



# 다크웹 내 위협 행위자 분석

포럼 가입과 정보 탐색

BCG 정보보호연구실 조대인



## 네트워크 상에서 자신을 숨기는 법

- Tor 브라우저를 이용
- 익명메일(Proton mail, tuta mail 등) 사용
- onion을 사용



## Tor에 연결하기


Tor 브라우저는 전세계 수천명의 자원 봉사자에 의해 운영되는 Tor 네트워크와 당신을 연결합니다.

☐ 항상 자동으로 연결

연결 구성중...

연결

# Proton 이메일 가입



[All](#) [Images](#) [Videos](#) [News](#) [Maps](#) [Shopping](#) [Chat](#) [Settings](#)

Always private Austria Safe search: moderate Any time

<https://proton.me>  
[Proton: Privacy by default](#)  
Proton offers encrypted email, VPN, cloud storage, password manager, and calendar with end-to-end encryption and Swiss privacy. Proton is a non-profit founded by CERN scientists and supports freedom of speech and information online.

### Mail

By choosing Proton, you join a movement of millions of volunteers...

### Create a Free Account

Proton Mail provides encrypted, secure email for over 100 million people and...

### Get Started With Proton

Download Proton Mail on your mobile device and log in to your account. Get...

### Sign In

Sign in to your Proton Account to access all encrypted Proton services...


### Pricing

More information A vault in Proton Pass is an encrypted digital container that...


### Password Manager

Proton Pass uses the same battle-tested end-to-end encryption as other Proton...

# 프로톤 메일 가입

 Proton Mail


Overview Security Pricing Bridge Download Support



### Keep your emails private

Proton Mail's end-to-end encryption and zero-access encryption ensure only you can see your emails. Not even Proton can view the content of your emails and attachments.


- End-to-end encryption
- Zero-access encryption
- Password-protected and expiring emails



### Block email trackers

Email trackers tell senders and advertisers what you read and click on, and can follow you around the web. Proton Mail protects you from these digital spies and prevents companies from monitoring you.


- Email tracking protection
- Tracking links protection
- No ads



### Trusted and reliable

Proton is incorporated and headquartered in Switzerland, meaning your data is protected by some of the world's strictest privacy laws. We also provide strong technical protections for your data.

- Protected by Swiss data privacy laws
- Open source and publicly audited
- Hosted on our own servers



## 프로톤 메일 가입

SAVE 0%

### Proton Free

€0/month

[Get Proton for free](#)

No credit card required

- ✓ Up to 1 GB Mail storage
- ✓ 1 user
- ✓ 1 email address

SAVE 20%

### Mail Plus

€4.99  
€3.99/month

Save €12

[Get Mail Plus](#)

30-day money-back guarantee

- ✓ 15 GB storage
- ✓ 1 user
- ✓ 10 email addresses
- ✓ Support for 1 custom email domain
- ✓ Unlimited folders, labels and filters

Premium value included

Mail Calendar

RECOMMENDED

SAVE 23%

### Proton Unlimited

€12.99  
€9.99/month

Save €36

[Get Proton Unlimited](#)

30-day money-back guarantee

- ✓ 500 GB storage
- ✓ 1 user
- ✓ 15 email addresses
- ✓ Support for 3 custom email domains
- ✓ Unlimited folders, labels and filters

Premium value included

Mail Calendar VPN Drive Pass

SAVE 20%

### Proton Family

€29.99  
€23.99/month

Save €72

[Get Proton Family](#)

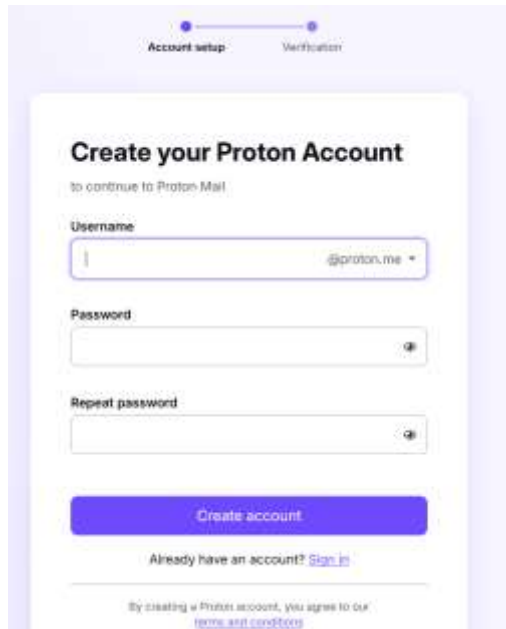
30-day money-back guarantee

- ✓ 3 TB storage
- ✓ Up to 6 users
- ✓ 90 email addresses
- ✓ Support for 3 custom email domains
- ✓ Unlimited folders, labels and filters

Premium value included

Mail Calendar VPN Drive Pass

# 프로톤 메일 가입



The image shows a mobile app interface for creating a Proton account. At the top, there's a progress bar with two dots; the first dot is active, labeled 'Account setup', and the second is labeled 'Verification'. Below this, the main heading is 'Create your Proton Account' with a subtitle 'to continue to Proton Mail'. The form consists of three input fields: 'Username' (with a placeholder '@proton.me'), 'Password', and 'Repeat password'. Each field has a small icon on the right side. Below the fields is a large blue button labeled 'Create account'. At the bottom, there's a link 'Already have an account? Sign in'. A footer note states 'By creating a Proton account, you agree to our terms and conditions' with a link to the terms and conditions.

Account setup    Verification

## Create your Proton Account

to continue to Proton Mail

Username

@proton.me

Password

Repeat password

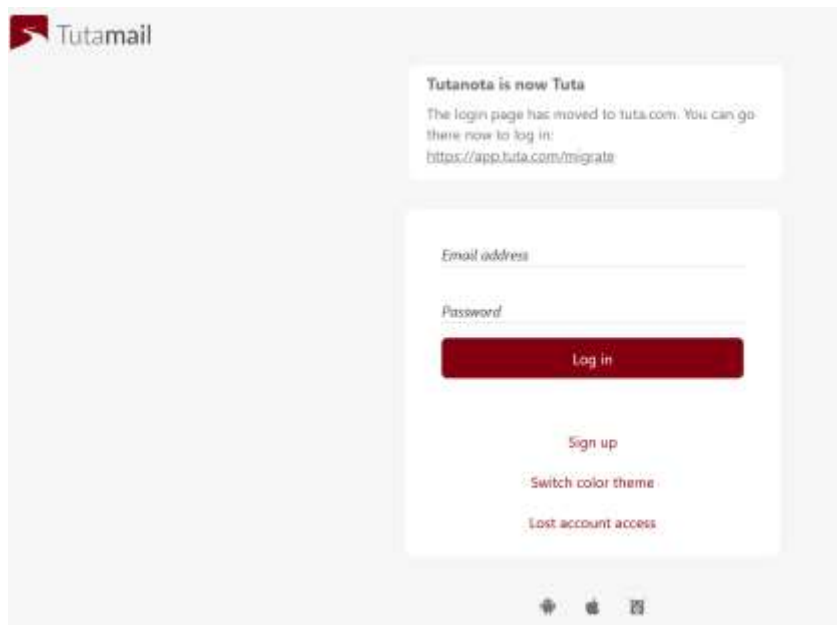
Create account

Already have an account? [Sign in](#)

By creating a Proton account, you agree to our [terms and conditions](#)

## 이외에 메일 서비스

- tutanota







## 다크웹 포럼

1. XSS.is 포럼
2. Breach 포럼
3. RAMP 포럼
4. Exploit포럼
5. ...



## XSS.is 포럼

- 2013년에 출시된 러시아 최고의 다크웹 포럼이다.
- 다루는 주요 주제로는 악성코드, 취약점, 카딩(타인의 카드를 되파는 것) 및 자격 증명 등이 있다.

<https://webz.io/dwp/xss-the-top-russian-dark-web-forum/>



## Breach 포럼

- 해킹된 데이터베이스와 개인정보를 거래하거나 무료 배포하는 포럼
- 이메일 인증만으로 가입되어 많은 유저들이 이용하였으나 5월 15일 FBI에 의해 압수됨.



## RAMP 포럼

- 랜섬웨어 관련 활동을 위한 주요 허브, 다양한 사이버 범죄자들이 정보를 교환하고 협력
- 가입 조건: 다른 주요 포럼(XSS.is, Exploit 등)에서 두달 이상 활동 및 최소 10개 이상 게시물 작성




## 포럼 상에서 중요 데이터 추출

- 포럼에서 OSINT를 통해 활용 가능한 데이터 수집
- 대상의 게시물, 프로필 등을 참조



## Initial Access broker(IAB)

- 컴퓨터 시스템과 네트워크에 침입
- 크리덴셜을 다른 악의적인 행위자에게 판매
- IAB 식별의 의의
- IAB는 멀웨어 및 랜섬웨어 공격과 같은 사이버 위협을 증가 시킴
- 악성 행위자가 사이버 공격을 단순화 하게함.



## 조사과정

1. 다크웹 내부 위협 행위자 선정 및 정보수집
2. Digital Foot Print 추적 및 분석
3. 분석 결과 정리 및 보고서 작성



## 악성 행위자가 동일인임을 확인하는 방법


- 이메일 주소, 텔레그램 주소, 트위터 계정 등을 통해 식별





## 분석 타겟 설정

- XSS.is 포럼 탐방 중 IAB로 추정되는 악성 행위자 발견
- 악성 행위자와 관련된 정보를 수집



## Kinuzo라는 유저에 대해

- XSS.is 포럼과 Breach 포럼에서 활동하던 유저
- 현재는 XSS.is 포럼에서는 벤을 당한 상태
- IAB로 추정 됨

Kinuzo



Advanced User

Posts:	51
Threads:	2
Joined:	Jul 2023
Reputation:	30

09-25-2023, 09:35 AM

#1

As the title said i will be searching your requests in my private base of logs

Message me on telegram with your request (link) and how much u paying per valid login:

<https://t.me/kinuzo>

<https://prnt.sc/el67XIR6-BdY>

Need a **middleman**? Try out our **Escrow App!**

## Результаты поиска



### WHITE RABBIT - CC Shop

+rep A good friend and the best I have ever worked with, no problems at all, and the best support. I highly recommend!

Kinuzo · Сообщение #80 · 05.04.2024 · Раздел: КАРДИНГ: cc, залив, вешевуха, банки, стафф



### Selling CMS - OpenCart, Magento, PrestaShop, WordPress and Joomla (Best prices in the market)

bump

Kinuzo · Сообщение #3 · 24.03.2024 · Раздел: ДОСТУПЫ: сети, rdp, шеллы, ftp, sql-inj, DB's



### Selling CMS - OpenCart, Magento, PrestaShop, WordPress and Joomla (Best prices in the market)

bump

Kinuzo · Сообщение #2 · 20.03.2024 · Раздел: ДОСТУПЫ: сети, rdp, шеллы, ftp, sql-inj, DB's



### Selling CMS - OpenCart, Magento, PrestaShop, WordPress and Joomla (Best prices in the market)

Selling CMS access (OpenCart, Magento, PrestaShop, WordPress and Joomla) If you have interest in any of these, message me on Telegram. My telegram: Kinuzo (Only message me to buy if you truly know how to work with it.) \*\*\*\*\* 1. Country: Italy Sales: 5-8 per day...

Kinuzo · Тема · 16.03.2024 · [access](#) [cms](#) [store](#) · Ответы: 2 · Раздел: ДОСТУПЫ: сети, rdp, шеллы, ftp, sql-inj, DB's

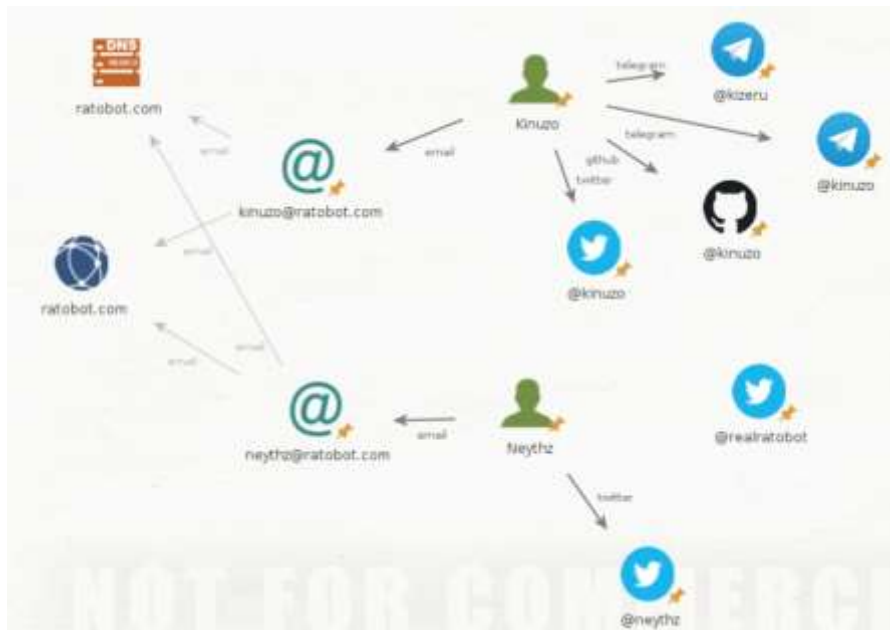


### Esse cara e brother

Esse cara e brother

Kinuzo · Сообщение в профиле · 15.01.2024

## Maltego를 활용한 도식화





# OSINT 프레임워크

<https://osintframework.com/>