

제1회 S2W WITH 웨비나

2023년 2월 28일 (화) LIVE
오후 2:00 - 3:30

For February
다크웹과 침해사고

Agenda

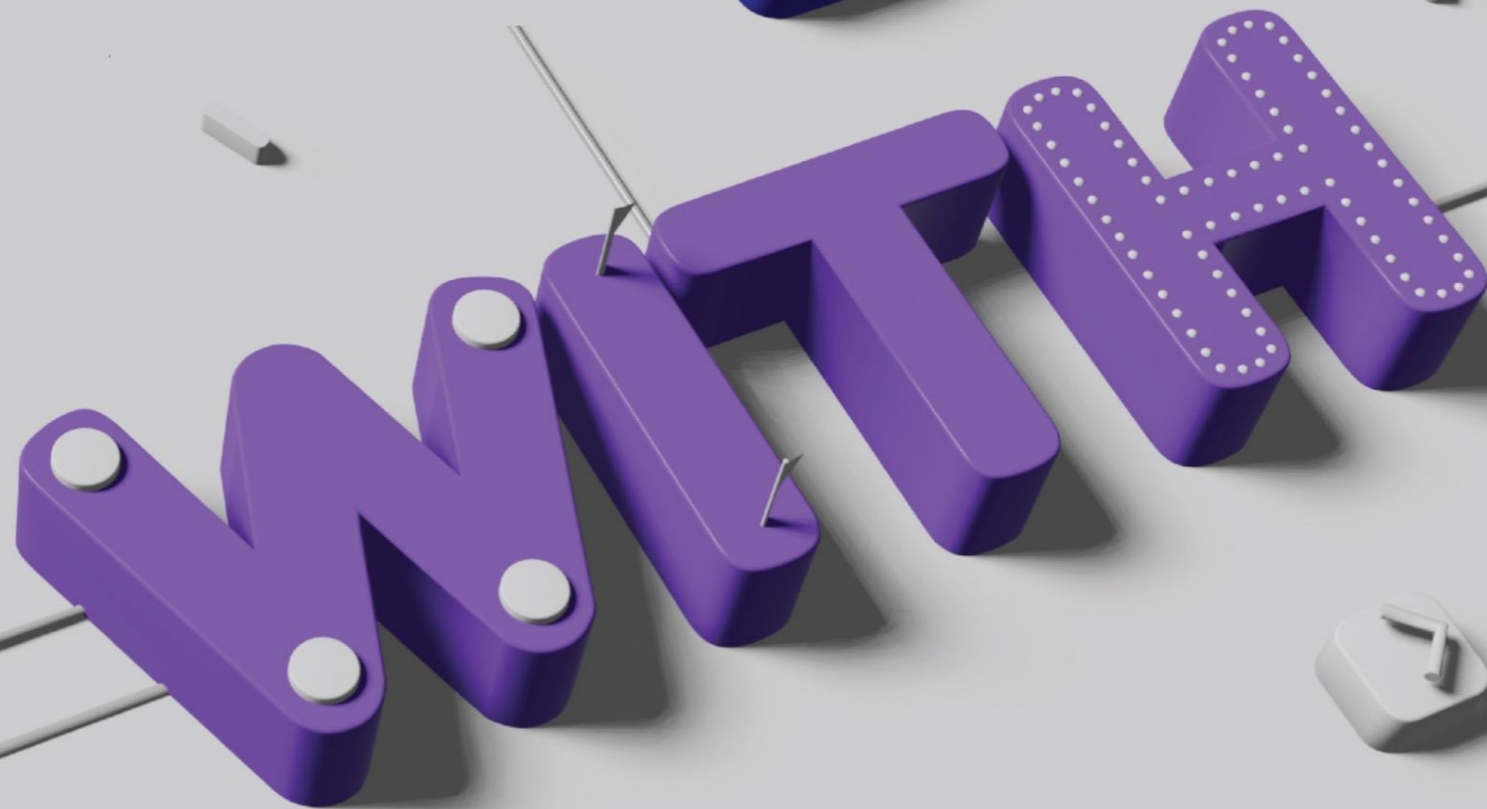
2:00 - 2:10	키노트
2:10 - 2:30	딥다크웹 동향 & 인사이트
2:30 - 3:00	Account Take Over 시나리오
3:00 - 3:30	QnA



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

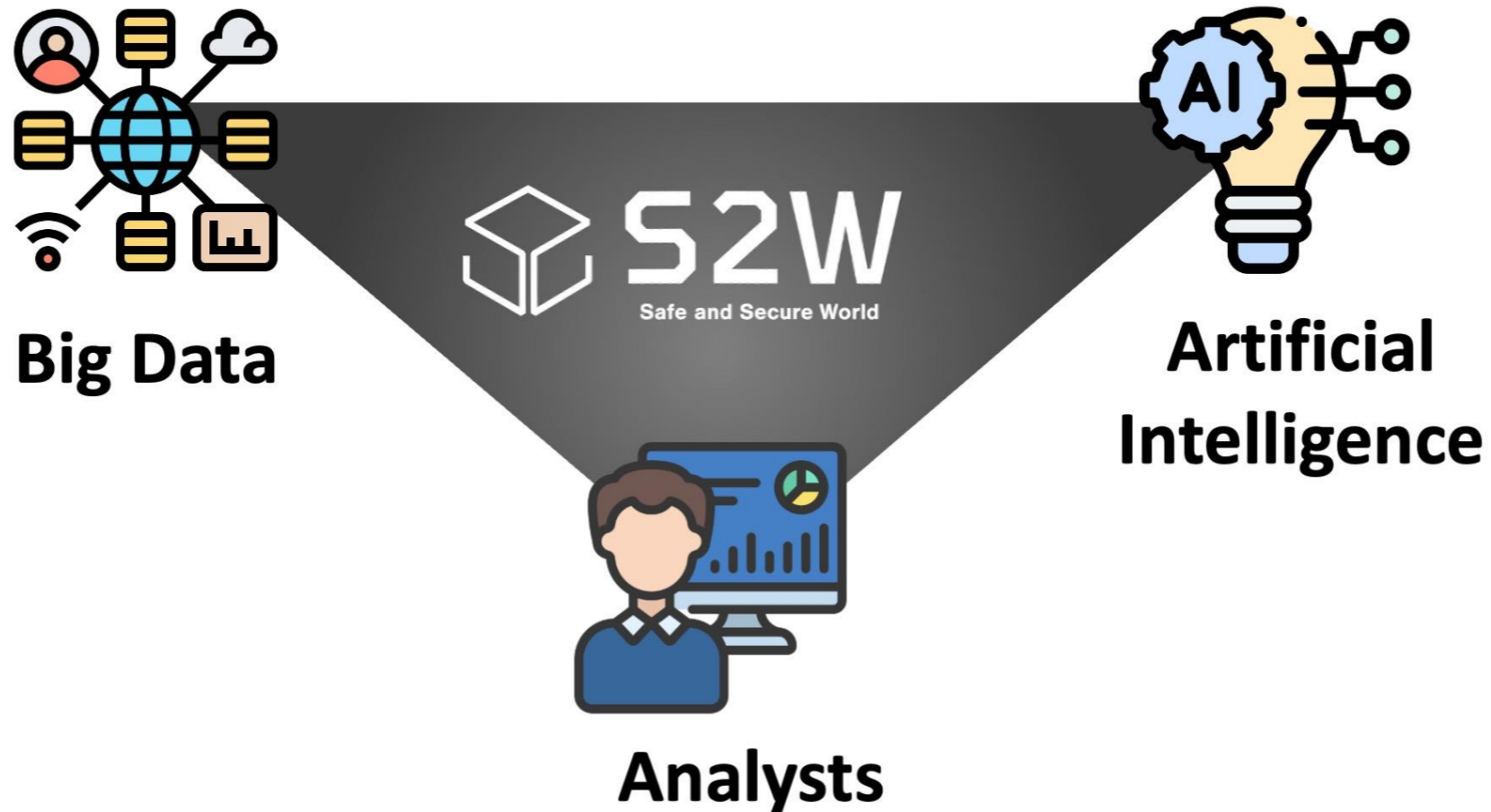
2. Cybersecurity Domain ?

ATTACK, LEAK, ABUSE, ...

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

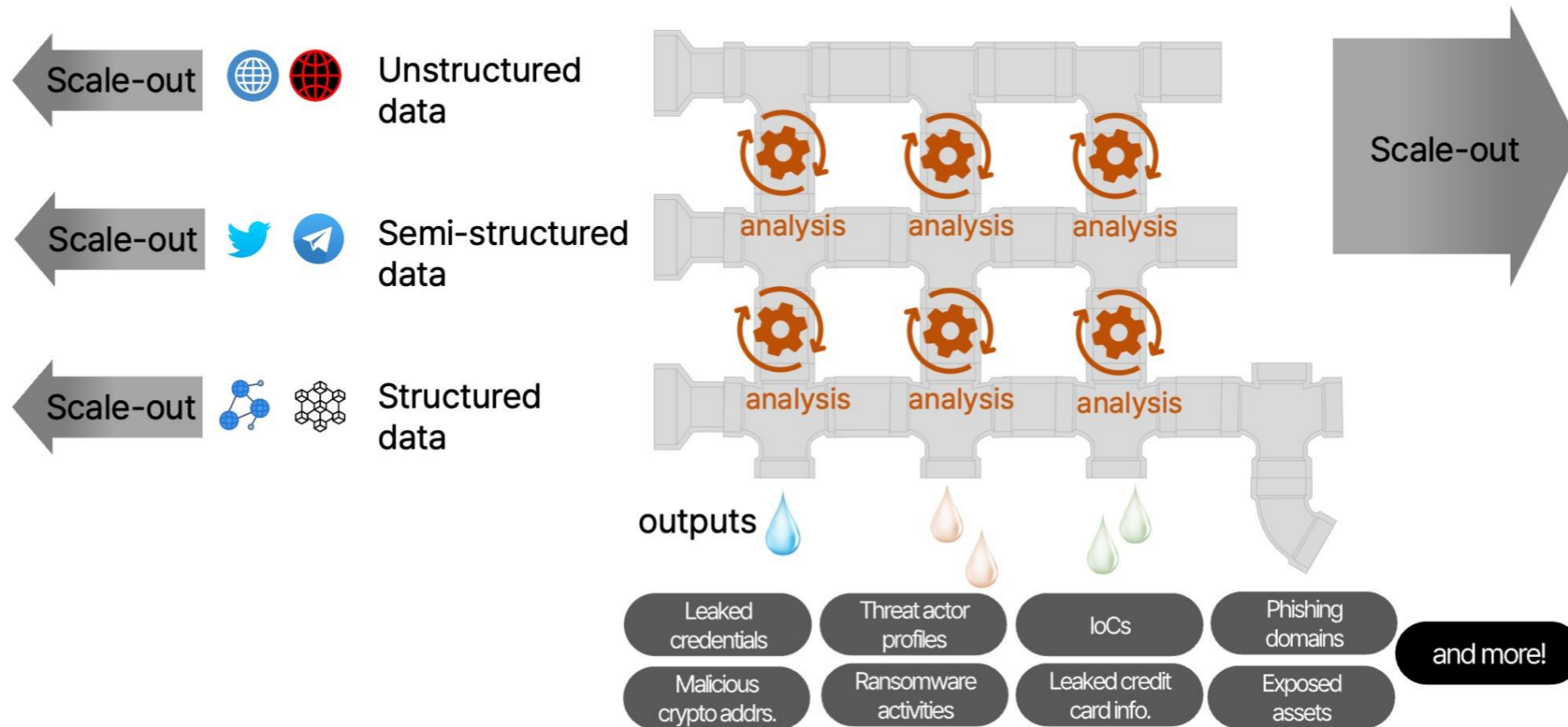
S2W 데이터 인텔리전스 경쟁력의 기반

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



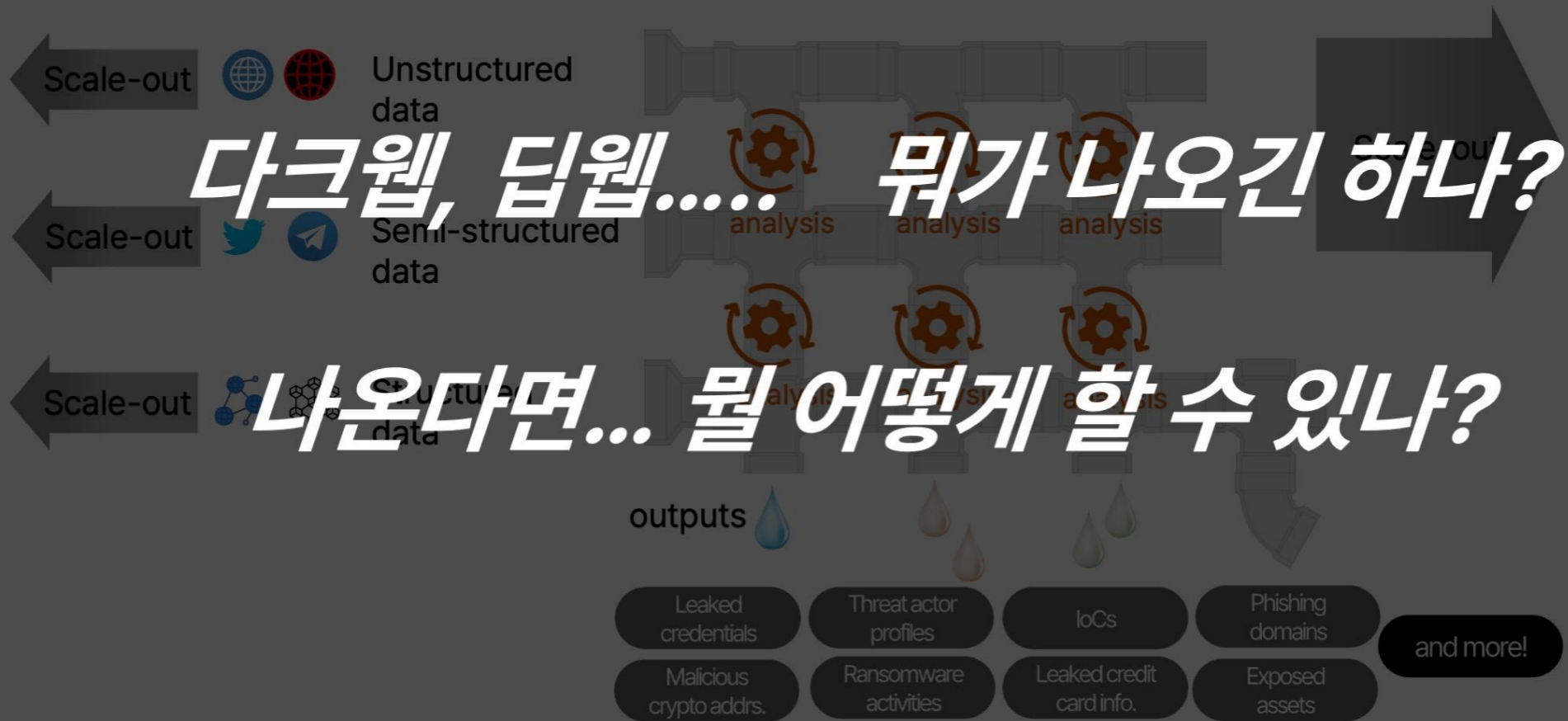
빅데이터 파이프라인 기반의 보안

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.



제1회 S2W <with>

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



S2W

제1회 S2W WITH 웨비나

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

For February
다크웹과 침해사고

Agenda

- 01 키노트
- 02 다크웹 인사이트 & 동향
- 03 Account Take Over 시나리오

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

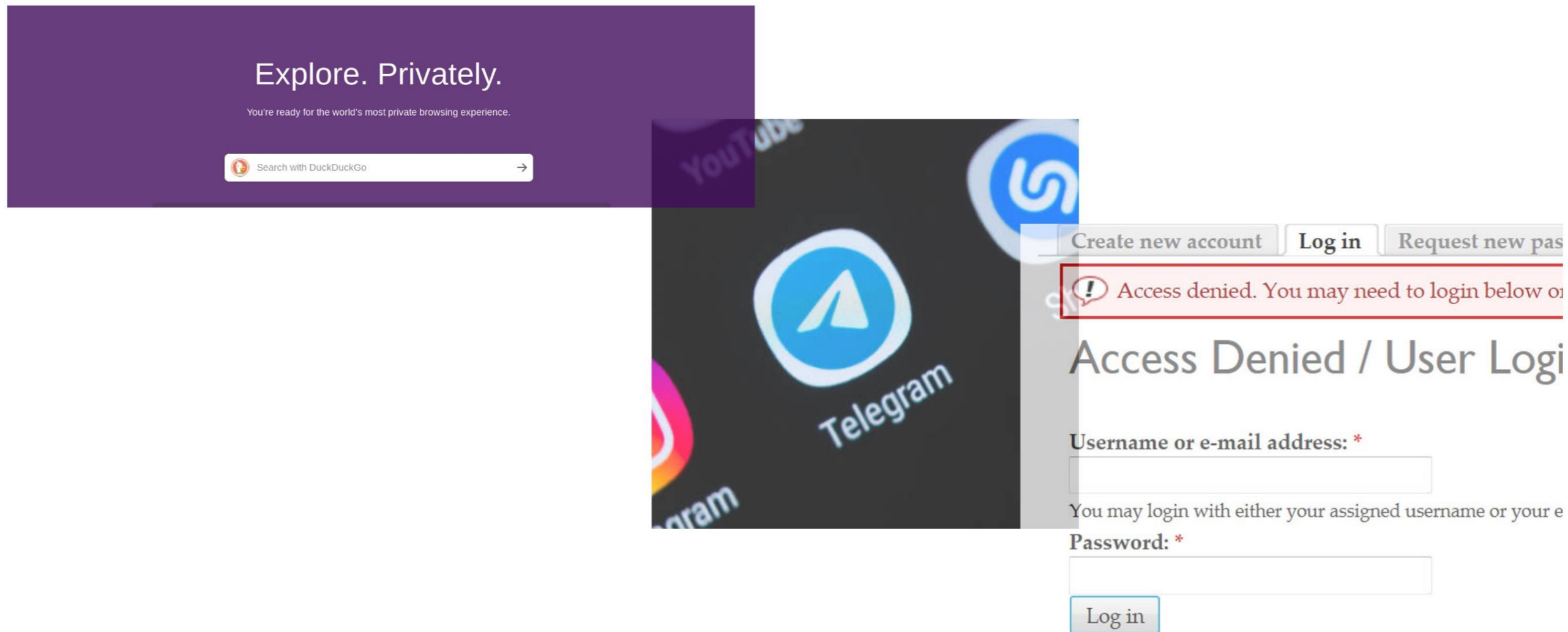
기업과 개인을 대상으로 사이버 공격을 수행하는 공격 그룹에 대한 프로파일링

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.





심선형

데이터 분석가

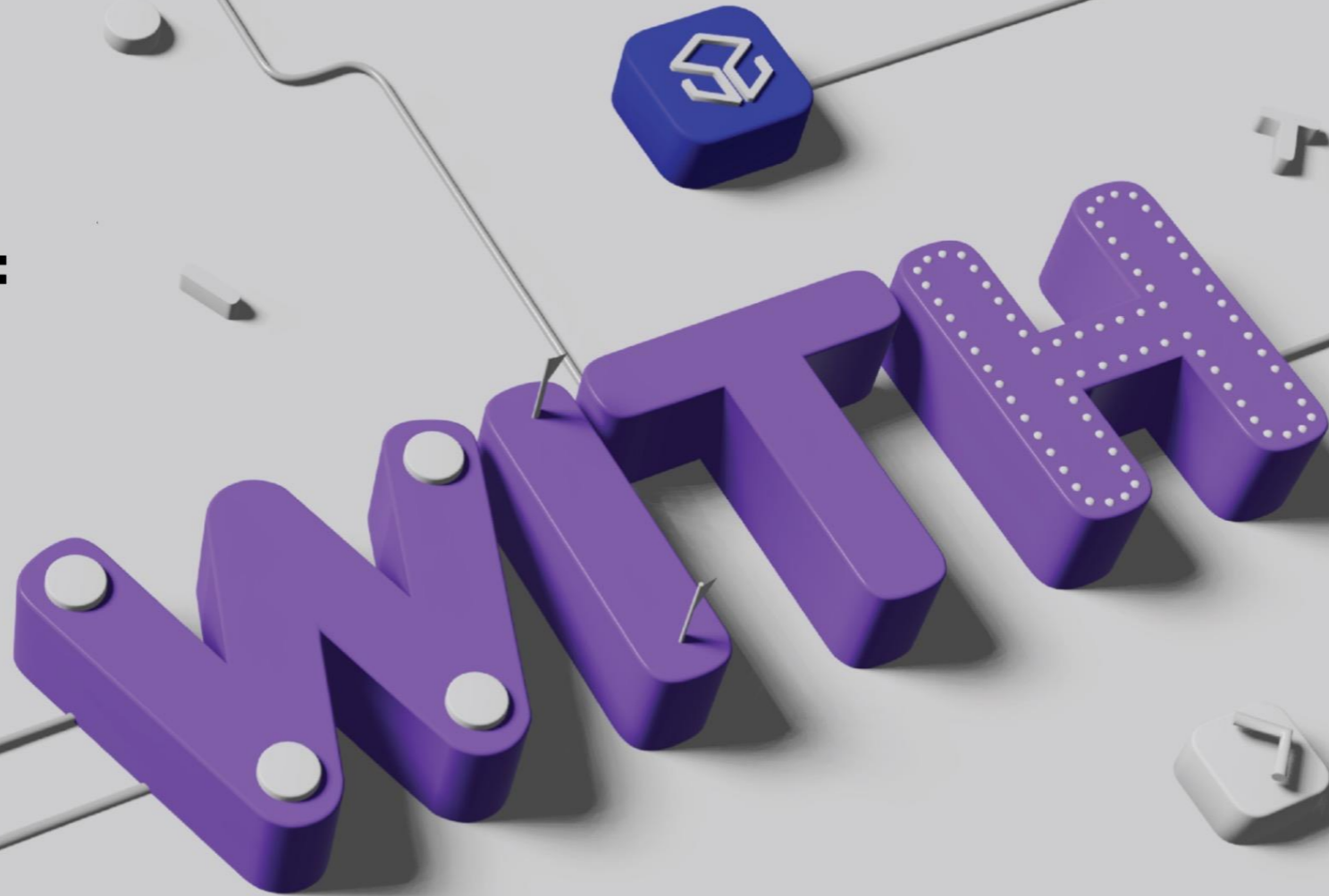
딥/다크웹 데이터 인사이트 도출 및 분석

The information contained in this document is proprietary and confidential.
If you are not the intended recipient, please note that any use or circulation of this document may be cause for legal action.

2. 딥다크웹 동향 및 인사이트

범죄의 목적,
다크웹 개요,
다크웹 최신 동향

심선형, Data Analyst

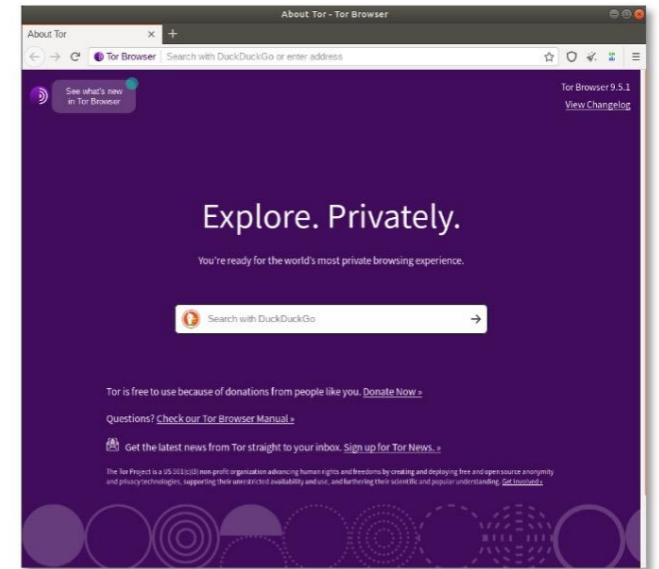
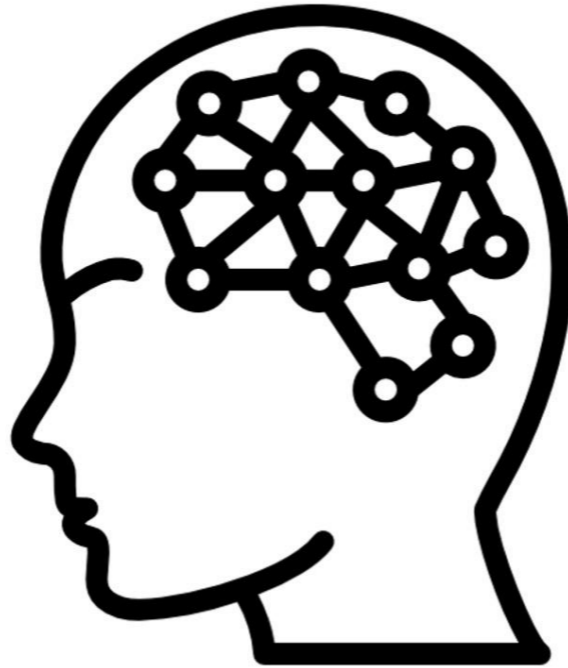


(1) 발표자 소개

AI를 통한 딥/다크웹 주요 이슈 발견

BF

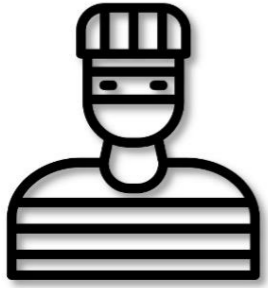
~/ XSS.is



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



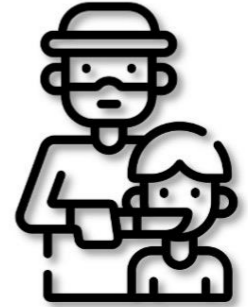
강도



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?

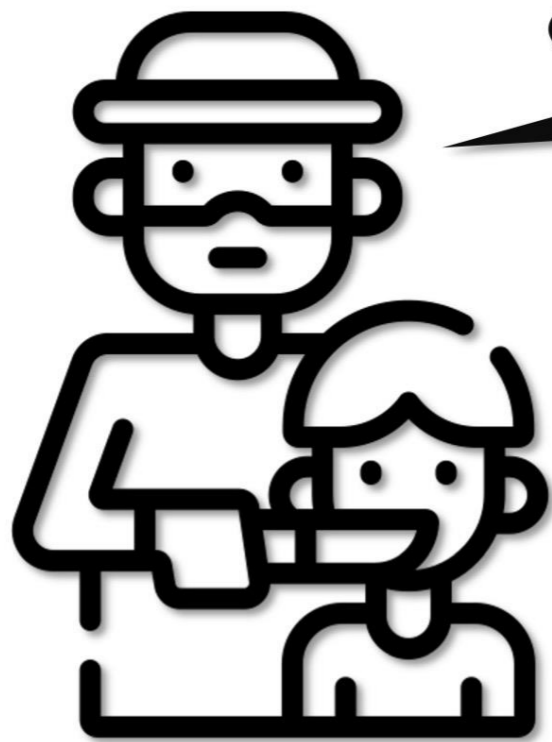


금전 및 자산 탈취



(2) 해커들의 대전제: 왜 사이버 공격을 할까?

유괴: 부모로부터 소중한 자식을 납치하여 협박하는 행위

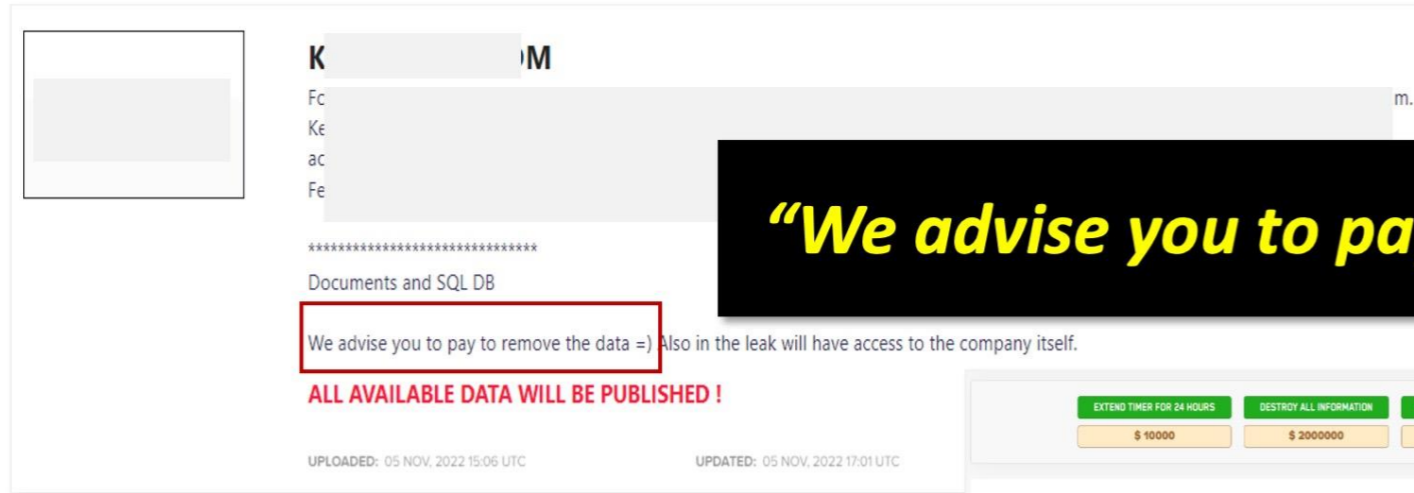


~~까지 일정 금액을 준비 하지 않으면 자식에게
위협을 가하겠다...

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

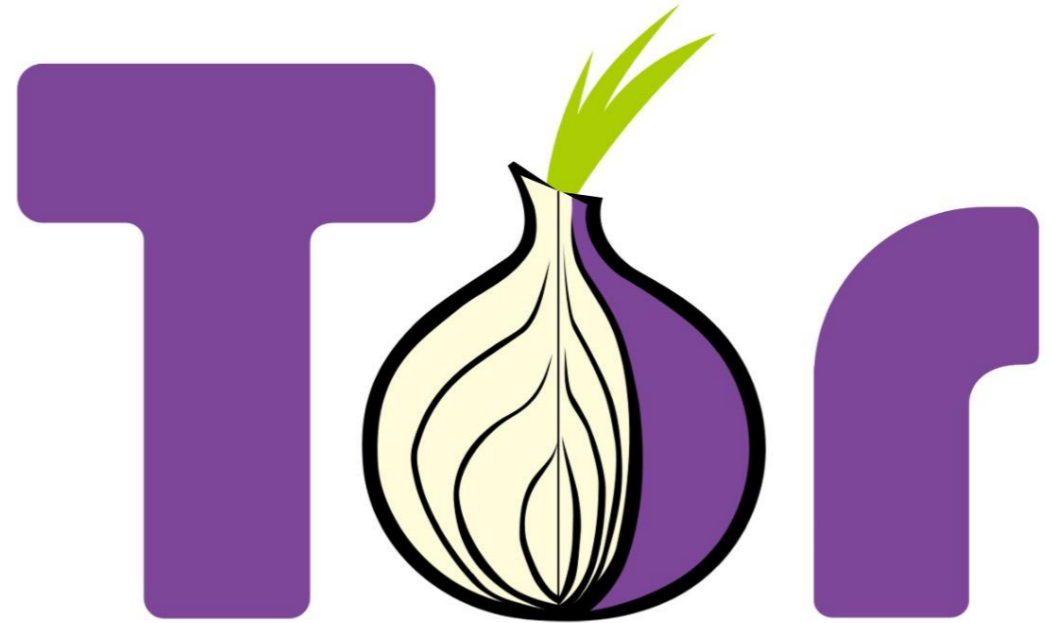
익명성이 보장됨
과 동시에, 금전과 자산을 갈취!

(2) 해커들의 대전제: 왜 사이버 공격을 할까?

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

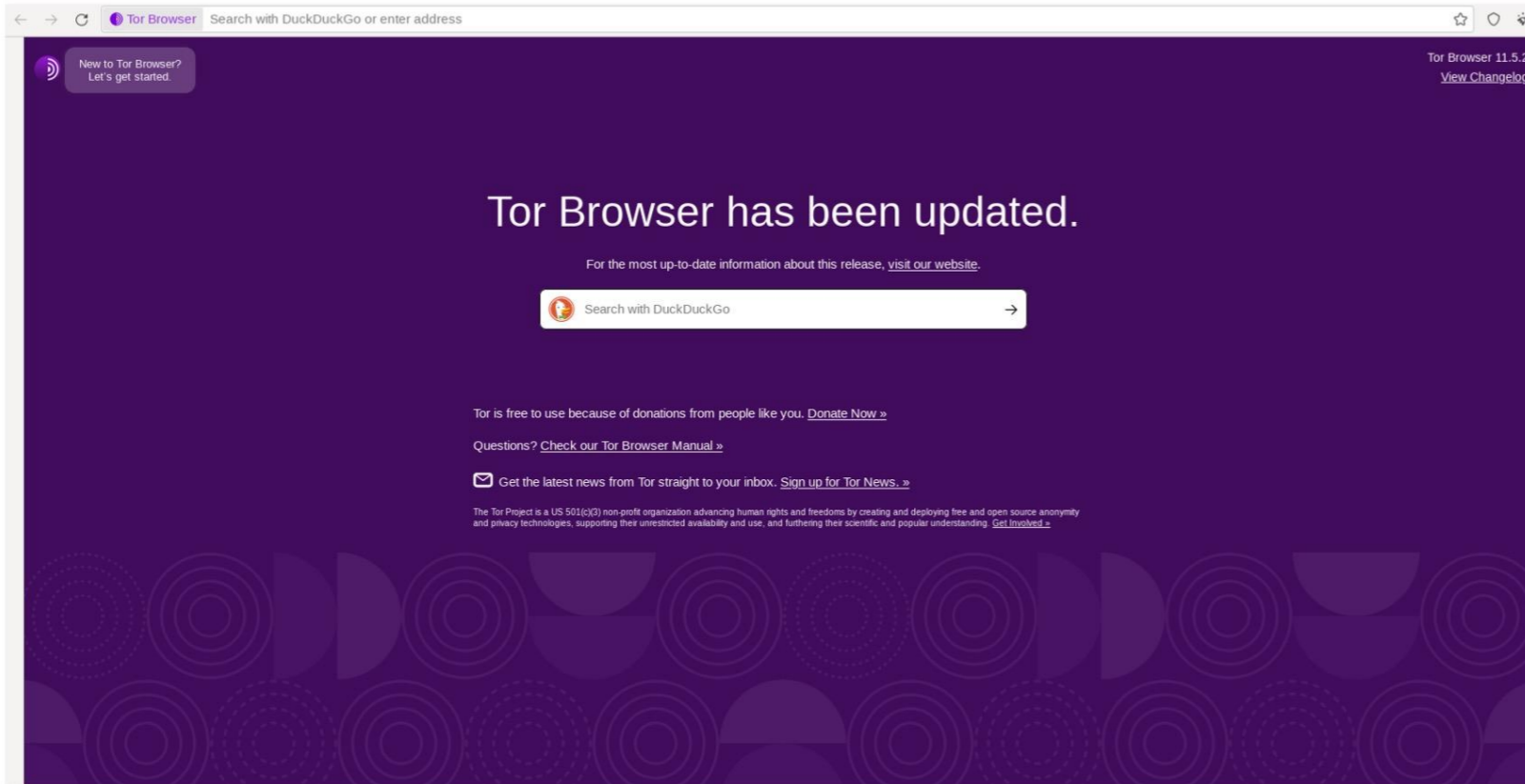
(3) 해커들의 무대. 딥/다크웹 공간이란?

다크웹은 특수한 브라우저 'Tor Browser'을 통해서만 접근 가능



(3) 해커들의 무대. 딥/다크웹 공간이란?

‘Tor Browser’ 메인 화면



다크웹 접속에 사용되는 TOR 브라우저

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

n3rnu4upio2b64g6gyw4dwboajmuyqarvlan4r3tgcemzy6ccjgveuad.onion
fdh6mpolzifswuemp3pz67fwvre5t2kmyhr63htymcjh5e5murnfcmqd.onion

(3) 해커들의 무대. 딥/다크웹 공간이란?

일반 웹 브라우저에서 확인한 IP 주소

The screenshot shows the 'WhatIs MyIPAddress.com' website interface. At the top, there is a search bar with the text 'Enter Keywords or IP Address...' and a blue 'Search' button. Below the search bar, the website displays the following information:

- My IP Address is:
 - IPv4: **222.110.10.33**
 - IPv6: **Not detected**
- My IP Information:
 - ISP: SK Broadband Co Ltd
 - City: Seongnam
 - Region: Gyeonggi-do
 - Country: Korea (Republic of)

To the right of the IP information, there is a warning: 'Your private information is exposed!' with a red button that says 'HIDE MY IP ADDRESS NOW'. Below this button is a link: 'Show Complete IP Details'. To the right of the warning, there is a map of South Korea with a red location pin. A tooltip above the pin says 'Click for more details about 222.110.10.33'. Below the map, there are two links: 'Location not accurate?' and 'Update My IP Location'.

(3) 해커들의 무대. 딥/다크웹 공간이란?

Tor 브라우저에서 확인한 IP 주소

The screenshot shows the 'WhatIs MyIPAddress.com' website interface. At the top left is the logo, which includes a globe and a magnifying glass. To the right of the logo is a search bar with the placeholder text 'Enter Keywords or IP Address...' and a blue 'Search' button. Below the search bar, the page displays 'My IP Address is:' followed by two rows of IP addresses: 'IPv6: ? 2a0b:f4c2:1::1' and 'IPv4: ? 192.168.1.45'. To the right of these IP addresses is a map of Wisconsin with a red location pin and a tooltip that says 'Click for more details about 2a0b:f4c2:1::1'. Below the IP addresses, there is a section titled 'My IP Information:' containing a table of details. A red button with a shield icon and the text 'HIDE MY IP ADDRESS NOW' is positioned to the right of the table. Below the button is a link 'Show Complete IP Details'. To the right of the map, there is a link 'Update My IP Location' and the text 'Location not accurate?'. A yellow box highlights the 'My IP Information:' table.

My IP Address is:

IPv6: ? 2a0b:f4c2:1::1

IPv4: ? 192.168.1.45

My IP Information:

ISP:	Zwiebelfreunde E.V.
Services:	Network Sharing Device
City:	South Beloit
Region:	Illinois
Country:	United States

Your private information is exposed!

[HIDE MY IP ADDRESS NOW](#)

[Show Complete IP Details](#)

Location not accurate?
[Update My IP Location](#)

(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 콘텐츠는 매일 쏟아져 나오고 있음



마약



해킹

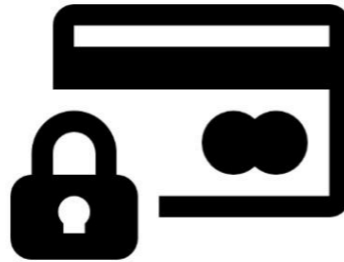


암호화폐 세탁

불법 콘텐츠는 그 유형이 매우 다양함



총기 & 장물



금융 범죄

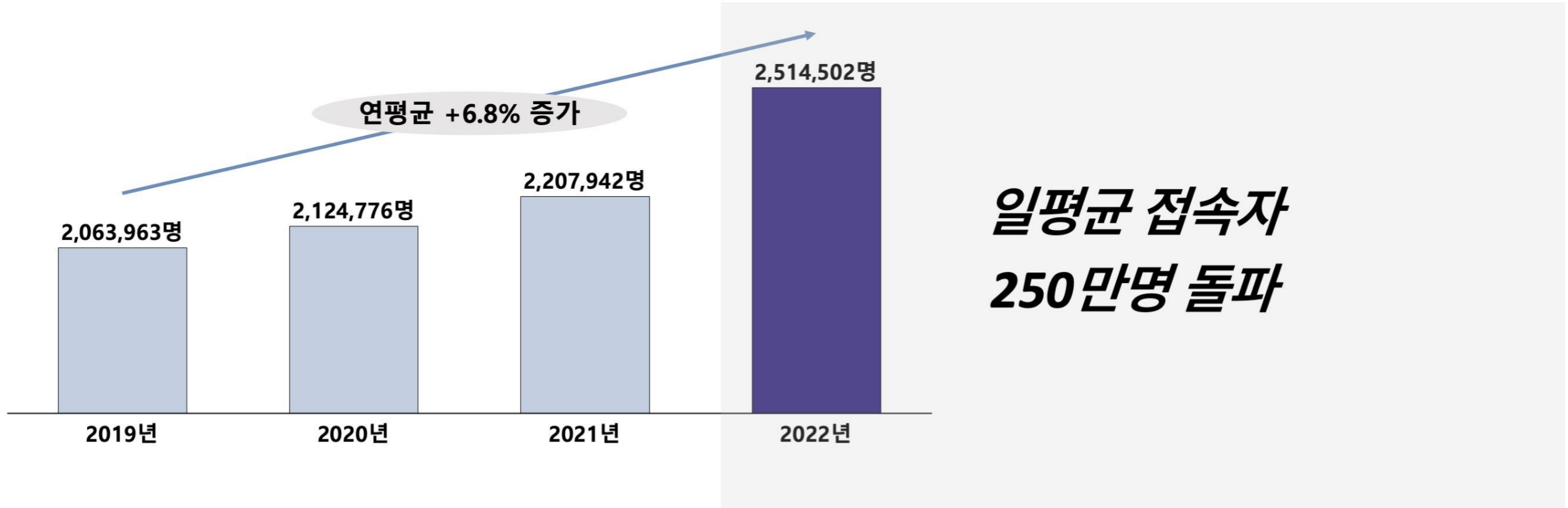


카지노 & 불법도박

(3) 해커들의 무대. 딥/다크웹 공간이란?

글로벌 다크웹 유저: 다크웹 접속자 수는 꾸준한 상승 추세

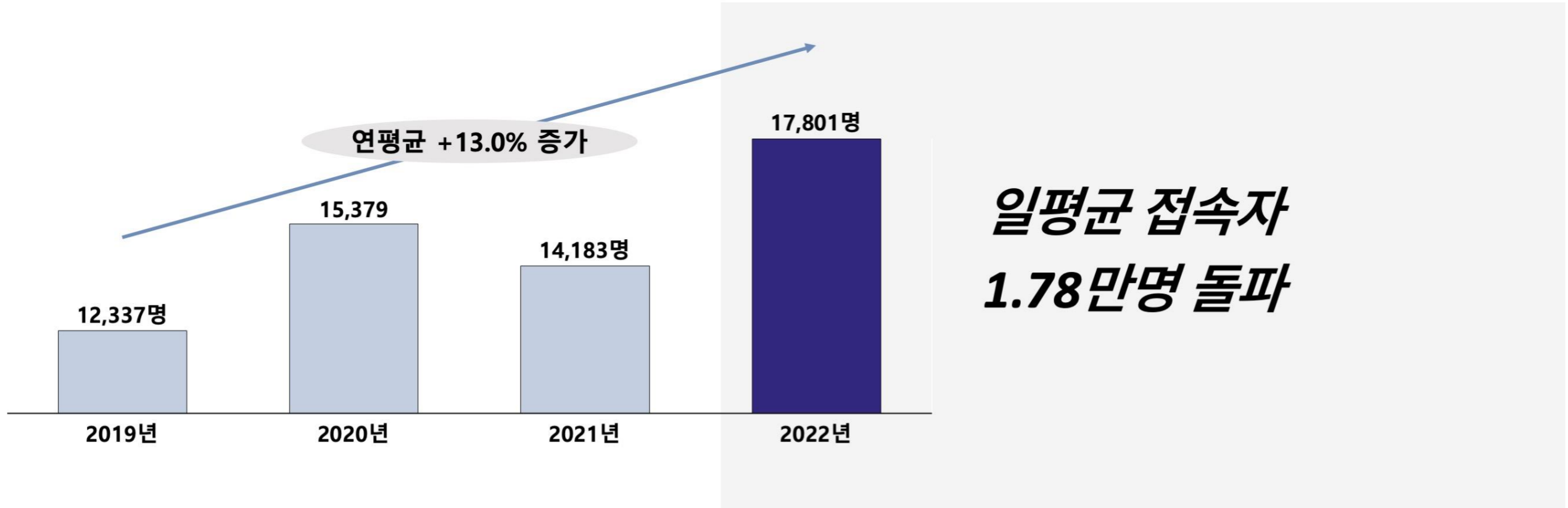
2019 – 2022 전세계 일평균 다크웹 접속자



(3) 해커들의 무대. 딥/다크웹 공간이란?

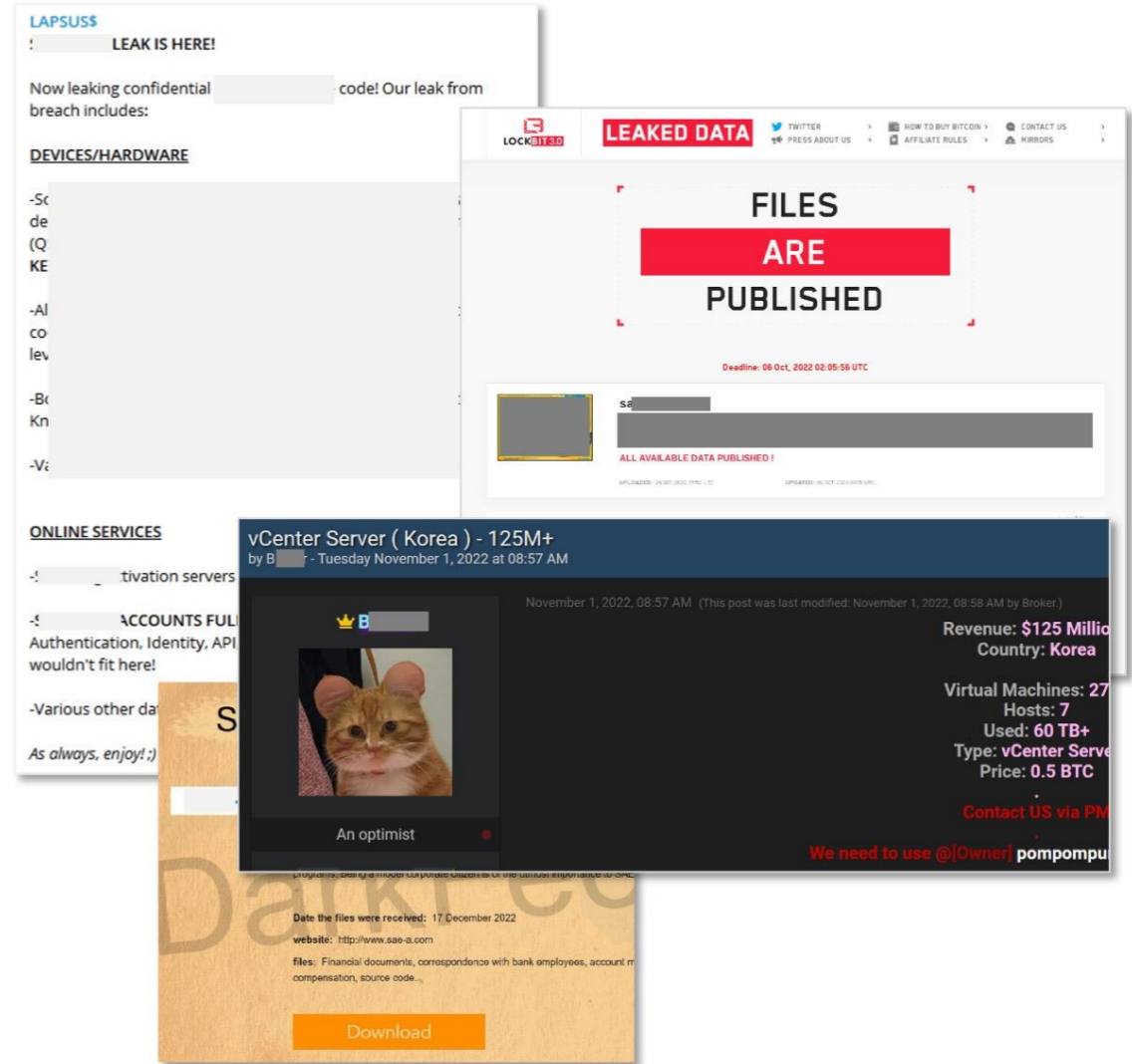
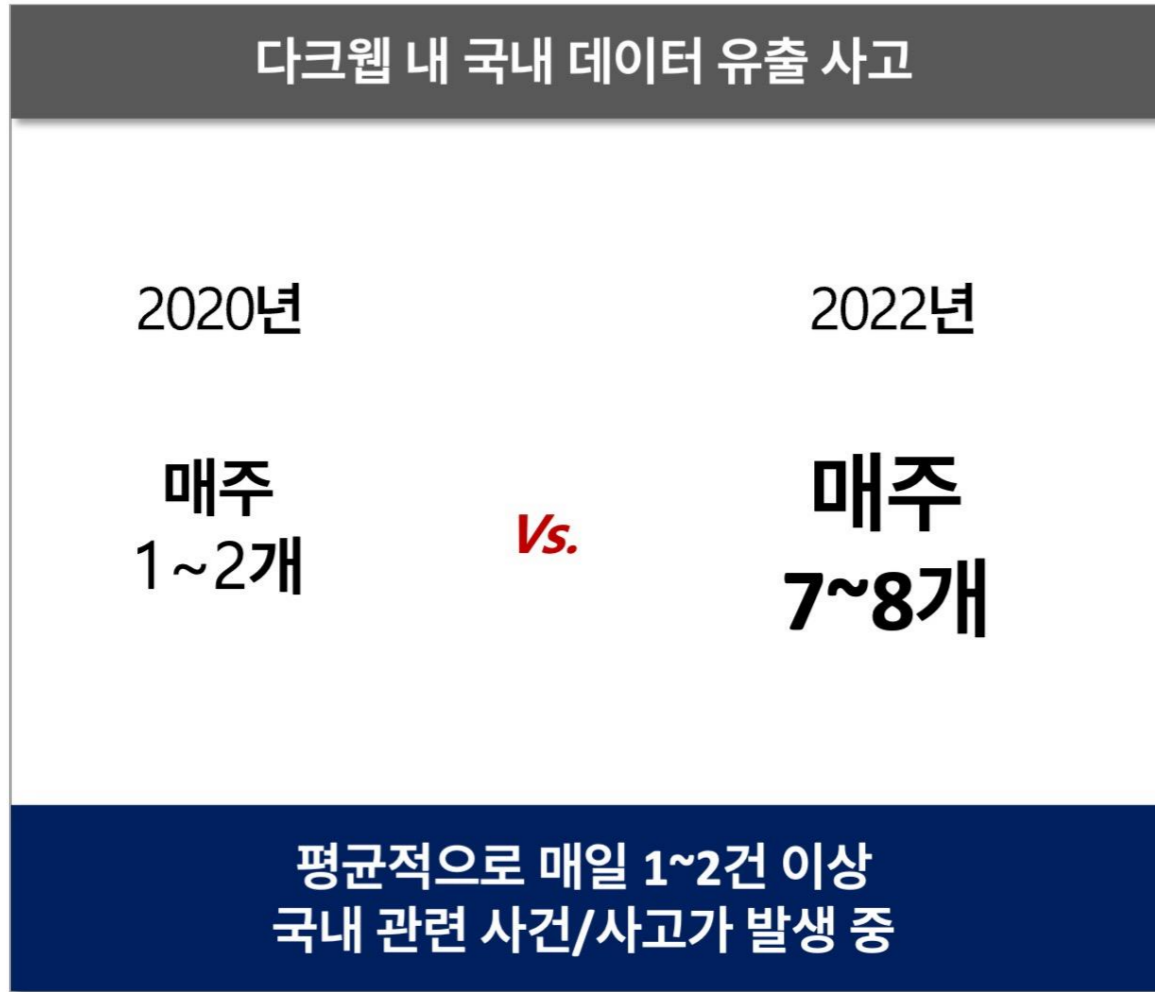
국내 다크웹 유저: 다크웹 접속자 수도 글로벌과 유사한 추이

2019 – 2022 국내 일평균 다크웹 접속자



(3) 해커들의 무대. 딥/다크웹 공간이란?

딥&다크웹 내 국내 관련 사건/사고는 과거와 비교해 현격히 증가



(3) 해커들의 무대. 딥/다크웹 공간이란?

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

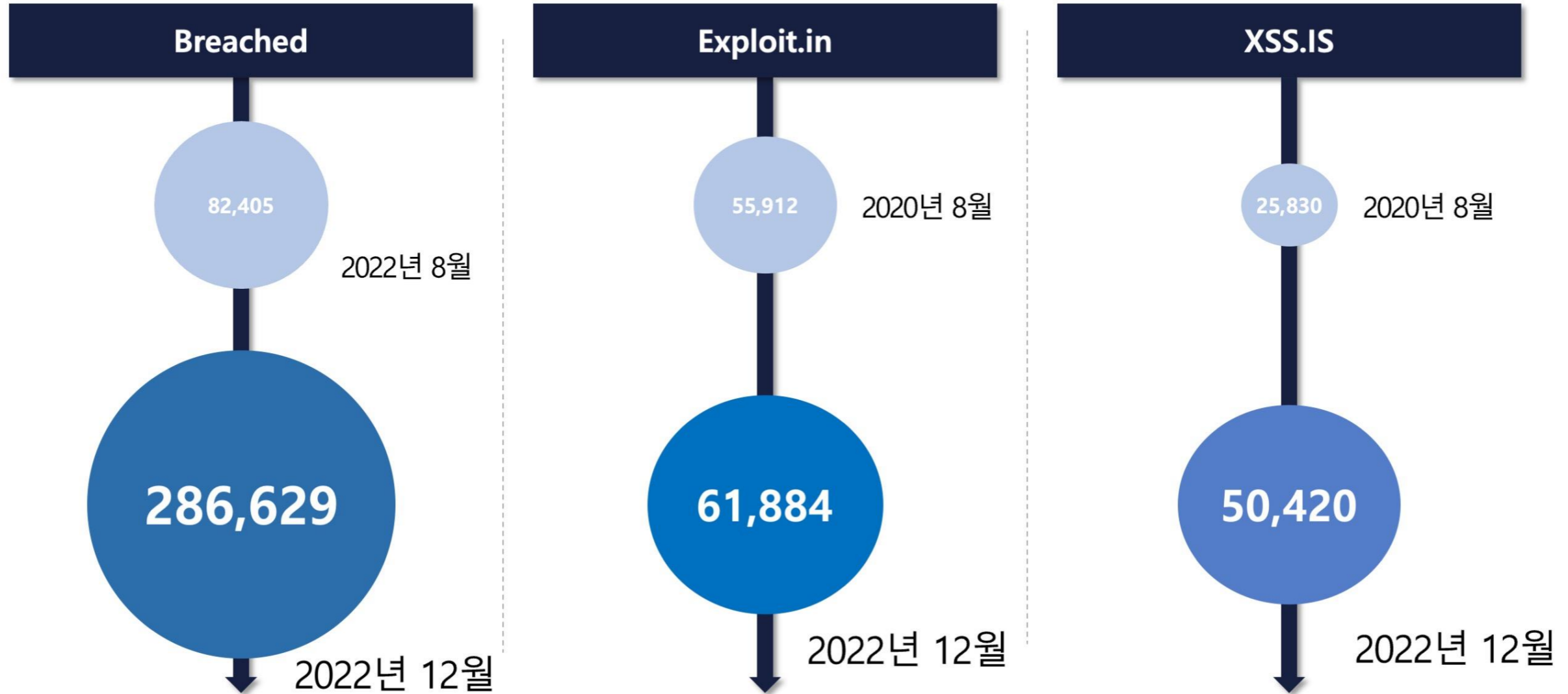
DATA LEAKAGE

The collage displays several types of leaked information:

- Top Left:** A form titled "보험금 지급 청구서" (Insurance Claim Form) and a "제적증명서" (Cancellation Certificate).
- Top Center:** A "1종보통" (Class 1 Ordinary) "자동차운전면허증 (Driver's License)" (Vehicle Driver's License) for a person from Gyeongbuk, with some details redacted.
- Top Right:** A "상품보증서" (Product Warranty Certificate) for a customer, and a "자동차보험가입증명서" (Vehicle Insurance Policy Certificate).
- Middle Left:** A "회의록" (Meeting Minutes) document titled "A사 내부 회의록" (Internal Meeting Minutes of Company A), dated 2020.11.19.
- Middle Center:** A technical diagram titled "D사 이메일 및 제품 도면" (Company D Email and Product Drawing).
- Middle Right:** A large spreadsheet with a green header and yellow body, containing multiple columns of data.
- Bottom Left:** A document titled "C사 내부 대외비 문서" (Internal External Document of Company C).
- Bottom Center:** A document titled "참석자 명단" (Attendee List) for a meeting.
- Bottom Right:** A document titled "B사 외부 평가단 협의 회의 참석자 명단" (Attendee List for Meeting with External Evaluation Team of Company B).

(4) 다크웹 최신 동향_사이버 범죄 공간 확대

딥/다크웹 3대 해킹 포럼의 유저 수 급증



(4) 다크웹 최신 동향_사이버 범죄 공간 확대

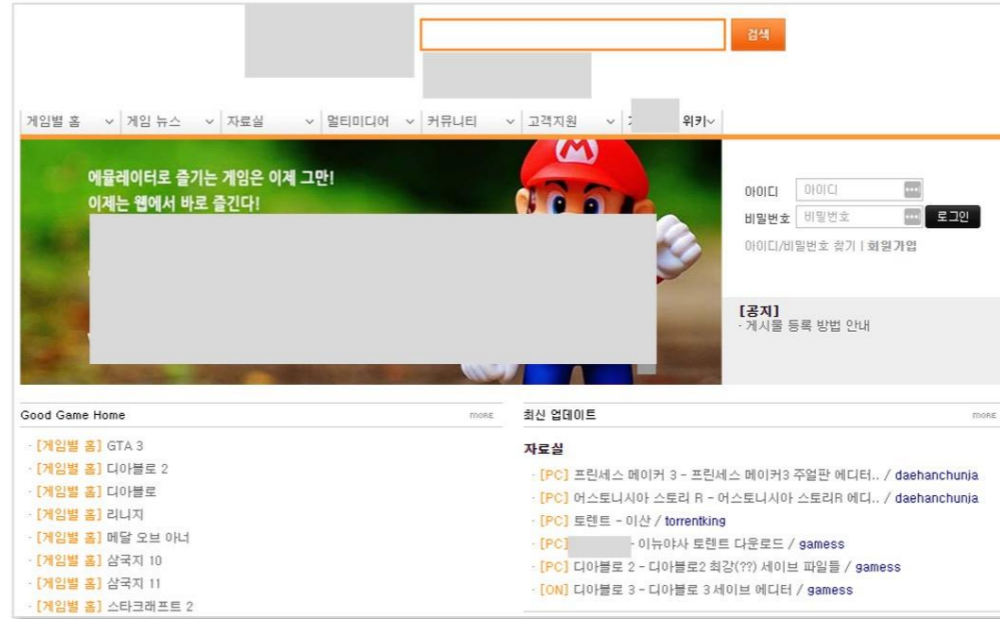
다크웹 + 텔레그램 채널로 사이버 범죄 공간 확대



(4) 다크웹 최신 동향_사이버 범죄 공간 확대

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

96W
 Korea data 2M
 Accounts 11lines
 =====
 id
 username
 ssn
 password
 name
 email
 zip
 address
 phone
 st1
 price
 gender
 dob



1	54,tjd	,0000-0-0	00:00:00,890	00	상	ng	@hanmail.net,	
1	55,g1	,0000-0-0	00:00:00,611	6-	19	jic	m.net,135-080	20
1	78,kdl	,0000-0-0	00:00:00,850	8-	id	la	lo@hotmail.co	0,
1	56,ho	,0,0000-0-0	00:00:00,	03	,1	4	315@hanmail	1,
1	57,sm	,0,0000-0-0	00:00:00,	06	7,6	6	e@ak.com,-,0	69
1	58,los	0000-0-0	00:00:00,900	2-	k6	조	nmir.com,-,01	29
1	60,aKl	0,0000-0-0	00:00:00,88	0-	js0	7	@hanmail.net,3	05
1	61,pal	,0,0000-0-0	00:00:00,9	09	,b	0	mat90@naver.c	1,
1	17,go	,0,0000-0-0	00:00:00,8	52	12	5,	@hanmail.net,7	-6
1	62,hrr	0000-0-0	00:00:00,560	2-	52	님	anmail.net,-,01	29
1	63,ok	,0,0000-0-0	00:00:00,85	24	jd	51	1224@hanmai	-4
1	64,jgt	000-0-0	00:00:00,83071	18	4	,le	korea.com,-,0	29
1	65,me	,0,0000-0-0	00:00:00,7	7-	,m	ill	@naver.com,-,1	12

(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 [redacted] source code! Our leak from breach includes:

DEVICES/HARDWARE


- Source code for every Trusted Applet (TA) installed on all Samsung device's TrustZone (TEE) with specific code for every type of TEE OS (Qualcomm) **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)
- Biometric source code for all recent Samsung devices, including Knox data and code for authentication.
- Various other data, confidential source code from Qualcomm.

ONLINE SERVICES

- Samsung activation servers source code (for first-time setup)
- Samsung **ACCOUNTS FULL SOURCE CODE!** Including Authentication, Identity, API, Services, and many more that wouldn't fit here!
- Various other data.

As always, enjoy! :)

LAPSUS\$

 [redacted]_LEAK.torrent
1.2 MB

68.8K 오전 5:29

901 comments

LAPSUS\$

****What should we leak next?***

Anonymous Poll

12.3K votes

35.3K 오전 9:12

1048 comments

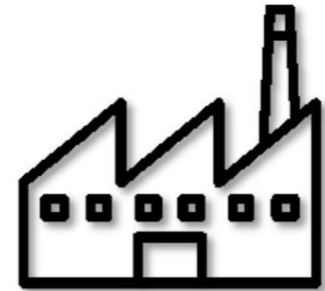
```
105 ST
106 ST
107
108 ST
109
110 /*
111 ST
112 /*
113 ST
114 /*
115 ST
116 /*
117 UI
118 UI
119
120 EFI_BLOCK_I02_TOKEN *Tokens = NULL;
121 #define MAX_TOKENS 4096
```


(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 게임을 타겟하여 공격하던 유저 포착

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

July 26, 2022, 05:07 AM (This post was last modified: July 26, 2022, 05:38 AM by pompompurin.)

donjuji
He drinks sprite.
GOD
Posts: 17
Threads: 11
Joined: Mar 2022
Reputation: 371

Hello BreachForums Community,
Today I have uploaded the [redacted] Database for you to download for free, thanks for reading and enjoy!

[redacted]

In approximately January 2022, the Forums for the MMORPG Gaming website [redacted] was breached by @donjuji, impacting 208k users. The breach included Email addresses, IP addresses, Usernames, Dates of birth and Passwords stored as bcrypt hashes.

Compromised data: Email addresses, IP addresses, Usernames, Dates of birth, Passwords

Contents

Hidden Content

https://cdn.breached.to/[redacted]

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

July 26, 2022, 04:47 AM (This post was last modified: September 21, 2022, 09:30 AM by pompompurin. Edit Reason: Official CDN Update.)

donjuji
He drinks sprite.
GOD
Posts: 64
Threads: 50
Joined: Mar 2022
Reputation: 543

Hello BreachForums Community,
Today I have uploaded the [redacted] Database for you to download, thanks for [redacted]

[redacted]

In May 2020, the Gaming forum (Now defunct & owned by C [redacted] S) G [redacted] suffered a data breach that Usernames, Email addresses, Dates of birth, IP Addresses and Passwords stored as MD5 (vBulletin) hashes.

Please note that a majority of the entries are botted, due to [redacted] not having [redacted]

Compromised data: Usernames, Email addresses, Dates of birth, IP Address

Contents

Hidden Content

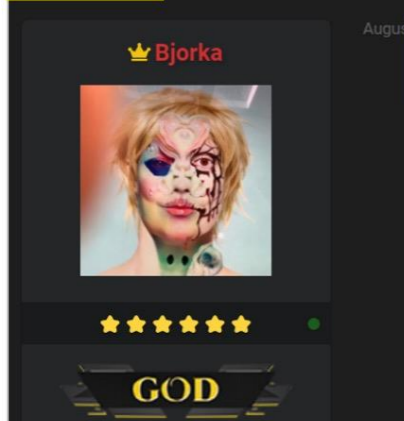
https://cdn.breached.to/[redacted]

Stream Your Bitch Checks My Valid's by Juji | Listen online for free on SoundCloud

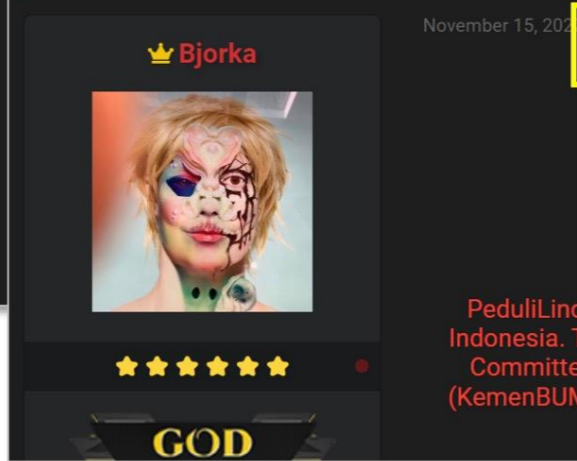
(4) 다크웹 최신 동향_특정 산업이나 국가를 공격하는 유저/집단

사건 2) 인도네시아를 집중 타격하는 유저 등장

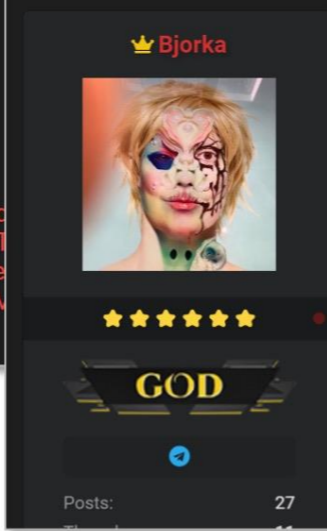
INDONESIA SIM CARD (PHONE NUMBER) REGISTRATION 1,3 BILLION
by Bjorka - Wednesday August 31, 2022 at 01:39 PM



INDONESIA COVID-19 APP PEDULILINDUNGI 3,2 BILLION
by Bjorka - Tuesday November 15, 2022 at 06:42 AM



INDONESIA CITIZENSHIP DATABASE FROM KPU 105M
by Bjorka - Tuesday September 6, 2022 at 10:06 AM



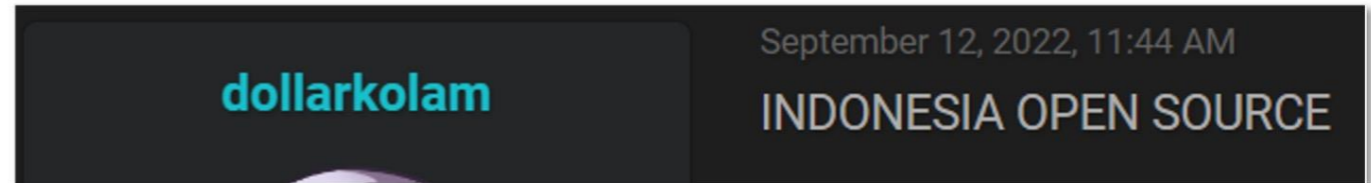
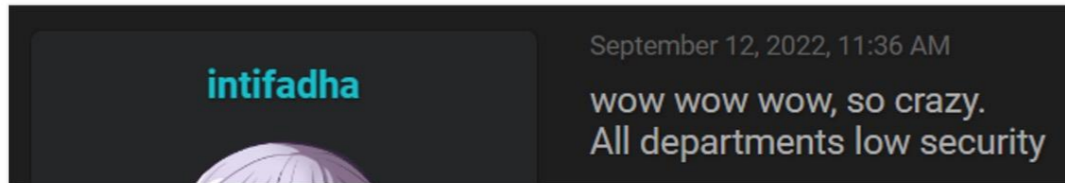
September 6, 2022, 10:06 AM (This post was last modified: January 23, 2023, 12:19 PM by Bjorka.)



The General Elections Commission

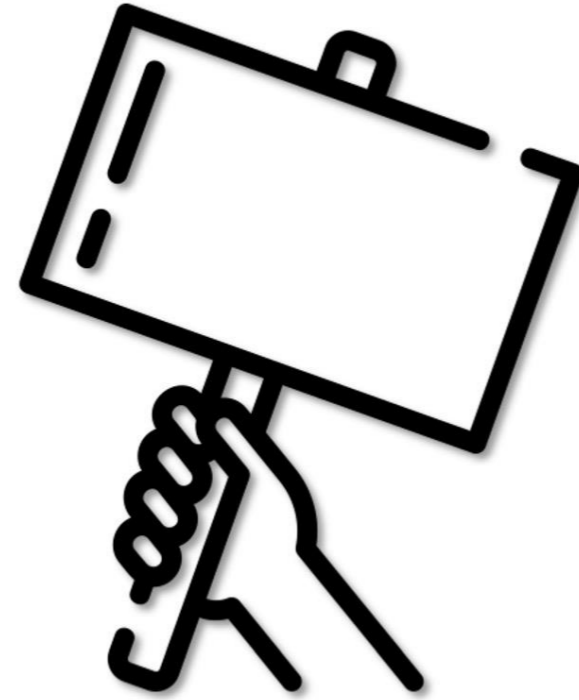
File Information

Compressed 4 GB



(4) 다크웹 최신 동향_해티비즘 활동 증가

반정부 성향을 사이버 공격을 통해 표출



Hacking (해킹) + Activism (정치행동주의) = Hacktivism

(4) 다크웹 최신 동향_해킹비즈니스 활동 증가

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

Kiaman Danesh Iran Database
19,591 Documents

#OPIRAN

We wanted to publish this data against the oppressive regime of the Iranian government.

SOURCE: Mc [redacted] s Iran

production, trade, sales & distribution of specialized chemicals in the territory of Iran. Specialty chemical distribution

TYPE OF LEAK: #DATABASE

COUNTRY: #IRAN

DATABASE FORMAT: #PDF - #DOCX - #XLS - #SQL

DATABASE CONTENTS:

19,591 Documents SIZE: 1,21 GB
DataBase SQL SIZE: 545 MB

DATABASE PASSWORD:
https://t.me/ai [redacted] nel

FOR MORE DATABASE FOLLOW US.

6104 오전 1:33

ARES_PRIVATE_M [redacted] s Iran.rar
35.2 / 1193.2 MB

6116 오전 1:33

1 comment

ما به وبسایت وزارت خارجه حکومت تروریستی اسلامی د ddos حمله...
We attacked the website of the M [redacted] irs of Iran as a warning to the terrorist regime and in support of the protesters

1702 Ali, 오후 8:27

1 comment

در حال به روز رسانی...
سایت مورد نظر در حال به روز رسانی میباشد.
لطفا مجدداً تلاش نمایید
وزارت امور خارجه

حمله ddos ما به وبسایت وزارت خارجه حکومت تروریستی اسلامی دست از دروغ پراکتی و کشتار مردم بردارید

#Fuckgovernment

#مرگ_بر_خامنه_ای

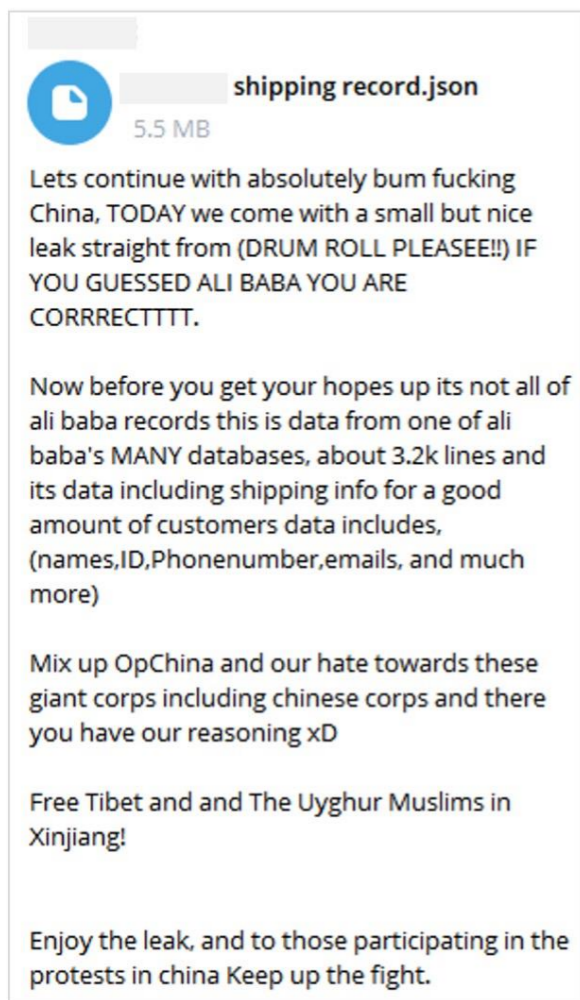
https://check-host.net/check-http?host=https://mfa.gov.ir/

1697 Ali, edited 오후 8:22

Leave a comment

(4) 다크웹 최신 동향_해티브이즘 활동 증가

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



shipping record.json
5.5 MB

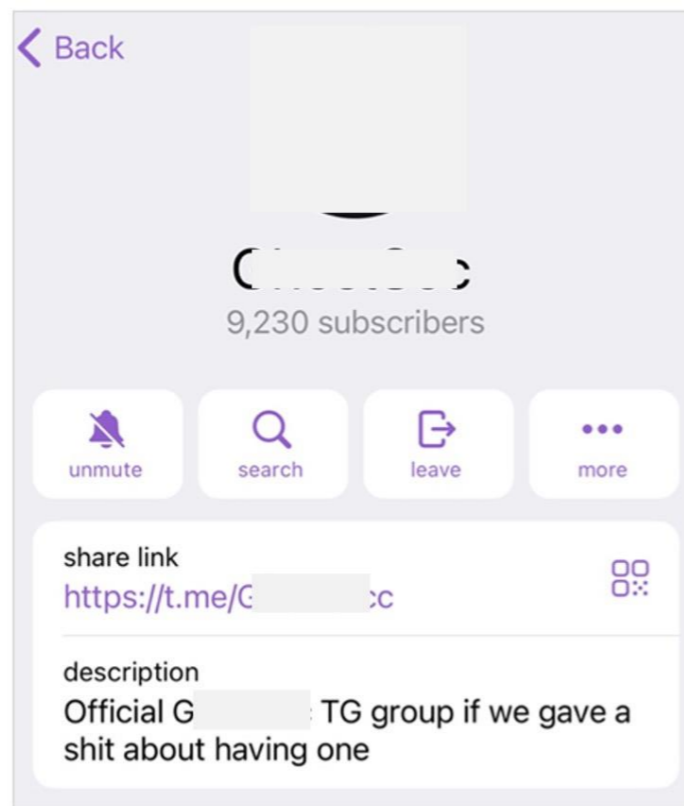
Lets continue with absolutely bum fucking China, TODAY we come with a small but nice leak straight from (DRUM ROLL PLEASEE!!) IF YOU GUESSED ALI BABA YOU ARE CORRECTTTT.

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.



Back

9,230 subscribers

unmute search leave more

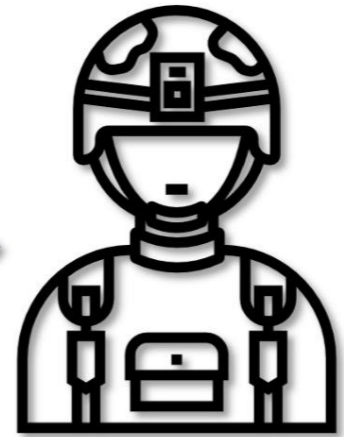
share link
<https://t.me/C...>

description
Official G... : TG group if we gave a shit about having one

```
a5d", "orderNumber": "HY24125598200759808", "shipmentStatus": "DELIVERED", "c
a5e", "orderNumber": "HY24156416738592256", "shipmentStatus": "SHIPPED", "ord
a5f", "orderNumber": "HY24161328524428800", "shipmentStatus": "DELIVERED", "c
a60", "orderNumber": "HY24194075955561984", "shipmentStatus": "DELIVERED", "c
a61", "orderNumber": "HY24210024364508672", "shipmentStatus": "CANCELLED", "c
a63", "orderNumber": "HY24216911780775424", "shipmentStatus": "SHIPPED", "ord
a64", "orderNumber": "HY24310188626413056", "shipmentStatus": "SHIPPED", "ord
a65", "orderNumber": "HY24524130753709568", "shipmentStatus": "DELIVERED", "c
a69", "orderNumber": "HY24826176300123648", "shipmentStatus": "CANCELLED", "c
a6a", "orderNumber": "HY24827695158265344", "shipmentStatus": "CANCELLED", "c
a6b", "orderNumber": "HY25083253379565056", "shipmentStatus": "DELIVERED", "c
a6c", "orderNumber": "HY28499896046716416", "shipmentStatus": "DELIVERED", "c
a6d", "orderNumber": "HY28503510928590336", "shipmentStatus": "DELIVERED", "c
a6e", "orderNumber": "HY28511065809618432", "shipmentStatus": "SHIPPED", "ord
a6f", "orderNumber": "HY28549391610545664", "shipmentStatus": "SHIPPED", "ord
a70", "orderNumber": "HY29915190870935040", "shipmentStatus": "DELIVERED", "c
a71", "orderNumber": "HY31560602384074240", "shipmentStatus": "SHIPPED", "ord
a72", "orderNumber": "HY36544684998264320", "shipmentStatus": "SHIPPED", "ord
a73", "orderNumber": "HY37496922553976320", "shipmentStatus": "DELIVERED", "c
a74", "orderNumber": "HY37535559974913536", "shipmentStatus": "SHIPPED", "ord
a75", "orderNumber": "HY37626468934616576", "shipmentStatus": "DELIVERED", "c
a76", "orderNumber": "HY37696842904897024", "shipmentStatus": "SHIPPED", "ord
a77", "orderNumber": "HY37702230958147072", "shipmentStatus": "SHIPPED", "ord
a78", "orderNumber": "HY37754964931511808", "shipmentStatus": "SHIPPED", "ord
a79", "orderNumber": "HY38229217195853312", "shipmentStatus": "DELIVERED", "c
```

(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

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://\[redacted\].sh/](http://[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 7COIMt7QU-YPwMub8z_SQ 150 0 22375506 1749307 25.2gb 25.2gb
nb_theme_address_company_dwd-total fpmEYB9SI6WvHnZIEwIA 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 g5f614LQcGL3oQ60N2Bbw 150 0 2017931 0 4.3gb 4.3gb
person_address_label_info_master t64pp9WnS3maY9jBzTtiw 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

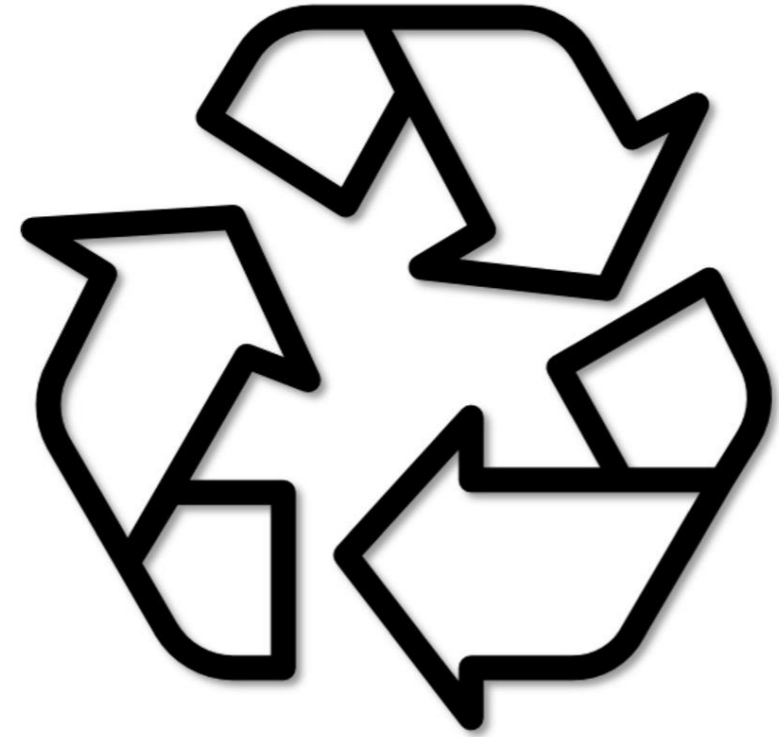
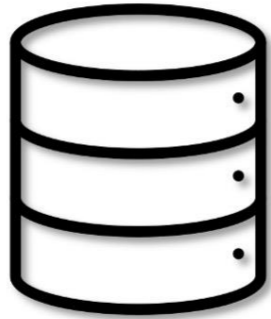
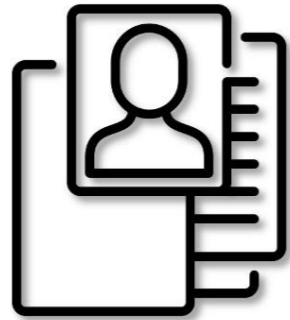
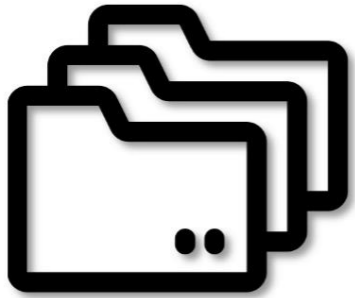
Sample of 3 main databases: <https://gofile.io/d/WIFNj0>

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

```
{ "CASE": { "BRIEF_CASE": "2015年08月11日13时00分,报警" }, "TYPE": null }
{ "CASE": { "BRIEF_CASE": "2008年11月8日20时34分,报警" }, "TYPE": null }
{ "CASE": { "BRIEF_CASE": "2011年08月08日10时27分,报警" }, "TYPE": null }
{ "CASE": { "BRIEF_CASE": "2016年08月16日10时44分,报警" }, "TYPE": null }
{ "CASE": { "BRIEF_CASE": "2007年9月13日上午11时接到11" }, "TYPE": null }
{ "CASE": { "BRIEF_CASE": "2010年10月06日16时53分,报警" }, "TYPE": null }
{ "CASE": { "BRIEF_CASE": "2019-06-09 14:44:48,手机号" }, "TYPE": null }
{ "CASE": { "BRIEF_CASE": "2016年05月22日17时26分,报警" }, "TYPE": null }
{ "CASE": { "BRIEF_CASE": "2014年10月20日14时46分,报警" }, "TYPE": null }
{ "CASE": { "BRIEF_CASE": "2012年04月14日03时02分,报警" }, "TYPE": null }
{ "CASE": { "BRIEF_CASE": "2002年8月18日上午11时30分左" }, "TYPE": null }
{ "CASE": { "BRIEF_CASE": "2019-06-23 20:39:36,手机号" }, "TYPE": null }
{ "CASE": { "BRIEF_CASE": "2007年3月28日晚20时20分许,家" }, "TYPE": null }
{ "CASE": { "BRIEF_CASE": "2010年5月8日14时30分许,我所" }, "TYPE": null }
{ "CASE": { "BRIEF_CASE": "2013年08月22日14时40分,报警" }, "TYPE": null }
```


(4) 다크웹 최신 동향_데이터의 끊임없는 재유통

1차 데이터 유출 이후 2차, 3차 재공유되는 데이터



(4) 다크웹 최신 동향_데이터의 끊임없는 재유통

국내 온라인 주류 쇼핑몰 데이터, 과거 유출된 데이터의 재공유

a [redacted] || full database download (mega) | Korean Database
by ranzap001 - Sunday September 4, 2022 at 06:15 PM

September 4, 2022, 06:15 PM
The csv file contains the following details of more the 18k korean residents:
m_no,m_id,level,name,nickname,password,status,resno1,resno2,sex,birth_year,birth,calendar,email,zipcode,company,service,item,busino,emoney,mailling,sms,mariyn,marridate,job,interest,regdt,last_login,last_logout,recommid,ex1,ex2,ex3,ex4,ex5,ex6,LPINFO,private1,private2,private3,dupeinfo,foreigner,pakey,rncheck,info

Link:
Hidden Content
https://mega[redacted]Do_mc4

ranzap001
BreachForums User
MEMBER
Posts: 9
Threads: 6
Joined: Sep 2022
Reputation: -30

South Korea - a [redacted] p. Kr-database
by ckckck8088 - March 24, 2020 at 08:34 AM

March 24, 2020 at 08:34 AM This post was last modified: March 24, 2020 at 09:04 AM by ckckck8088.

I'm happy to share this data with you. I hope you like it~Quantity: 188789
m_id , level , name , nickname , password , status , resno1 , resno2 , sex , birth_year , birth , calendar , email , zipcode , company , service , item , busino , emoney , mailling , sms , mariyn , marridate , job , interest , regdt , last_login , last_logout , recommid , ex1 , ex2 , ex3 , ex4 , ex5 , ex6 , LPINFO , private1 , private2 , private3 , dupeinfo , foreigner , pakey , rncheck , info


full data
You must register or login to view this content.

ckckck8088
V.I.P User
VIP
Posts: 11
Threads: 4
Joined: Mar 2020
Reputation: 1
1 YEAR OF SERVICE

```
nm_no,m_id,level,name,nickname,password,status,resno1,resno2,sex,birth_year,birth,calendar,email,zip
0, [redacted] 7F62FA356E5C96232129C98B7556B0AB9514B3D8,1,d41d8cd98f00b204e9800998ecf8
100 [redacted] *A114F30AAE0C508121F7CFCDFA14E34CE9074E1,1,e1c0a9b507cf1eedaa329b93859
131 [redacted] ,*2B3F582C05D8A0BBC84681876A381D0C8257E22B,1,1c17b54b643f0421dd0e48662
ljh [redacted] 자루,*F19D21492C461854564C5E8172F519784525A025,1,1af4ae2ff2272ebec16964c
1,홍 [redacted] C6CA864B217C83B06D8B1807125735962322D86,1,1cdb45b47d6a8fffd15232829e86f
,10 [redacted] e,*3F94BE801470D3CA382A3E57D93498FFB5ABA9EC,1,108f8456f367a5f60bbc07b4
6457,30123,10,김민성,김민성,30BE60EBD13581C22D26DD84ADDD7705D1499576,1,d41d8cd98f00b204e9800998ecf8
```

(4) 다크웹 최신 동향_데이터의 끊임없는 재유출

ALPHV(BlackCat) 랜섬웨어 onion 사이트

 2022-07-05

Su[REDACTED] IV 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 breach-surfing - Al [REDACTED] 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\[REDACTED\].password](http://vqifk[REDACTED].password)
[http://vqifk\[REDACTED\].lohn%20Hannan](http://vqifk[REDACTED].lohn%20Hannan)
[http://vqifk\[REDACTED\].let%20income%20](http://vqifk[REDACTED].let%20income%20)

ALPHV Collections | Search | Explore | Meta

Simple query string or partial path: *doc*.txt or *

Found 64120 files, Indexed 61456 resources.

Al [REDACTED] ns | Search | Explore | Meta

Q .pdf

About 14 results

data [REDACTED] contract.zip

Sc [REDACTED] 1 Contract.zip

Sch [REDACTED] 17227_Schrenk Consulting LLC_106003_2021-12-01.pdf

data [REDACTED] tro.docx

all [REDACTED] tter for maestro.docx

://w [REDACTED] its-Menu-Of-Serv

M [REDACTED] content/uploads/bsk-pdf-manager/2022/02/Spa-T...

Match #5: .pdf to view our menu or spa services. We look forward to providing authenti...

data [REDACTED] 0210903152221.pdf

Sp [REDACTED] 210903152221.pdf

2021-09-03T13:59:10-0700 Digitally verifiable PDF exported from www.docusign.com

(5) 정리

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

대응도 중요하지만, 사건 사고에 대한 예방도 중요함



김다솜

위협 분석가

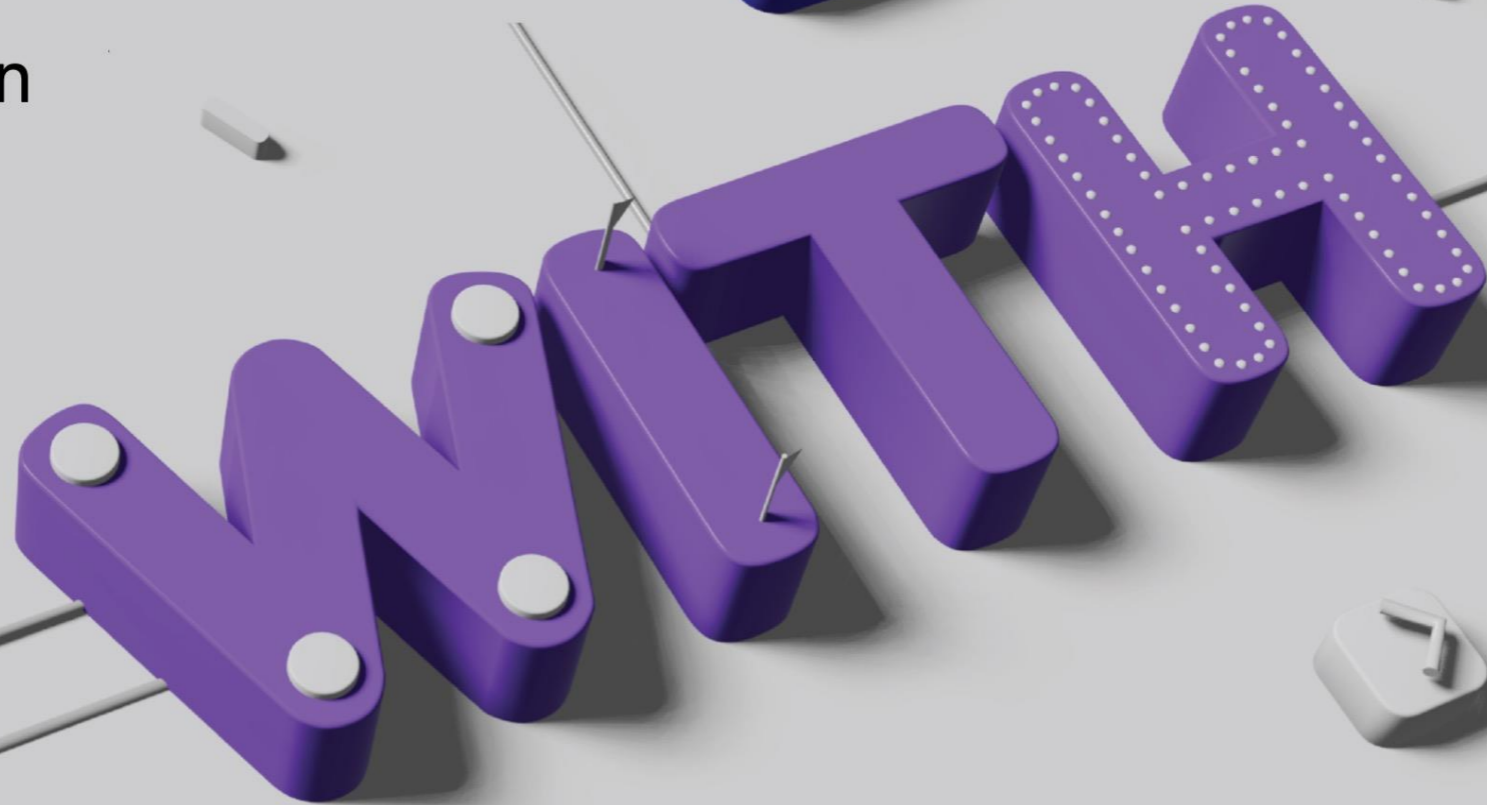
사이버 위협 탐지 및 대응 관련 연구개발

The information contained in this document is proprietary and confidential.
If you are not the intended recipient, please note that any use or circulation of this document may be cause for legal action.

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.

OSINT

가상자산
추적·분석

**사이버 범죄자
프로파일링**

익명채널
데이터 영향도
분석

위협데이터
수집·분석
자동화

계정 유출 현황

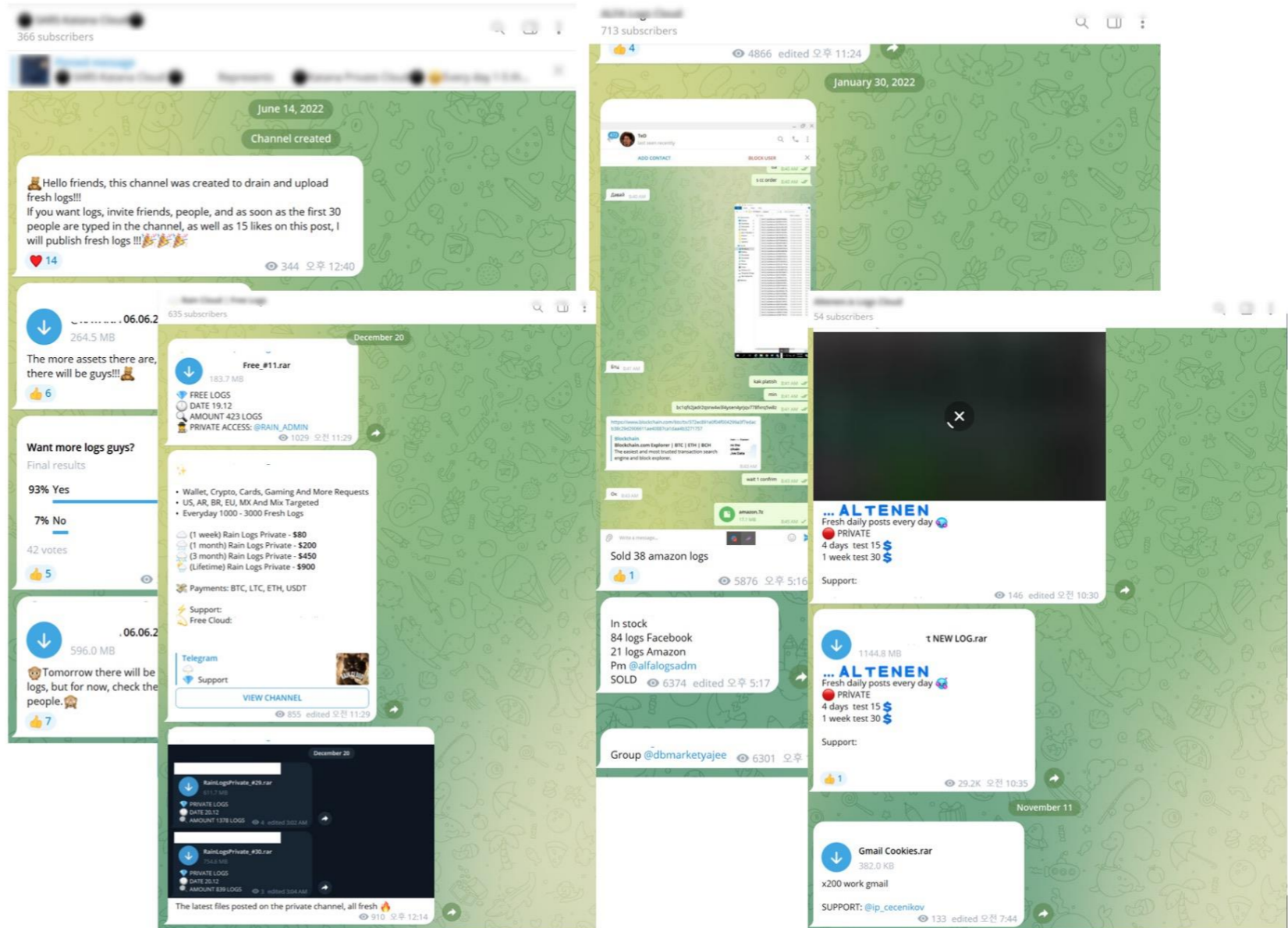
스틸러 로그

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

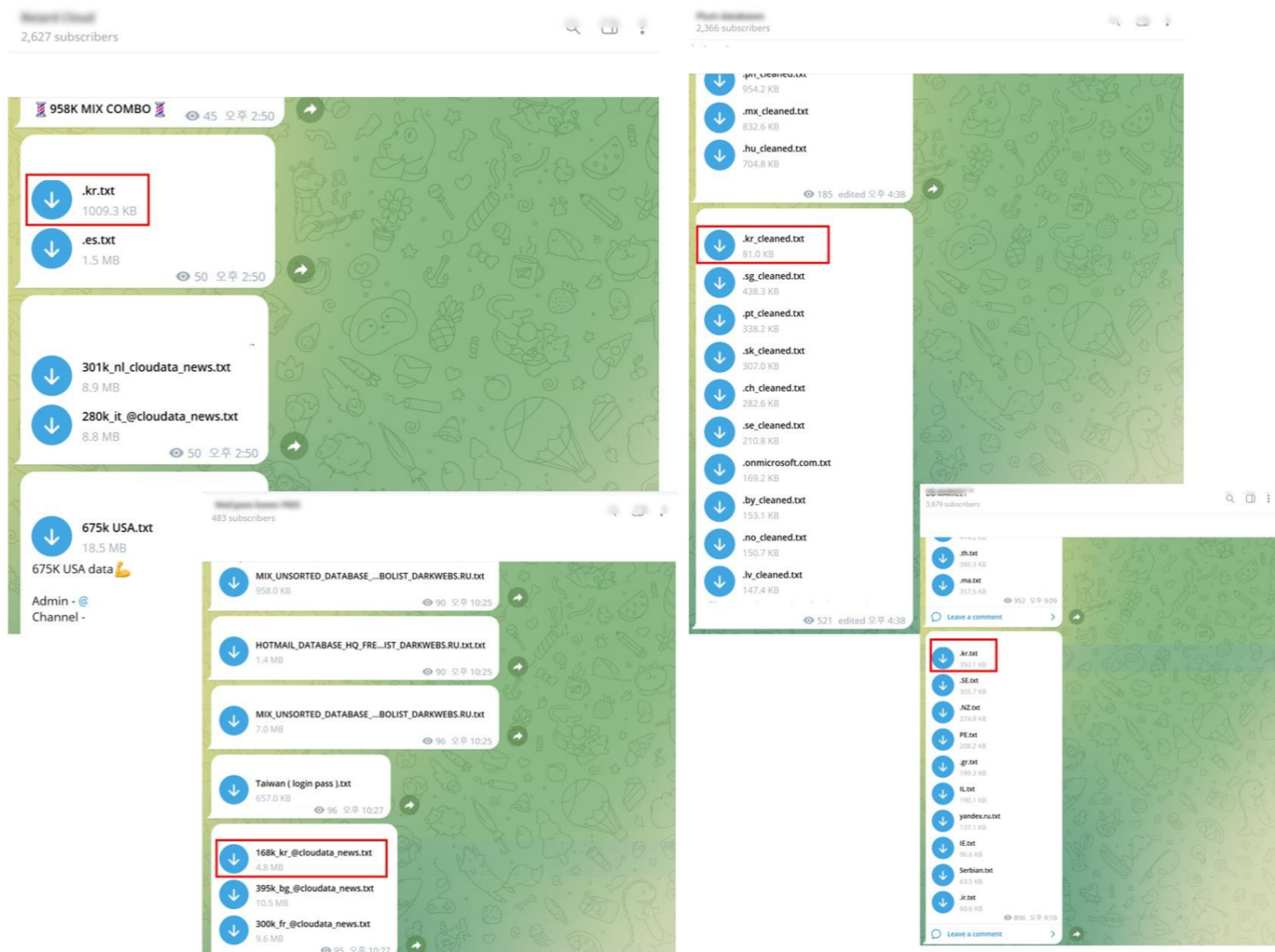
**파일명 kr, korea 관련 키워드 포함

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

시나리오 1. GitHub 상에서 임직원 MySQL 계정 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 메시지와 함께 GraphQL 설정값을 업로드함.
- 해당 사용자에게 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    
```

```
1 import {SequelizeModuleOptions} from "@nestjs/sequelize";
2 import {Log} from "../logs/log.model";
3 require('dotenv').config()
4
5 const dbConfig = (env: string): SequelizeModuleOptions => {
6   switch(env) {
7     case 'development':
8       return {};
9     case 'production':
10      return {};
11     // default -> dev db
12     default:
13       return {
14         dialect: 'mysql',
15         // [REDACTED]
16         // [REDACTED]
17         username: [REDACTED],
18         password: [REDACTED],
19         database: 'latency_log',
20         models: [Log],
21         timezone: '+09:00',
22         define: {
23           timestamps: false
24         },
25       };
26   }
27 };
28
29 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, 비밀번호, 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
1 # MySQL dump 7.1
2 #
3 # Host: cghost Database: gumpu
4 #-----
5 # Server version 3.23.51-log
6
7 #
8 # Table structure for table 'mailinglist'
9 #
10 CREATE TABLE mailinglist (
11   email varchar(30) DEFAULT '' NOT NULL,
12   name varchar(20) DEFAULT '' NOT NULL,
13   randno varchar(10) DEFAULT '' NOT NULL,
14   PRIMARY KEY (email)
15 );
16
17 #
18 # Dumping data for table 'mailinglist'
19 #
20
21 INSERT INTO mailinglist VALUES ('12345678901234567890', '12345', '1234567890');
22 INSERT INTO mailinglist VALUES ('12345678901234567890', '12345', '1234567890');
23 INSERT INTO mailinglist VALUES ('12345678901234567890', '12345', '1234567890');
```








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

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	2021-01-12 오후 8:15
 Cookies	2021-01-12 오후 8:15
 Files	2021-06-16 오전 12:35
 hardware.txt	2020-12-24 오후 2:46
 ip.txt	2020-12-24 오후 2:46
 passwords.txt	2020-12-24 오후 2:46
 screenshot.jpeg	2020-12-24 오후 2:46

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	담당매니저	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		

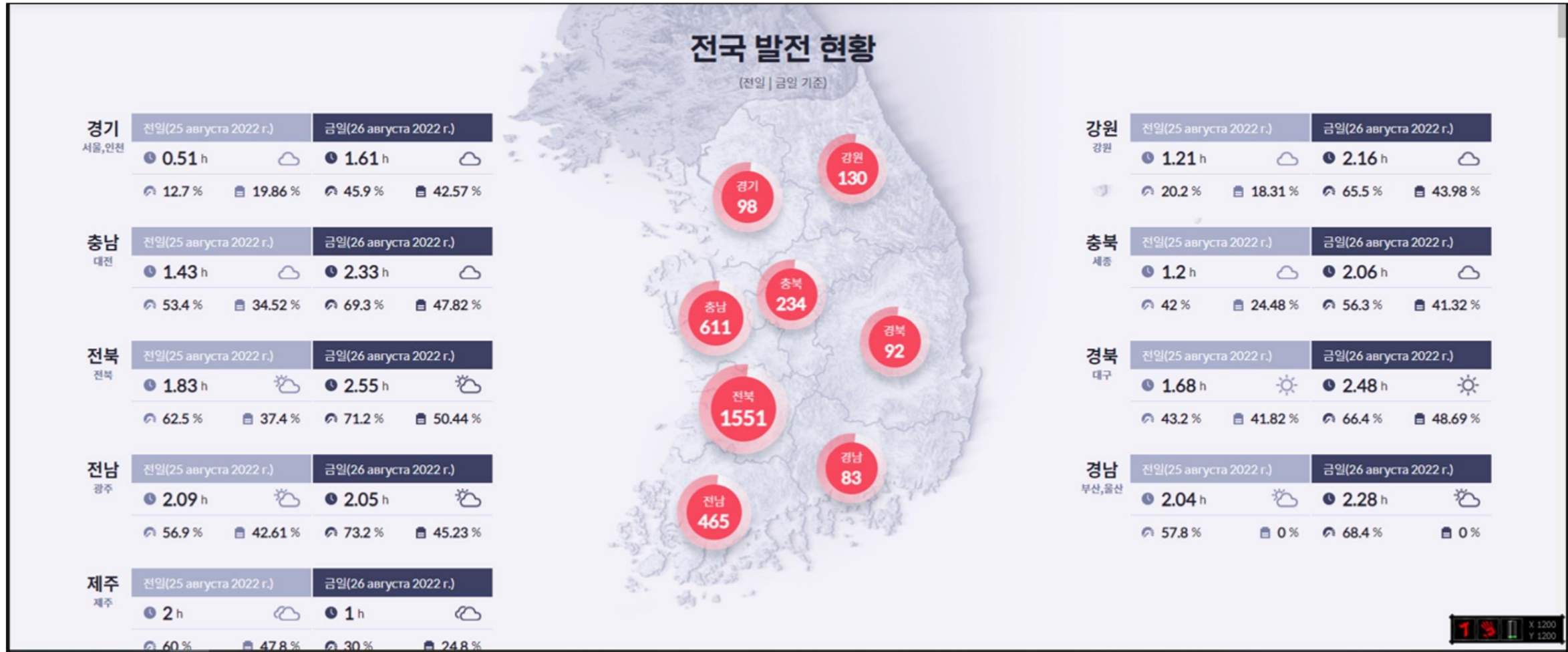
대응방안

- **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 비밀번호 초기화 조치

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

The screenshot displays the Quaxar platform interface. At the top, there is a navigation bar with the Quaxar logo, menu items for Alerts, Report, and Intelligence Vault, a search bar labeled 'Search Quaxar', and a language selector. Below the navigation bar, a list of alerts is shown. The first alert (ID 65) is titled 'Онлайн казино Тайланд суппорт доступ. Цена - 4000\$' and the second (ID 66) is 'Онлайн казино Тайланд админ доступ. Цена - 10000\$'. Both alerts include contact information: 'Контакты - ЛС, ТОХ - E75E9544618128DDD730C68467BEEF57BCF8303BF493B5EFB77C6094D684AD3F339ADCDF2CB2'. The first alert has a 'Жалоба' (Report) button and 'Like' and 'Answer' icons. Below the alerts, a user profile for 'NikaC (L1) cache' is visible. The profile includes a 'Пользователь' (User) button and statistics: 'Регистрация : 06.11.2021', 'Сообщения : 563', 'Реакции : 137', and 'Гарант сделки : 2'. A post from this user, dated 'Четверг в 16:05', is shown with the title '67. Системы мониторинга электростанций Южной Кореи админ доступ. Цена 5000\$' and the same contact information. It also features a 'Жалоба' button and 'Like' and 'Answer' icons. A 'Автор темы' (Topic author) badge is present on the post.

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



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

```
UserInformation.txt
*****
*                                     *
*  REDLINE                           *
*                                     *
*  Telegram: https://t.me/REDLINEVIP  *
*                                     *
*****
Build ID: REDLINEVIP (Telegram: @Fatherofcarder)
Current Language: Korean (Korea)
ScreenSize: {Width=1920, Height=1080}
TimeZone: (UTC+09:00) 서울
Operation System: Windows 10 Enterprise x64
UAC: AllowAll
Process Elevation: False
Log date: 8/16/2022 5:21:47 PM

Available KeyboardLayouts:
Korean (Korea)
```

kaboom karavan

Keil Mdk Arm 5 Keygen Download
yanigaut

2021. 8. 29. 10:18 · 카테고리 없음

[Click DOWNLOAD NOW](#)

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)

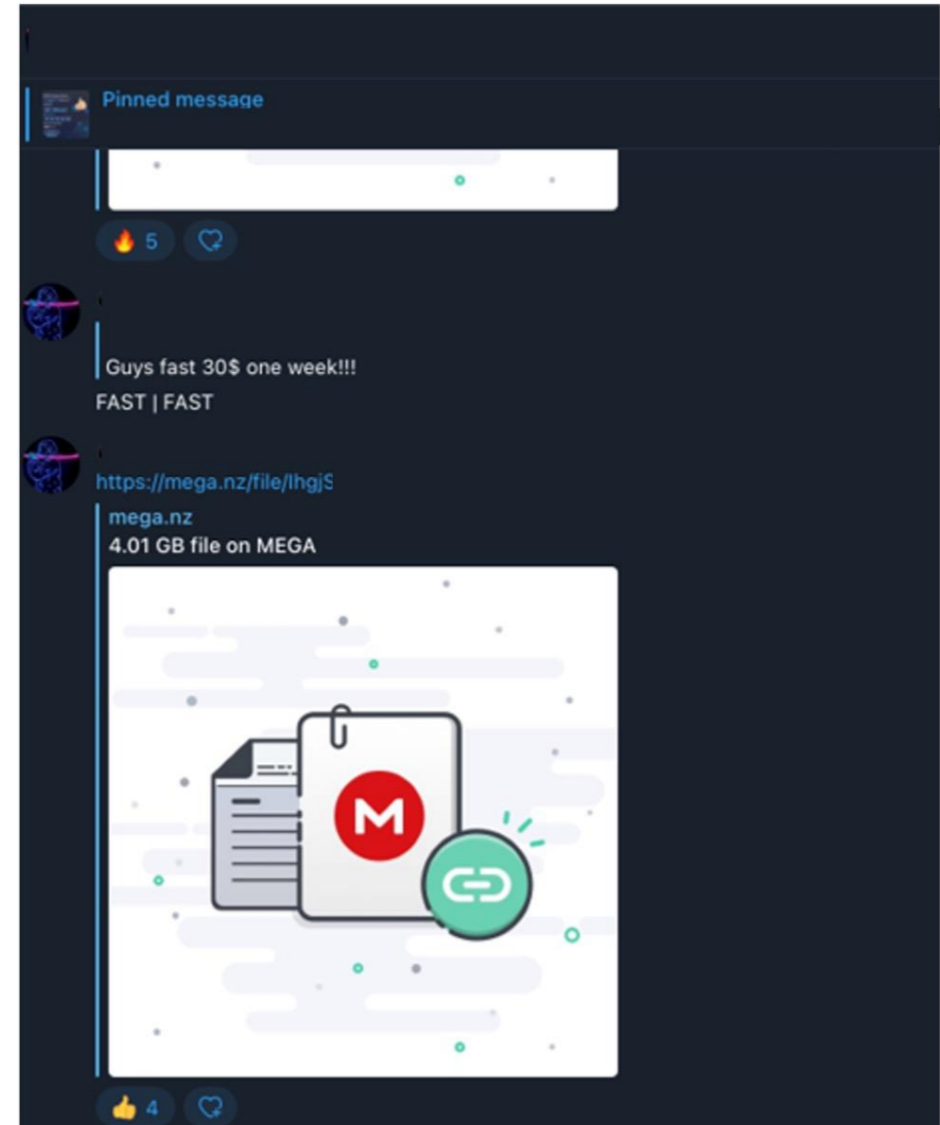
- https://t.me/lo*****free/73

(2022-08-23) B*** O***N

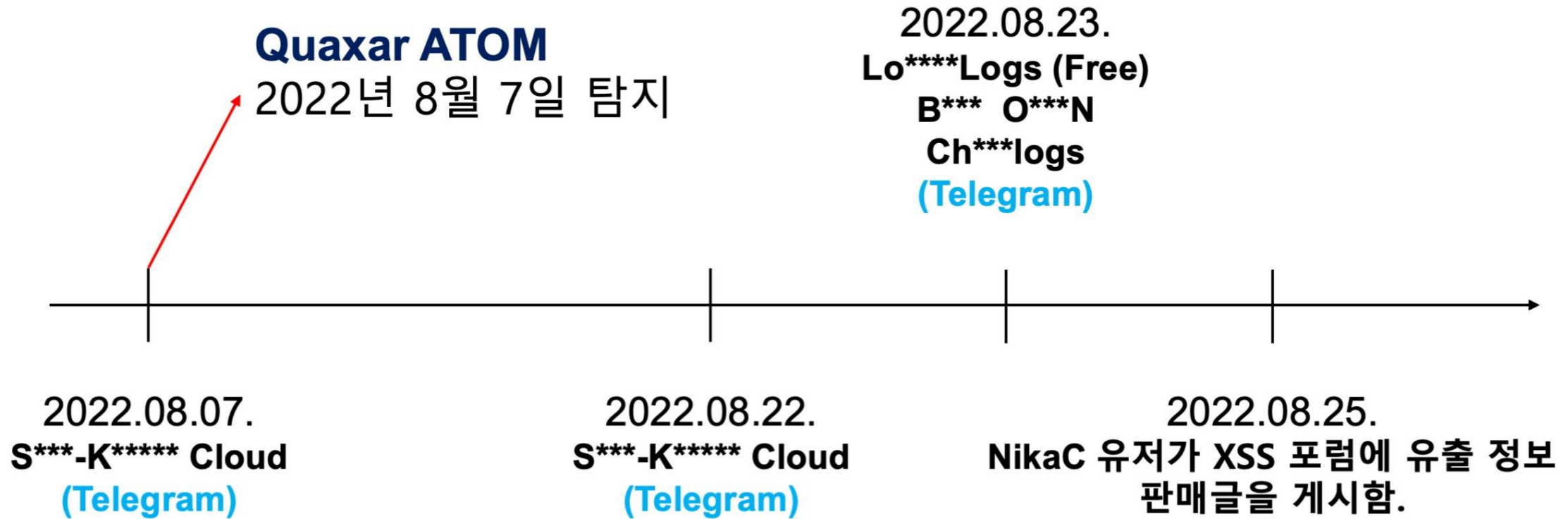
- https://t.me/re*****eo****1/221607

(2022-08-23) Cha*****

- https://t.me/cha*****/37758



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



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 업체로부터 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.



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

The information contained in this document is proprietary and confidential.
If you are not the intended recipient, please note that any use or circulation of this document may be cause for legal action.

QnA