '+09:00',
                define: {
                    timestamps: false
                },
            };
    }
};

export default dbConfig;
```

# 대응방안

- **민감 정보가 노출된 레포지토리 삭제 조치**
  - GitHub 플랫폼 측에 Takedown 요청 접수
    - 요청 시, 민감 정보에 대한 설명이 필요함.
  - GitHub 의 경우, 작성자에게 일주일 내로 레포지토리를 삭제할 것을 공지함.
    - 일주일 내로 삭제하지 않을 경우, GitHub 측에서 임의로 삭제 조치를 취함.

- **임직원 계정 유출 안내 및 초기화 조치**
  - 유출된 임직원 계정 정보를 바탕으로 계정 유효성 확인
  - 유출 당사자에게 계정 유출 안내
  - 유출 당사자가 사용 중인 계정 정보 일괄 패스워드 초기화 조치

# 배경 및 요약

- 2021년 12월 13일 GitHub을 모니터링하던 중, 2014년 8월 8일에 작성된 특정 마라톤클럽 사이트와 관련된 사용자 정보가 업로드된 코드가 탐지됨.
- 레포지토리를 확인한 결과, 레포지토리의 운영자는 국내에서  IT 서비스를 제공하는 C사에 재직 중인 것으로 확인됨.
  - 2014년 8월 8일에 마지막으로 커밋되고 업데이트는 없는 상태이며, 해당 웹 사이트는 운영 중인 것으로 확인됨.
  - 웹 사이트 상에서 2021년 일정이 공지되어 있으며, 2020년 12월 5일까지의 일정이 업로드된 상태임.
- 사용자 정보가 노출되어 있는 페이지를 확인한 결과, 총 2965건의 사용자 정보가 노출된 것으로 확인됨.
  - 이름, 이메일만 노출된 정보는 2763건으로 확인됨.
  - 이름, 이메일, 아이디, 패스워드, 주민등록번호, 재직 중인 기업명, 주소가 노출된 정보는 202건으로 확인됨.

# 시나리오 2. GitHub 상에서 마라톤클럽 웹 사이트 유저 개인 정보 유출

3885 lines (3790 sloc) | 307 KB

Raw Blame

```
# MySQL dump 7.1
#
# Host: cgihost    Database: gumpu
#--------------------------------------------------------
# Server version        3.23.51-log

#
# Table structure for table 'mailinglist'
#
CREATE TABLE mailinglist (
  email varchar(30) DEFAULT '' NOT NULL,
  name varchar(20) DEFAULT '' NOT NULL,
  randno varchar(10) DEFAULT '' NOT NULL,
  PRIMARY KEY (email)
);

#
# Dumping data for table 'mailinglist'
#

[redacted]
```

# 대응방안

- **민감 정보가 노출된 레포지토리 삭제 조치**
  - GitHub 플랫폼 측에 Takedown 요청 접수
    - 요청 시, 민감 정보에 대한 설명이 필요함.
  - GitHub 의 경우, 작성자에게 일주일 내로 레포지토리를 삭제할 것을 공지함.
    - 일주일 내로 삭제하지 않을 경우, GitHub 측에서 임의로 삭제 조치를 취함.

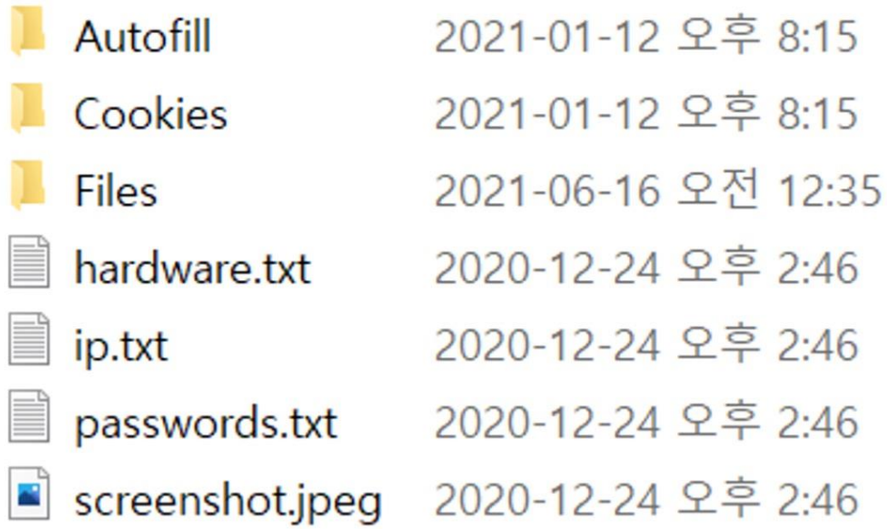
- **임직원 계정 유출 여부 확인, 계정 유출 안내 및 초기화 조치**
  - 유출된 임직원 계정 정보를 바탕으로 계정 유효성 확인
  - 유출 당사자에게 계정 유출 안내
  - 유출 당사자가 사용 중인 계정 정보 일괄 패스워드 초기화 조치

# 시나리오 3. 국내 IT 인프라 운영 및 유지보수 업체 임직원의 스틸러 감염으로 인해 기업 민감 정보 유출

## 배경 및 요약

- 다크웹 모니터링 중, 국내 IT 인프라 운영 및 유지보수 업체인 B사 직원의 PC가 Ficker Stealer 에 의해 감염되어 해당 PC에 저장된 B사 고객사의 내부 데이터가 유출된 사실을 확인함.
  - **Ficker Stealer : 감염 기기내 브라우저 정보, 문서 파일, 원격 계정정보 등을 유출하는 악성코드**
- 총 77개의 문서가 유출되었으며, 그 중 보안 진단 가이드라인과 총괄유지보수현황 및 접속정보 관련 파일이 포함되어 있음.
  - 총괄유지보수현황 파일에는 접속 IP, 관리자 계정 정보, 하드웨어 및 소프트웨어 버전에 대한 상세 내용이 모두 포함되어 있는 점으로 보아 유출 시 매우 큰 위협이 될 수 있을 것으로 판단함.

# 시나리오 3. 국내 IT 인프라 운영 및 유지보수 업체 임직원의 스틸러 감염으로 인해 기업 민감 정보 유출




Autofill : 브라우저 자동 완성 데이터

Cookies : 브라우저 쿠키 데이터

Files : 감염기기에 저장된 모든 문서 파일

hardware.txt : 감염기기 하드웨어 및 설치 소프트웨어 정보

ip.txt : 감염 당시의 감염기기 IP

passwords.txt : 브라우저에 저장된 웹 사이트 계정정보

screenshot.jpeg : 감염 당시 화면 캡처

# 시나리오 3. 국내 IT 인프라 운영 및 유지보수 업체 임직원의 스틸러 감염으로 인해 기업 민감 정보 유출

| 구분 | | | | 서비스 | | 도입환경 |
|---|---|---|---|---|---|---|
| 분류#1 | 분류#2 | 분류#3 | 호스트네임 | 제공서비스 | 담당매니 | 도입연 |
| 행안망 | SQMS | | | VOIP | | |
| VoIP_B1 | TAPS | | | 인증 | | |
| VoIP_B1 | TAPS | | | 인증 | | |
| 기타 | 통합일지 | | | 전국통합운용 | | |
| 기타 | IOMC | | | 관제 | | |
| 기타 | IOMC | | | 관제 | | |
| 기타 | IOMC | | | 관제 | | |
| 기타 | IOMC | | | 관제 | | |
| 기타 | IOMC | | | 관제 | | |
| 기타 | IOMC | | | 관제 | | |
| 기타 | CTMS | | | 관제 | | |
| 기타 | CTMS | | | 관제 | | |
| 기타 | CTMS | | | 관제 | | |

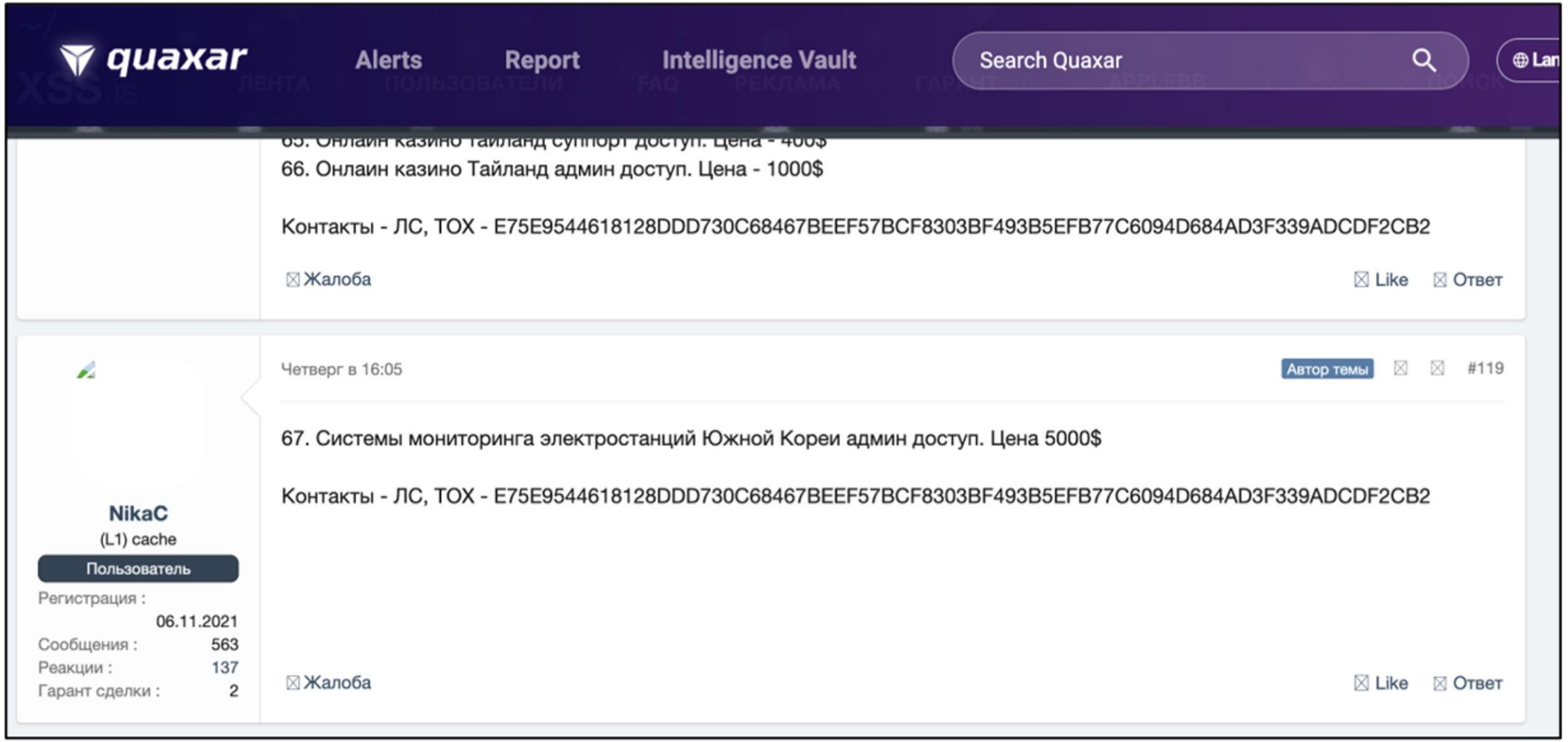
# 시나리오 3. 국내 IT 인프라 운영 및 유지보수 업체 임직원의 스틸러 감염으로 인해 기업 민감 정보 유출

## 대응방안

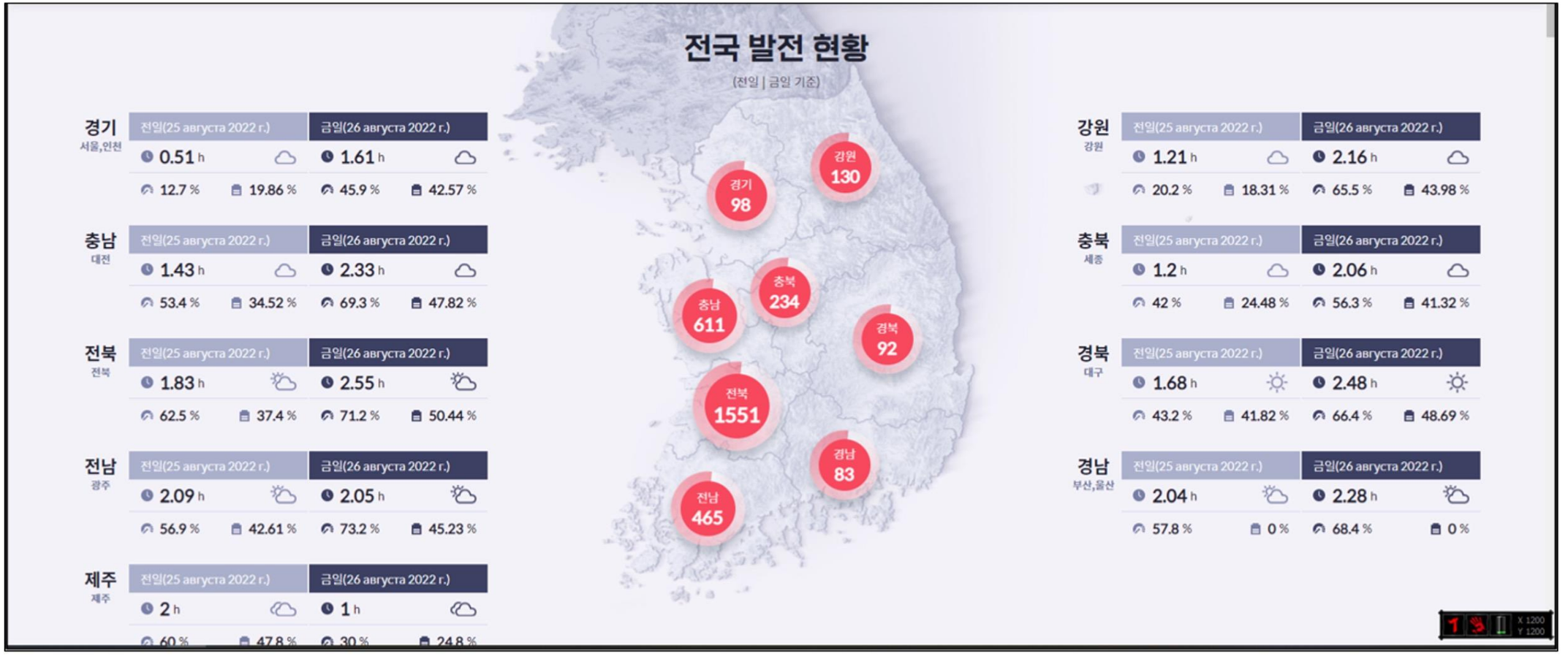
- **민감 정보가 노출되어 있는 스틸러 로그 유출 소스 확보**
  - 딥웹 & 다크웹 해킹 포럼 및 히든 채널 내 스틸러 로그 관련 소스 전수 조사
  - 유출 범위 및 영향도 파악

- **임직원 계정 유출 여부 확인, 계정 유출 안내 및 초기화 조치**
  - 유출된 임직원 계정 정보를 바탕으로 계정 유효성 확인
  - 유출 당사자에게 계정 유출 안내
  - 유출 당사자가 사용 중인 계정 정보 일괄 패스워드 초기화 조치

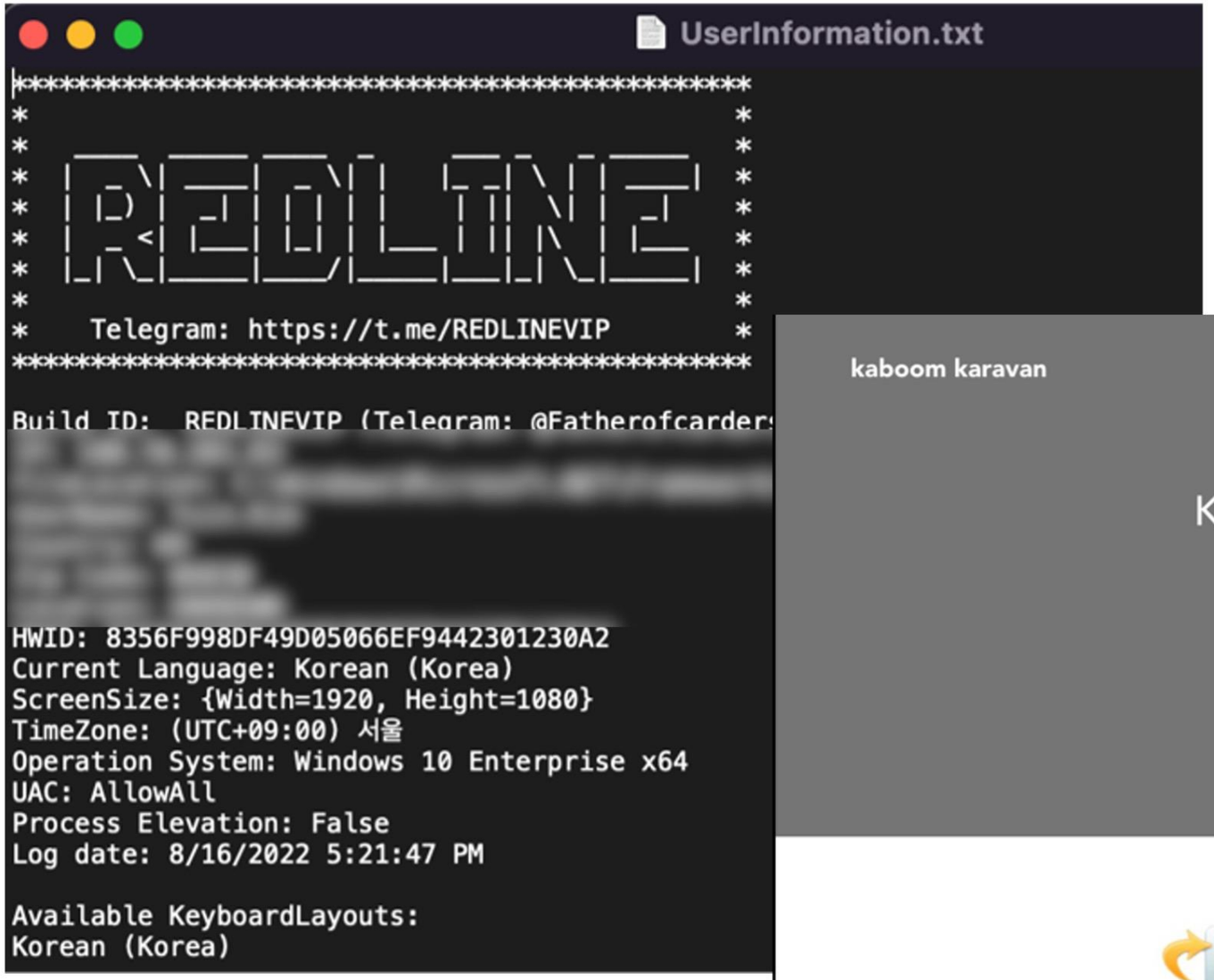
# 탐지 케이스. 협력사 임직원의 스틸러 감염으로 인해 기업 민감 정보 유출



# 탐지 케이스. 협력사 임직원의 스틸러 감염으로 인해 기업 민감 정보 유출



# 탐지 케이스. 협력사 임직원의 스틸러 감염으로 인해 기업 민감 정보 유출




# 탐지 케이스. 협력사 임직원의 스틸러 감염으로 인해 기업 민감 정보 유출

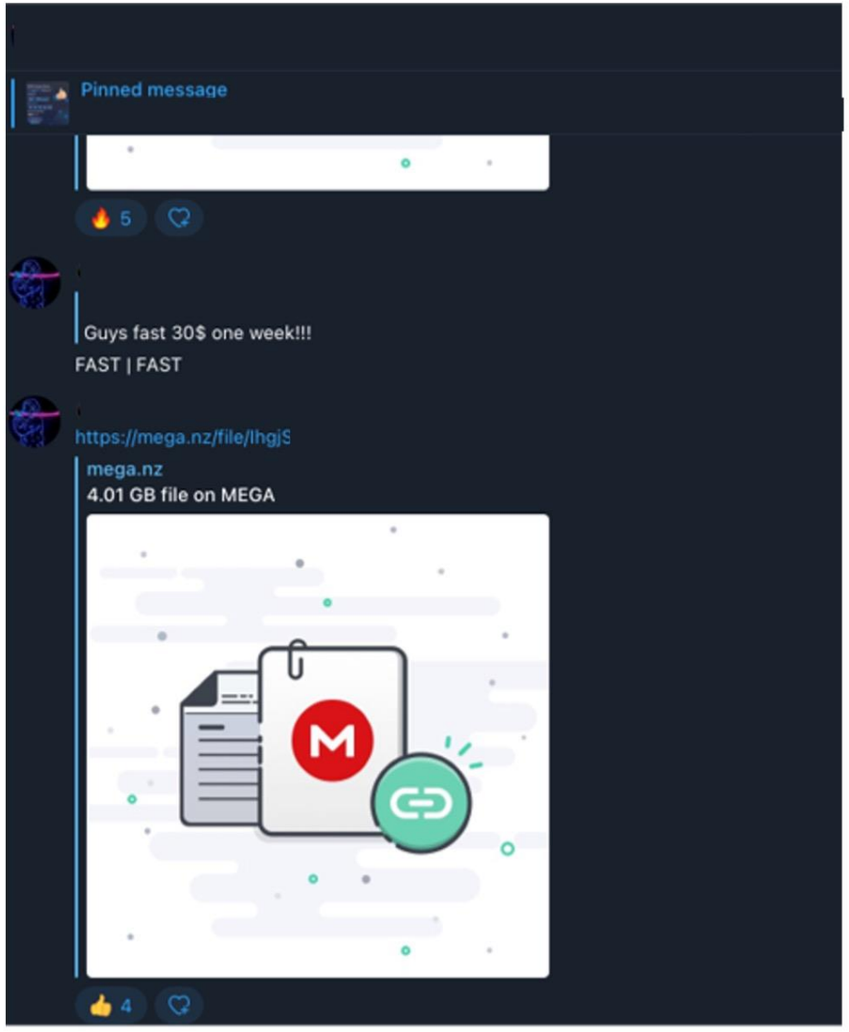
## 스틸러 로그 판매 경로

**(2022-08-07) S***-K***** Cloud**
- (2022-08-07) https://t.me/Sa********Cloud/81
- (2022-08-22) https://t.me/Sa********Cloud/104

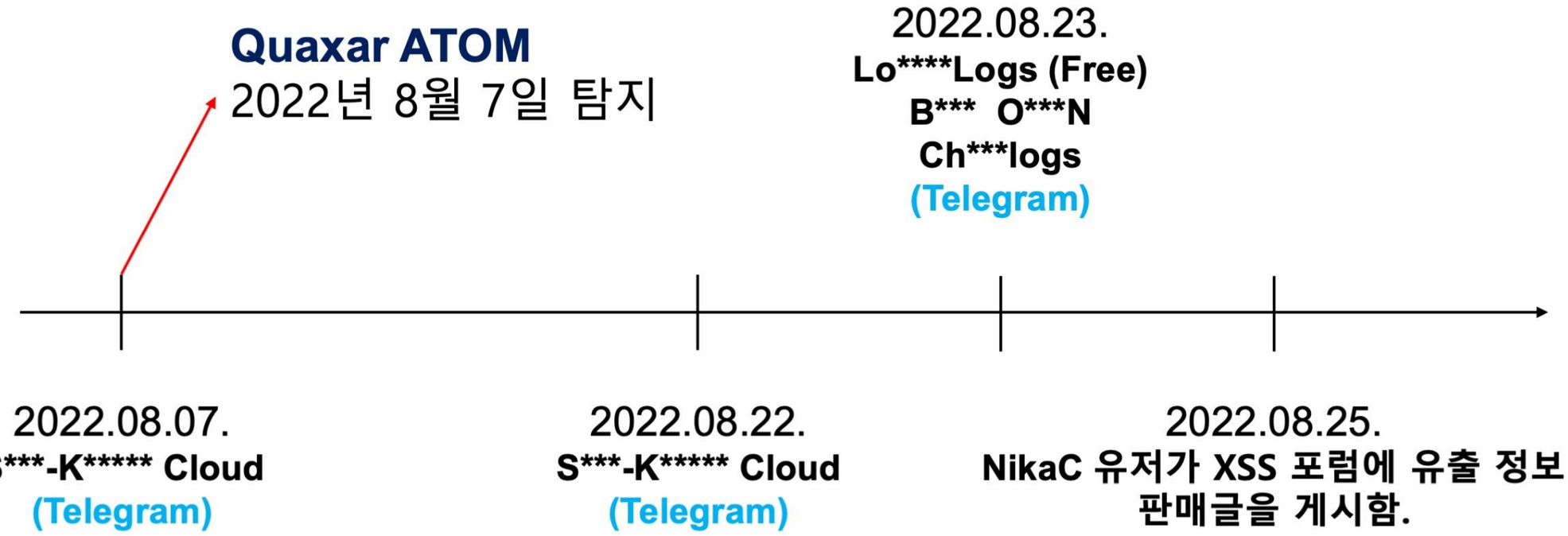
(2022-08-23) Lo**********  (Free)
- https://t.me/lo**********free/73

(2022-08-23) B***  O***N
- https://t.me/re*****eo****1/221607

(2022-08-23) Cha*******
- https://t.me/cha*******/37758



# 탐지 케이스. 협력사 임직원의 스틸러 감염으로 인해 기업 민감 정보 유출



# 탐지 케이스. 협력사 임직원의 스틸러 감염으로 인해 기업 민감 정보 유출

## 대응방안

- **민감 정보가 노출되어 있는 스틸러 로그 유출 소스 확보**
  - 딥웹 & 다크웹 해킹 포럼 및 히든 채널 내 스틸러 로그 관련 소스 전수 조사
  - 유출 범위 및 영향도 파악

- **임직원 계정 유출 여부 확인, 계정 유출 안내 및 초기화 조치**
  - 유출된 임직원 계정 정보를 바탕으로 계정 유효성 확인
  - 유출 당사자에게 계정 유출 안내
  - 유출 당사자가 사용 중인 계정 정보 일괄 패스워드 초기화 조치

# 계정 유출 대응방안

**딥웹 & 다크웹 해킹 포럼 및 히든 채널 상에서의 계정 유출 판매 및 공유 채널 모니터링 필요**

- 계정 유출 정보를 판매하는 포럼 유저와 채널 운영자는 주기적으로 활동 포럼과 채널을 변경함.
- 타 유저가 업로드한 유출 정보를 재판매 및 재공유하는 브로커도 존재함.
- 기 유출된 유출 정보의 경우, 포럼과 채널에서 반복적으로 공유됨.

**GitHub, Gitee 등과 같은 소스코드 관리 서비스(원격 저장소) 상에서 노출된 민감 정보 모니터링 필요**

- 프로토타입 및 제품 개발 과정에서 이력 관리 용도로 의뢰 업체로 부터 허가없이 GitHub에 소스코드 정보를 공개적으로 업로드하는 유저가 존재함.
- 소스코드만 업로드하는 과정에서 실수로 민감 정보를 업로드하는 유저가 존재함.

**계정 유출 이력 관리 필요**

- 동일한 계정 정보를 반복적으로 업로드하는 판매자나 브로커도 존재함.
- 판매자 및 브로커에 대한 평판을 평가하는 기준이 됨.
- 딥웹 & 다크웹 상에서 유출된 계정 덤프에 대한 유출 범위 파악에 도움됨.

S2W

Safe and Secure World

## S2W와 솔루션에 대해 더 알고 싶으신가요?

아래의 메일 주소로 문의주세요.

info@s2w.inc

www.s2w.inc

경기도 성남시 분당구 판교역로 192번길 12, 판교미래에셋센터 3층 | +82 07 5066 5277

# QnA