Operation So-seki: You Are a Threat Actor. As Yet You Have No Name.

May 23rd , 2025

Ryo Minakawa, Kaichi Sameshima, Atsushi Kanda

NTT Communications / N.F.Laboratories

$whoami

We are threat intel. team, NA4Sec !!

NA4Sec
Network Analytics for Security

strinsert1Na

Ryo Minakawa
@N.F.Laboratories

islairand

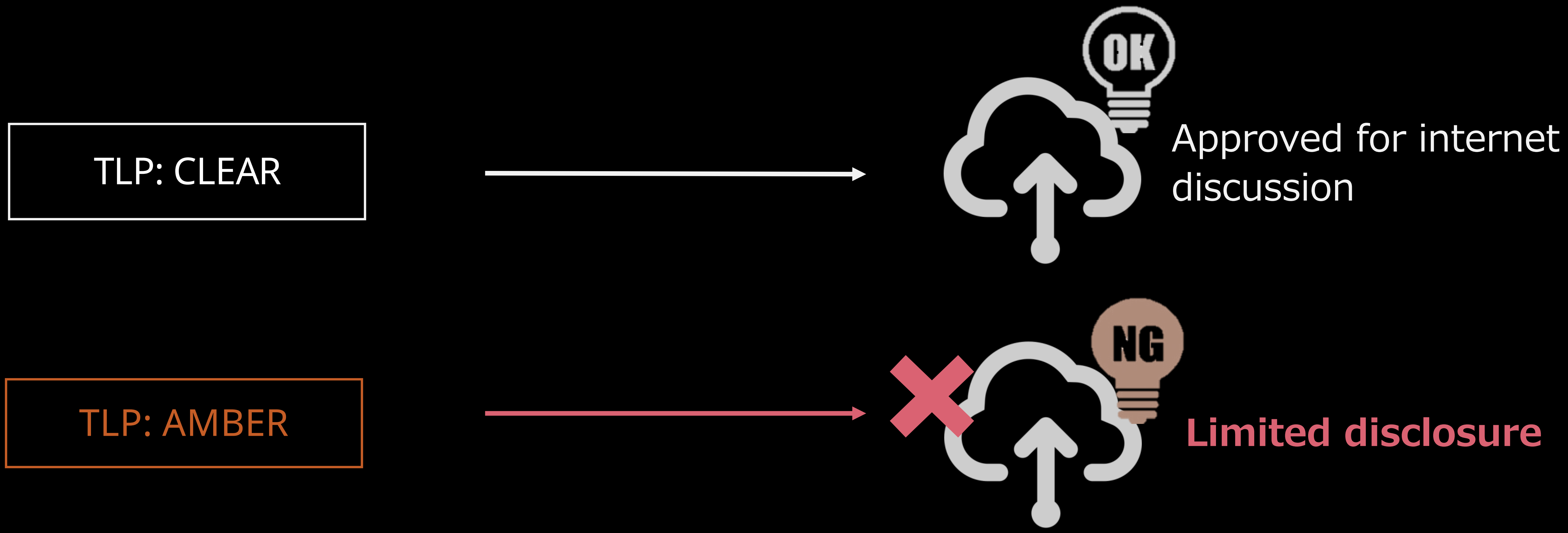
Kaichi Sameshima
@NTT Communications

ashy0x41

Atsushi Kanda
@NTT Communications

⚠ Notes

Please use the content within the scope of the TLP !!



TLP: CLEAR

Approved for internet discussion

TLP: AMBER

Limited disclosure

Do not carelessly discuss hacktivist-related topics in public spaces like SNS.

Outline

- Operation So-seki
- Threat Actor Profile
- DDoS Infrastructure and Capability
- DDoS Activities
- Hacktivist and Threat Intelligence Sharing
- Summary

Outline

- Operation So-seki
- Threat Actor Profile
- DDoS Infrastructure and Capability
- DDoS Activities
- Hacktivist and Threat Intelligence Sharing
- Summary

Our topic is…

CENSORED

Outline

- Operation So-seki
- Threat Actor Profile
- DDoS Infrastructure and Capability
- DDoS Activities
- Hacktivist and Threat Intelligence Sharing
- Summary

CENSORED

Outline

- Operation So-seki
- Threat Actor Profile
- DDoS Infrastructure and Capability
- DDoS Activities
- Hacktivist and Threat Info. Sharing
- Summary

CENSORED

Outline

- Operation So-seki
- Threat Actor Profile
- DDoS Infrastructure and Capability
- DDoS Activities
- Hacktivist and Threat Intelligence Sharing
- Summary

CENSORED

Outline

- Operation So-seki
- Threat Actor Profile
- DDoS Infrastructure and Capability
- DDoS Activities
- Hacktivist and Threat Intelligence Sharing
- Summary

Hacktivist?

“Annoying influencer”

What are we gonna do?

Information sharing in Operation So-seki

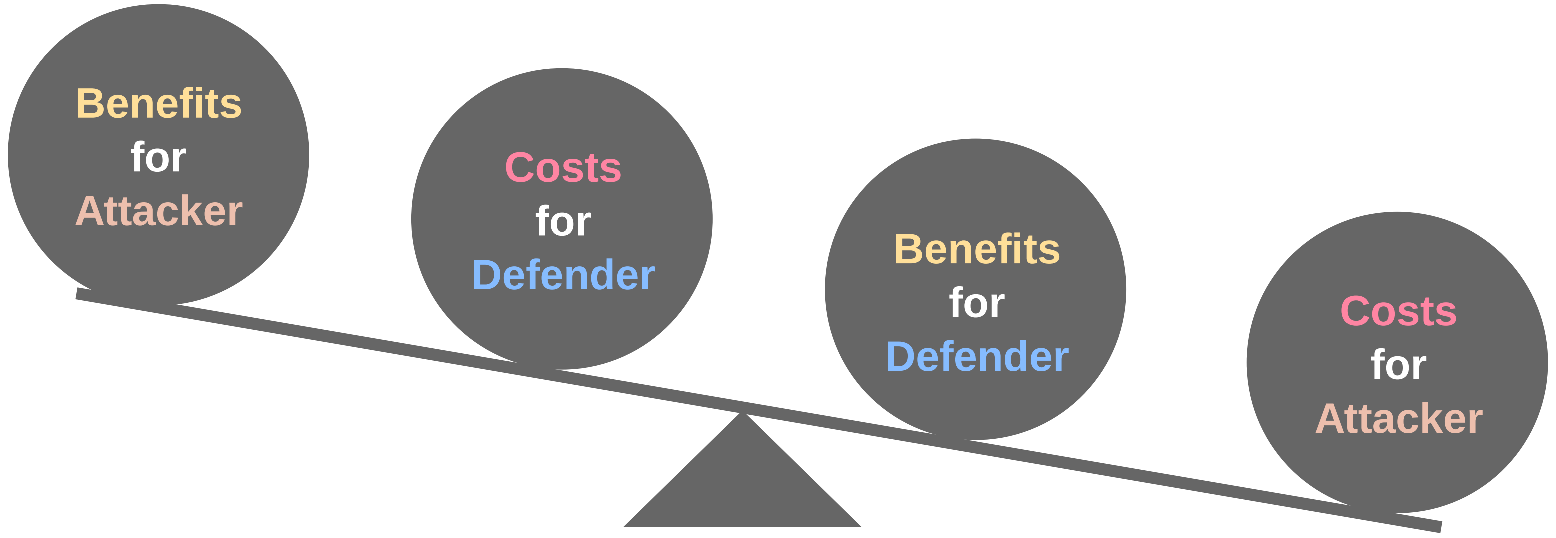
Sharing the intelligence without being noticed by the hacktivist in a timely and effective manner

- Directly to the targeted organization
  - C2 tracking techniques enables early recognition of...
    - Incident occurrence : timely action
    - **Cause** : save investigation cost
    - **Impact scope** : efficient resource allocation

- To ISAC
  - **Efficiently** share findings within (potential) target industries

Lessons learned from confronting hacktivists

- **Intelligence sharing tailored to the nature of each threat actor**
  - **Think about costs and benefits for both attacker and defender**
    - Public disclosure is inappropriate when confronting hacktivists
  - Back to basics of threat intelligence (4As)
    - Accurate
    - Audience Focused
    - Actionable
    - Adequate Timing
  - Pay attention to secondary information sharing
    - Careless information spreading is more beneficial for attackers



Outline

- Operation So-seki
- Threat Actor Profile
- DDoS Infrastructure and Capability
- DDoS Activities
- Hacktivist and Threat Intelligence Sharing
- Summary

Summary

- Long-term investigation of pro-Russian hacktivist

- **Key Takeaways:**
  - Techniques for tracking and analyzing the DDoS infrastructure
    - Infrastructure/Tools/Capability, Active scan

  - Long-term multi-perspective study of the DDoS actor
    - Businesslike/Well-organized, Possibly sponsored, Target selection preference

  - Lessons learned from confronting hacktivists
    - Intelligence sharing tailored to the nature of each threat actor

NA4Sec
Network Analytics for Security

Thank you !

docomo business | NTT Communications NFLabs.

Your comments & feedbacks
are always welcome

ic-na4sec@ntt.com

𝕏 strinsert1Na

𝕏 islairand

𝕏 ashy0x41