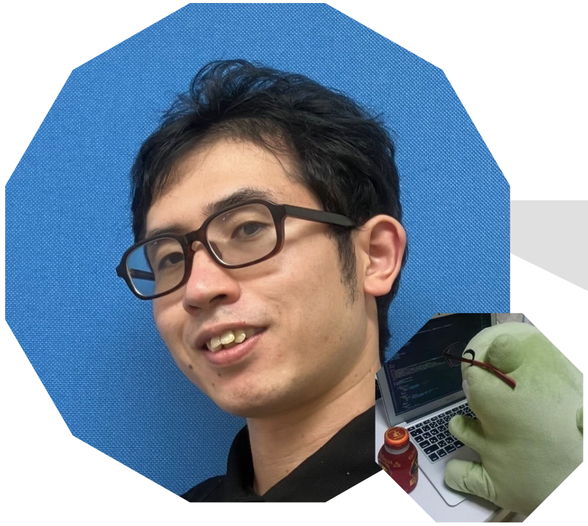
Operation So-seki: You Are a Threat Actor. As Yet You Have No Name.

Jan. 25th , 2024

Ryo Minakawa, Kaichi Sameshima, Atsushi Kanda

NTT Communications / N.F.Laboratories

$whoami



Ryo Minakawa
@N.F.Laboratories

NA4Sec
Network Analytics for Security

Atsushi Kanda
@NTT Communications

Kaichi Sameshima
@NTT Communications

Outline

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

Hacktivists are monitoring public information related to them

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

Please refrain strictly from spreading any information linking this presentation to the actor's real name.

Outline

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

Overview: Operation So-seki

- **Investigation of a cyber threat actor who names themselves [redacted]**
  - Tracking pro-Russian DDoS attack agitators operating mainly on Telegram
  - Multi-perspective analysis from the viewpoints of [redacted], and so on

- **Key Takeaways:**
  - Techniques for tracking and analyzing the DDoS infrastructure
  - Long-term multi-perspective study of the DDoS actor
  - The status quo of C2 discovery techniques using flow information
  - Lessons learned from confronting the hacktivists

Outline

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

Venue only

Outline

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

Venue only

Outline

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

Venue only

Outline

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

The Use of Flow Information by ISPs

- 『電気通信事業者におけるサイバー攻撃等への対処と通信の秘密に関するガイドライン（第6版）』 (“Guidelines for Telecommunications Carriers Regarding Response to Cyber Attacks and Secrecy of Communications (Revision 6)”[Japanese only]), 2021
  - Allowing telecom carriers to investigate and discover C2 server using Flow information
  - The scope is to “identify C2 server”

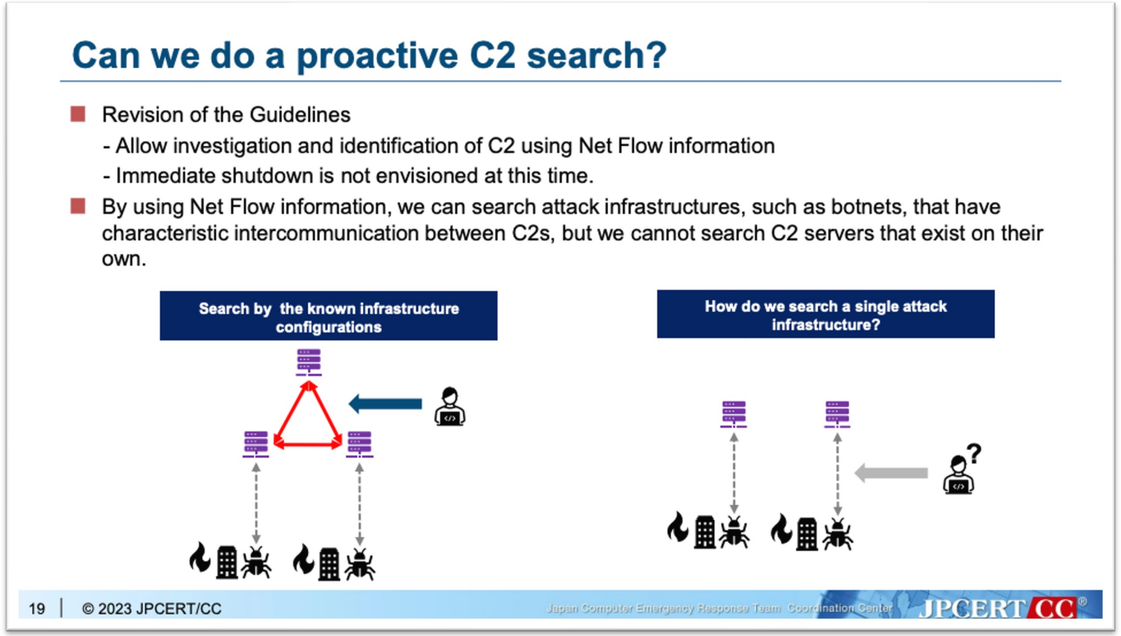
- 『国家安全保障戦略』(“National Security Strategy” [Japanese only]), 2022
  - The document includes a discussion on the effort implicitly assumed the use of Flow information by telecom carriers as a consideration to introduce so-called “Active Cyber Defense”

Against these backgrounds,
Operation So-seki uses Flow to track C2 server

Venue only

Limitation of Flow information

- Coverage: **Only a subset of the whole Internet traffic** can be observed
  - Constraints on collection points:
    Traffic that do not pass through
    the collection points can not be observed
  - Constraints of sampling:
    There is stochastically unobservable traffic
    (especially low-volume traffic)
- Amount of information :
  The basic component of Flow is 5-tuple*
  - It's quite difficult **to determine whether it is the C2 communication** based on the Flow information alone



"First Step to Active Cyber Defence: The Significance of Profiling Attackers" (JSAC2023)

There are valuable insights that can only be obtained from the Flow, but they aren't sliver bullets.
It is essential to combine with various contextual information to increase confidence.

* 5-tuple=Source IP, Source port, Destination IP, Destination port, Protocol

Outline

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

Negative effects of sharing/spreading threat intelligence

Public disclosure of TTP information ▶ Changes in TTPs

Spread of victim’s information ▶ Reinforcing the attacker’s experience of success

Reuse for further propaganda

Venue only

Hacktivist-specific situations

- The Ultimate goal
  = **Influence public opinion by making their claims widely known**
  - DDoS is just a means of attracting public interest
  - Hacktivists are concerned about how well their message is reaching the world
    - “Are the people aware of us and our attacks?”
    - “How fascinate the impact caused by our attacks is?”

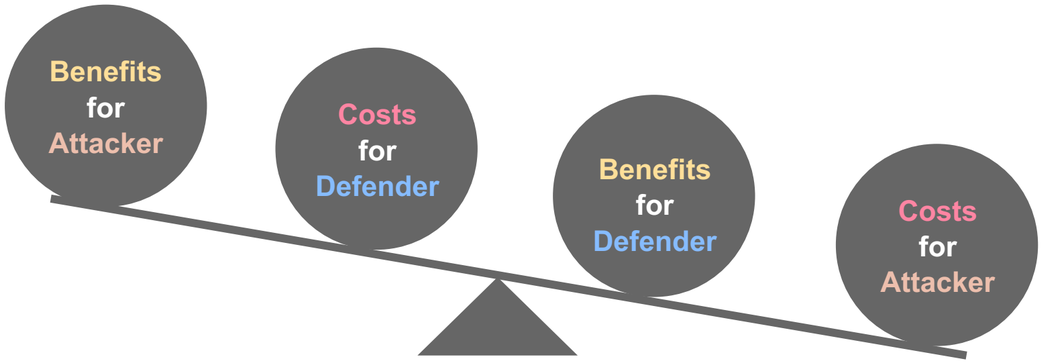
Hacktivists want to make them and their activities more known

Public disclosure of the threat intelligence is inappropriate when confronting hacktivists

Venue only

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
- Exploring Threat Infrastructure using Flows
- Hacktivist and Threat Intelligence Sharing
- Summary

Summary

- Long-term investigation of pro-Russian hacktivist [redacted]
- **Key Takeaways:**
  - Techniques for tracking and analyzing the DDoS infrastructure
    - [redacted]
  - Long-term multi-perspective study of the DDoS actor
    - [redacted]
  - The status quo of C2 discovery techniques using flow information
    - Values and limitations of using flow information
  - 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