

정보보안학과 20231773 김신아

Rippersec

사이버 범죄 그룹 분석 및 동향

Priority One

목차.

01

사이버 범죄 그룹

02

Rippersec
그룹 분석

03

Rippersec
동향 분석

04

마무리

사이버 범죄 그룹

정보통신망을 이용하여 다양한 범죄 행위를 저지르는 조직체

주로 사이버 사기, 금융사기, 개인 정보 침해, 저작권 침해 등 다양한 형태의 범죄를 수행

사이버 범죄 그룹

사이버 범죄 그룹의 주요 활동

사이버 사기: 인터넷을 통해 돈을 가로채거나 개인 정보를 탈취하는 행위.

사이버 금융 범죄: 피싱, 파밍, 스미싱, 메모리 해킹, 뮌캠 피싱 등 금융 거래를 이용한 범죄.

개인 정보 침해: 개인의 정보, 위치, 사생활 등을 침해하는 행위.

사이버 스팸: 불필요한 메시지나 광고를 발송하여 피해를 입히는 행위.

악성 코드 유포: 바이러스, 웜, 스파이웨어 등 악성 프로그램을 유포하여 시스템을 손상시키거나 정보를 탈취하는 행위.

DDoS 공격: 특정 웹사이트나 서버에 과도한 트래픽을 발생시켜 서비스 장애를 유발하는 행위.

사이버 범죄 그룹

사이버 범죄 그룹의 종류

- 친러시아 사이버 범죄 그룹: 친러시아적 성향을 가진 그룹.
- 국가 지원 그룹: 특정 국가의 지지를 받는 사이버 범죄 그룹.
- 사이버 범죄 조직: 조직적으로 활동하는 사이버 범죄 집단.
- 해커 그룹: 악성 코드를 개발하거나 시스템을 해킹하는 그룹.

Rippersec

Rippersec



2023년 6월에 결성된 사이버 해커 집단

팔레스타인과 무슬림을 옹호하는 말레이시아 활동가
친이슬람 해티비스트 그룹

해커티비즘 성향을 가진 그룹이며,
정치적 이슈나 사회적 메시지를 알리기 위한 목적의 공격을 감행

Rippersec



Rippersec은 고도의 해킹 기술을 사용하지는 않는다.

단, 멤버들이 다양한 나라에서 해티비즘 공격을 목적으로 모였기 때문에 그룹 멤버와 공격의 수가 점차 늘어나고 있어 위협적인 영향력을 확대하고 있다.

Rippersec 그룹 분석

〈다크웹, 트위터, 텔레그램 등을 통해 공격 예고/성과를 공개〉

1년 넘게 누적 구독자 수가 2000명을 넘고있다.

Priority One

RipperSec (ريفرسيك)

DDoS Target Order

**We Demand Pattani Darussalam
Free From Thailand Colonizing**

Pattani Will Be Independent
•FreePattani •JusticeForPattani

DDOS TIME 🕒 02:00 pm (SG)
DATE 📅 :15-Jan-2025

TARGET 📍 : <https://www.seagate.co.th/>
IP 📡 :
ISP 🛡️ :
Ports 📡 : 80 |

⚠️ Our Message ⚠️

➡️ Patani Will Be Independent 🚩
#FreePatani #OpsPutus #StandWithPatani

-> Our Royal Comrades 👑

#RipperSec
#SedihCrew
#NetGhostSec
#StucxTeam
#Zenimous #TengkorakCyberCrew
#Dxploit

Follow For More Updates 📢 :
[@RipperSec](#) | [@RipperSecIO](#) | [@RipperSecGroup](#) | [@PyRoxyForum](#)

👁 4 11:36

💬 Leave a comment

Rippersec 그룹 분석

Nation Of Saviors과 Rippersec의 협력

갑자기 사라졌던 Rippersec은
NOS과의 동맹을 발표

〈Holy League 동맹에 속해있으며, NoName057(16),
UserSec 등 40개 이상의 그룹과 협력 관계〉

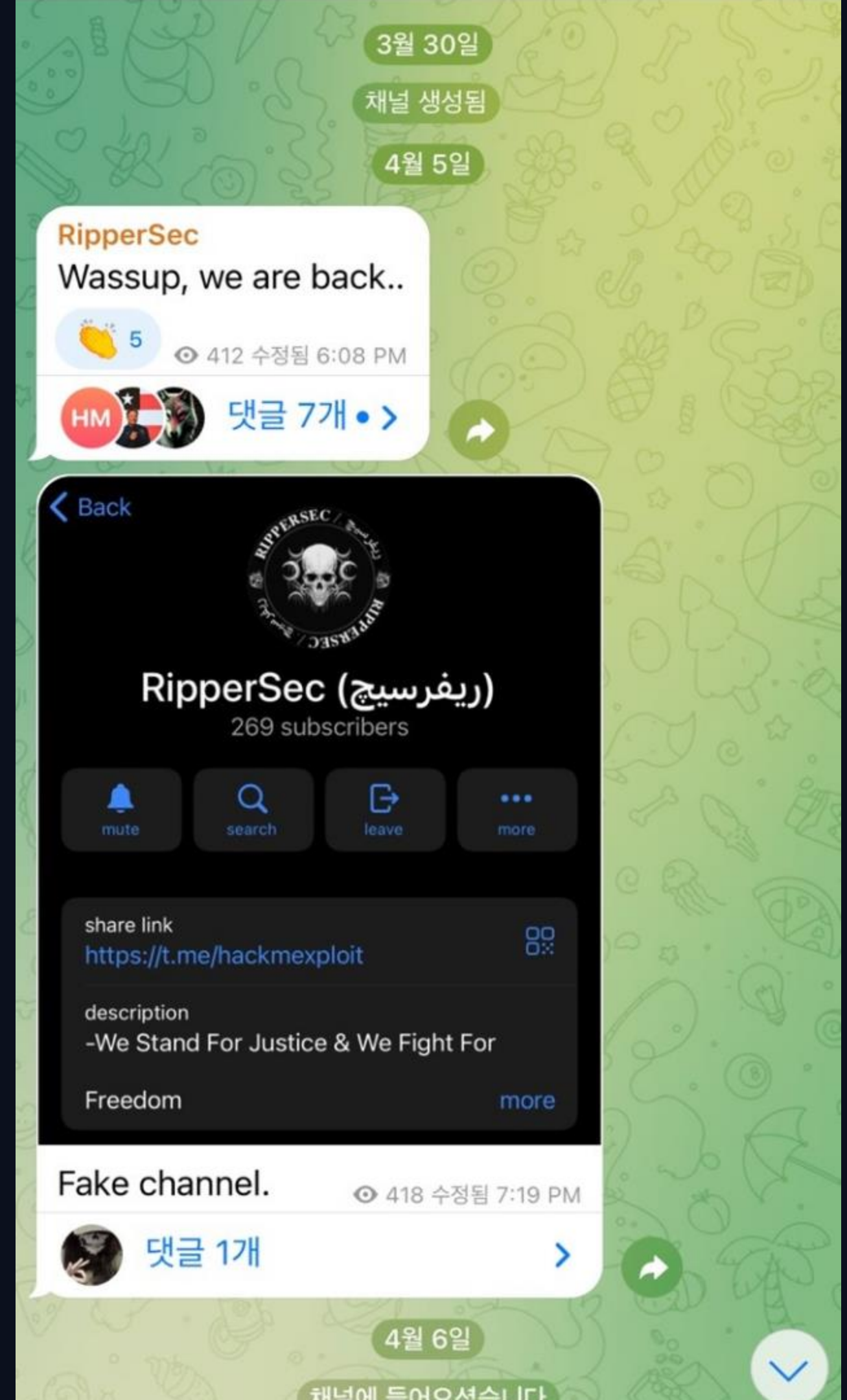
Priority One



Rippersec 그룹 분석

Wassup을 외치며 복귀를 알림
〈+ 현재는 다시 채널 삭제됨〉

Priority One



Rippersec 동향 분석



01

한국 정부 사이트
디도스 공격

<https://www.etnews.com/20250310000215>



02

Mega Medusa

<https://youtu.be/xGDqfAUwQ94?si=Pdnjru8VeXiWAmFT>

Rippersec 동향 분석



01

한국 정부 사이트 디도스 공격

한국 정부 사이트 디도스 공격



목표

2025년 3월 4일,
이스라엘에 대한 군사 지원 중단을 촉구하고
팔레스타인의 자유를 표방하며 한국 대상 공격을 시작



공격 실행

디도스 공격 알림 문자에 한국 정부 사이트를 표적으로 지정
디도스 공격으로 일시적으로 접속 장애 발생

한국 정부 사이트 디도스 공격



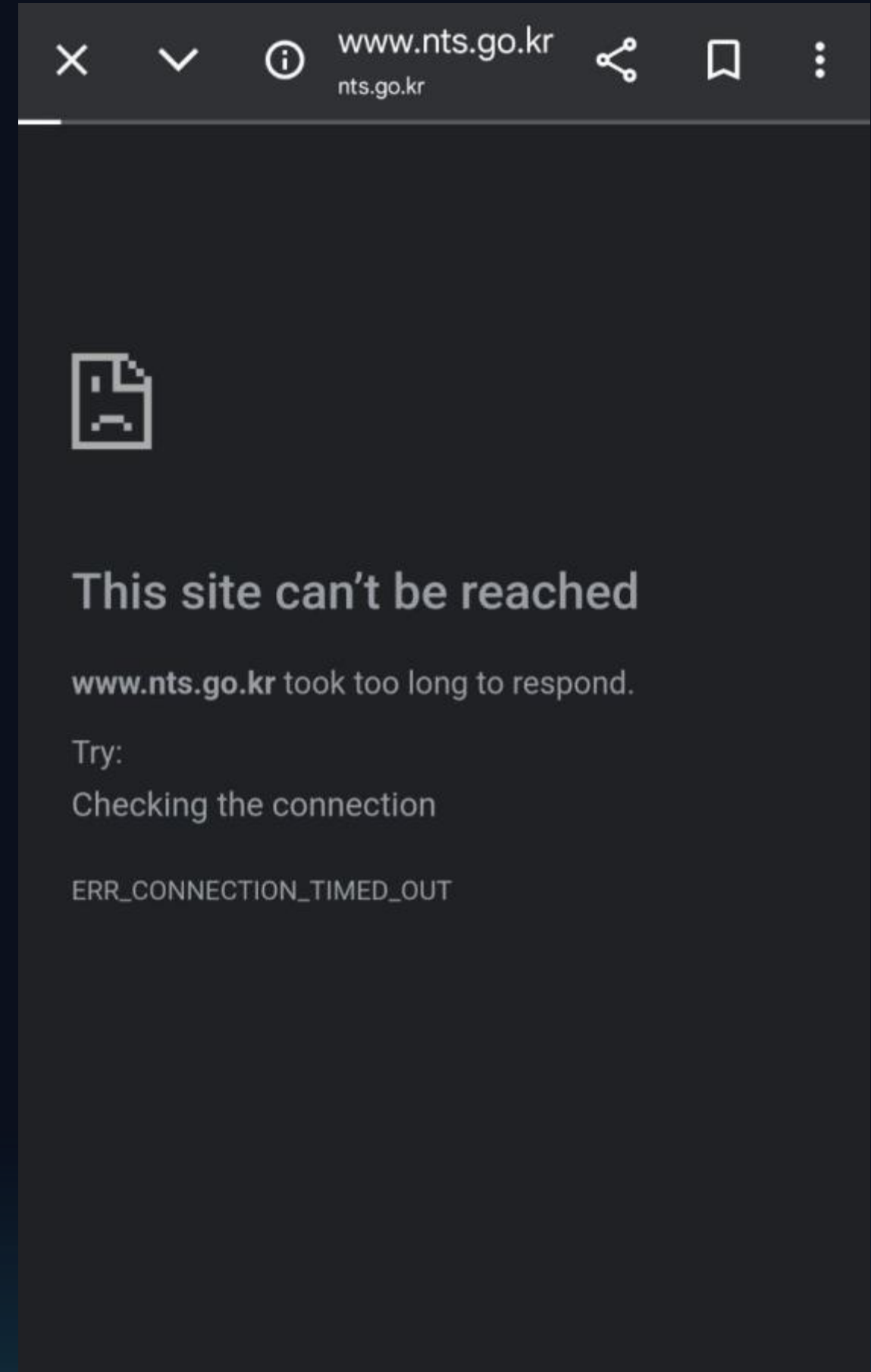
DDoS Attack Order
We Stand For Justice & Fight For Freedom

DDOS TIME 🟡 04:00pm (SG)
DATE 📅 :07-March-2025

TARGET 🚩 : <https://www.nts.go.kr/>
IP 🟢 : 116.67.121.13
ISP 🛡️ : National Information Resources Service
Ports 📘 : 80 | 443 |

⚠️ Our Message ⚠️

➡ Stop funding weapons to Israel and stealing Palestinian land! 🗨️



× ✓ ⓘ www.nts.go.kr
nts.go.kr

📄

This site can't be reached

www.nts.go.kr took too long to respond.

Try:
Checking the connection

ERR_CONNECTION_TIMED_OUT

Rippersec 동향 분석



02

Mega Medusa

Mega Medusa



MegaMedusa 란?

RipperSec 그룹 회원이 개발 및 관리하는
공개 웹 DDoS 공격 도구



DDoS 공격 도구

이 도구의 소스 코드는 GitHub에 공개되어 있으며,
JavaScript 코드는 난독화되어 있지만,
읽기 가능한 코드는 쉽게 난독화 해제하고 복구할 수 있다.

Mega Medusa



MegaMedusa 란?

RipperSec 그룹 회원이 개발 및 관리하는
공개 웹 DDoS 공격 도구



DDoS 공격 도구

이 도구의 소스 코드는 GitHub에 공개되어 있으며,
JavaScript 코드는 난독화되어 있지만,
읽기 가능한 코드는 쉽게 난독화 해제하고 복구할 수 있다.



!!!!!!진짜 너무너무 위험하다!!!!!!

Mega Medusa

MegaMedusa Layer-7 DDoS Tool v3.1

MEQUSA v3.1

```
-> Target : https://www.
```

→ Time : 100

→ Rate : 30

-> Thread : 10

→ ProxyFile : proxy.txt

-> Github : <https://github.com/TrashDono>

[Medusa] (20:18:43) Attack Thread 1 Started

[Medusa] (20:18:43) Attack Thread 2 Started

Medusa (20:18:43) Attack Thread 3 Started

[Medusa] (20:18:43) Attack Thread 4 Started

[Medusa] (20:18:43) Attack Thread 5 Started

[Medusa] (20:18:43) Attack Thread 6 Started

[Medusa] (20:18:43) Attack Thread 7 Started

[Medusa] (20:18:43) Attack Thread 8 Started

[Medusa] (20:18:44) Attack Thread 9 Started

```
[Medusa] (20:18:44) Attack Thread 10 Started
```

[Medusa] (20:18:44) Medusa Attacking...

```
[Medusa] (20:18:47) Medusa: Reconnecting...
[Medusa] (20:18:49) > Title: Top Online (200)
```

```
[Medusa] (20:18:53) > Request timed out
```

```
[Medusa] (20:18:55) > Request timed out
```

```
[Medusa] (20:18:57) > Request timed out
```

```
[Medusa] (20:18:54) > Request timed out
```

```
[Medusa] (20:19:01) > Request timed out
```

```
{ "id": 1, "name": "Root", "children": [ { "id": 2, "name": "Child 1", "children": [ { "id": 3, "name": "Grandchild 1"}, { "id": 4, "name": "Grandchild 2"} ] }, { "id": 5, "name": "Child 2", "children": [ { "id": 6, "name": "Grandchild 3"} ] } ] }
```

□

JavaScript로 작성된 MegaMedusa

Node.js 크로스 플랫폼 JavaScript 런타임 환경에서 실행되는 명령줄 도구

Node.js는 비동기 및 논블로킹 I/O를 제공하여 여러 요청을 동시에 처리할 수 있다.


따라서 대량의 네트워크 연결 관리와 같은
I/O 관련 작업에 매우 효율적

Node.js 애플리케이션은 플랫폼별 코드 없이도 여러 플랫폼(Windows, macOS, Linux)에서 실행될 수 있다.

Mega Medusa

Installation Command :

```
sudo apt install curl  
curl https://raw.githubusercontent.com/creationix/nvm/master/install.sh | bash  
source ~/.bashrc  
nvm install --lts  
python3 installer.py
```



Node.js 런타임 환경과 모든 필수 종속성을 다운로드하고 설치하는 데는 단 다섯 개의 간단한 명령만 필요

집에서 Linux 기반 시스템을 운영하거나
퍼블릭 또는 방탄 클라우드에서 Linux 기반 가상 사설 시스템을 임대하는 사람이라면

누구나 단 몇 분 만에 원하는 대상에 대해 확장성이 뛰어난 웹 DDoS 공격을 실행할 수 있다.

Mega Medusa

이 이야기를 선정하게 된 이유..

블랙해커? 노노
우리 모두 화이트해커 고고

마무리

권장 사항 및 조치 방안



01

지속적인 위협
인텔리전스 수집

02

보안 시스템의
선제적 점검 및
강화

03

국가 간 협력
및 정보 공유

04

보안 교육 및
인식 제고

— Thank you. ■

감사합니다!

