✅ [WHS-3기][사이버 범죄]-33반-김신아(9502)

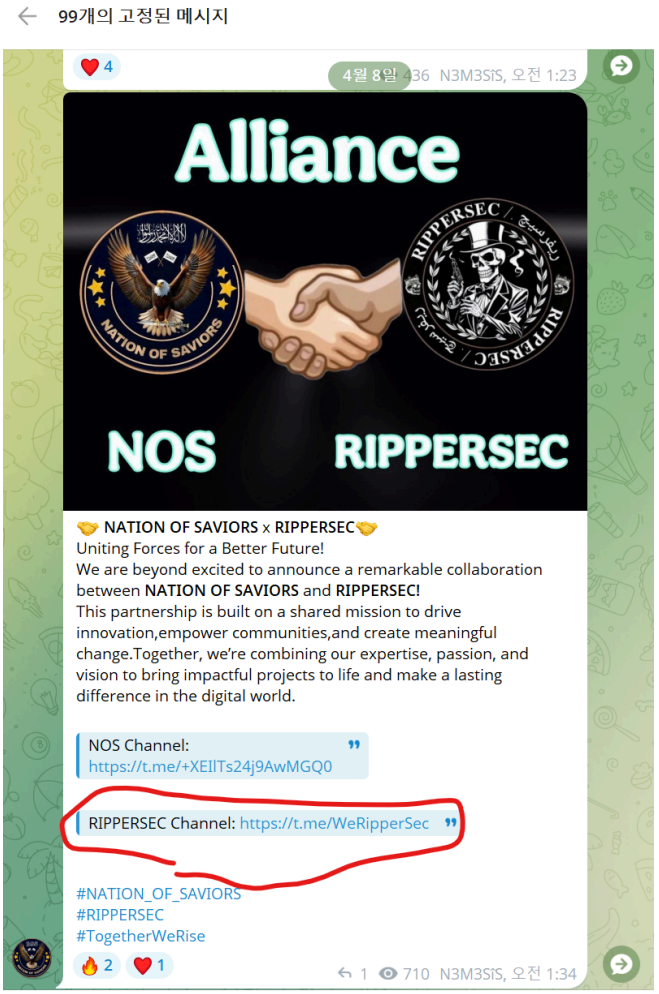
📗보고서 요약

- **RipperSec은 친이슬람, 친러시아 성향의 핵티비스트 해커 그룹**으로 정치적·사회적 메시지를 전달하기 위해 다양한 국제 이슈에 개입하며 활동하고 있다.
- **대만의 금융기관 및 정부 시스템을 포함한 여러 기관을 대상으로 DDoS 공격**을 수행했으며, NoName057과 같은 해커 그룹과 협력해 공격의 규모를 키우고 있다.
- 사이버 공격은 **사회적 혼란 유발과 보안 체계의 허점을 노리는 목적**을 가지고 있으며, 대응을 위해 위협 인텔리전스 수집, 보안 시스템 강화, 국제 협력, 교육 등이 필요하다.

🕵️ RipperSec

2023년 6월에 결성된 사이버 해커 집단으로, 친이슬람 핵티비스트 단체이다.

Anonymous와 유사한 해커티비즘 성향을 가진 그룹이며, 정치적 이슈나 사회적 메시지를 알리기 위한 목적의 공격을 감행하고 있다. <다크웹, 트위터, 텔레그램 등을 통해 공격 성과를 공개>



고정된 메시지 보지 않기

Rippersec의 텔레그램 채널에 들어가보았지만, 최근 채널을 새로 개설하여 추가적인 정보를 얻지는 못하였습니다.

📌 상세 분석

2024년 8월 12일

[X 플랫폼의 도널드 트럼프와 일론 머스크 인터뷰 중단 시도]

일론 머스크와 도널드 트럼프의 인터뷰 생중계가 DDoS공격으로 중단된 사건이 발생하였습니다.

해커 그룹 RipperSec는 도널드 트럼프와 일론 머스크의 인터뷰가 진행되던 X 플랫폼에 대한 DDoS 공격을 주장하였습니다. 하지만 DDoS공격은 실제로 누가 배후인지 입증하는 것이 어려워 Rippersec의 주장은 의심을 받았습니다.

- https://www.ccn.com/news/technology/rippersec-hactivist-ddos-trump-musk/

2024년 9월 12일

[대만 금융 기관 및 타이완 증권거래소 공격]

RipperSec은 친러시아 해커 그룹 NoName057과 함께 대만의 주요 금융 기관인 Mega Financial Holding Co.와 타이완 증권거래소에 대한 DDoS 공격을 감행했습니다. 이로 인해 일시적으로 접속 불안정 현상을 겪었으나, 신속한 대응으로 정상 운영을 재개했다고합니다.

☠️ 공격기법

MegaMedusa라는 도구를 활용하여 HTTPS 플러드 공격을 수행

이 공격은 대량의 HTTPS 요청을 목표 시스템에 보내 시스템을 과부하 상태로 만들어 정상적인 서비스를 방해하는 방식입니다.

- https://www.radware.com/security/threat-advisories-and-attack-reports/pro-russian-hacktivists-target-organizations-in-taiwan-with-ddos-attack-campaign/
- https://www.bnnbloomberg.ca/business/international/2024/09/13/hackers-hit-taiwan-bourse-major-bank-in-mystery-foreign-attack/

2024년 10월

[대만 정부 기관 및 공항 시스템 공격]

RipperSec는 친러시아 해커 그룹인 NoName057과 대만의 세무, 항공 등 여러 기관을 대상으로 50건 이상의 분산 서비스 거부 공격을 감행했다고 합니다. 이러한 공격이 대만 해협 위기와 관련이 있는지는 명확하지 않지만, 컴퓨터 시스템에 대한 주요 침해는 없었다고 합니다.

☠️ 공격기법

DDoS 공격을 사용하였습니다. 한꺼번에 다수의 트래픽을 유입시켜 웹사이트를 마비시키는 방식으로 피해를 입혔습니다.

- https://www.thisdaylive.com/index.php/2024/10/30/pro-russia-hackers-accused-of-targeting-taiwans-computer-systems/

☑️ 결론

RipperSec는 정치적, 사회적 메시지를 전달하기 위해 사이버 공격을 활용하는 핵티비스트 그룹으로, 최근 다양한 국제 이슈에 개입하며 활동 범위를 넓히고 있습니다. 친러시아 성향의 다른 해커 그룹과 협력하여 대규모 DDoS 공격을 수행하고 있으며, 대만의 금융기관과 정부 시스템을 대상으로 한 일련의 공격은 사이버 공간이 국제 분쟁의 또 다른 전장이 되고 있음을 나타내고 있습니다. 이들의 공격은 피해 규모와 관계없이 사회적 혼란을 유발하고 보안 체계의 허점을 노리는 데 목적이 있기 때문에, 단순한 기술적 문제를 넘어 사회적 경각심을 가져야할 것입니다.

☑️ 대응 방안

- **지속적인 위협 인텔리전스 수집**
  - 다크웹, 텔레그램 등에서의 위협 그룹 활동 추적
  - RipperSec와 연계된 해커 그룹(N0Name057 등)의 동향도 함께 모니터링
- **보안 시스템의 선제적 점검 및 강화**
  - DDoS 공격 방어를 위한 CDN 서비스, 웹 방화벽(WAF), 트래픽 분산 기술 적용
  - HTTPS Flood와 같은 최신 공격 유형에 대한 탐지 및 대응 체계 마련
- **국가 간 협력 및 정보 공유**
  - 사이버 범죄는 국경을 넘나드는 만큼, 국제 보안 기관 및 CERT 간의 협력이 필수
  - 유사 피해 사례를 공유하고, 공동 대응 프로토콜 수립 필요
- **보안 교육 및 인식 제고**
  - 사이버 위협의 사회적, 정치적 배경에 대한 이해 교육 강화
  - 공공기관 및 금융기관 종사자 대상 DDoS 대응 시나리오 훈련 시행