STARDUST: Large-scale Infrastructure for Luring and Monitoring Cyber Adversaries

Yu Tsuda

National Institute of Information and Communications Technology (NICT)

Background & Motivation

- Targeted attacks are recognized as serious social concerns.
  - Security vendors reports several attack campaigns.
    - See also: https://github.com/kbandla/APTnotes
- However, we cannot obtain actual data.
  - Security logs include confidential data.
  - The logs aren’t preserved in the long term.

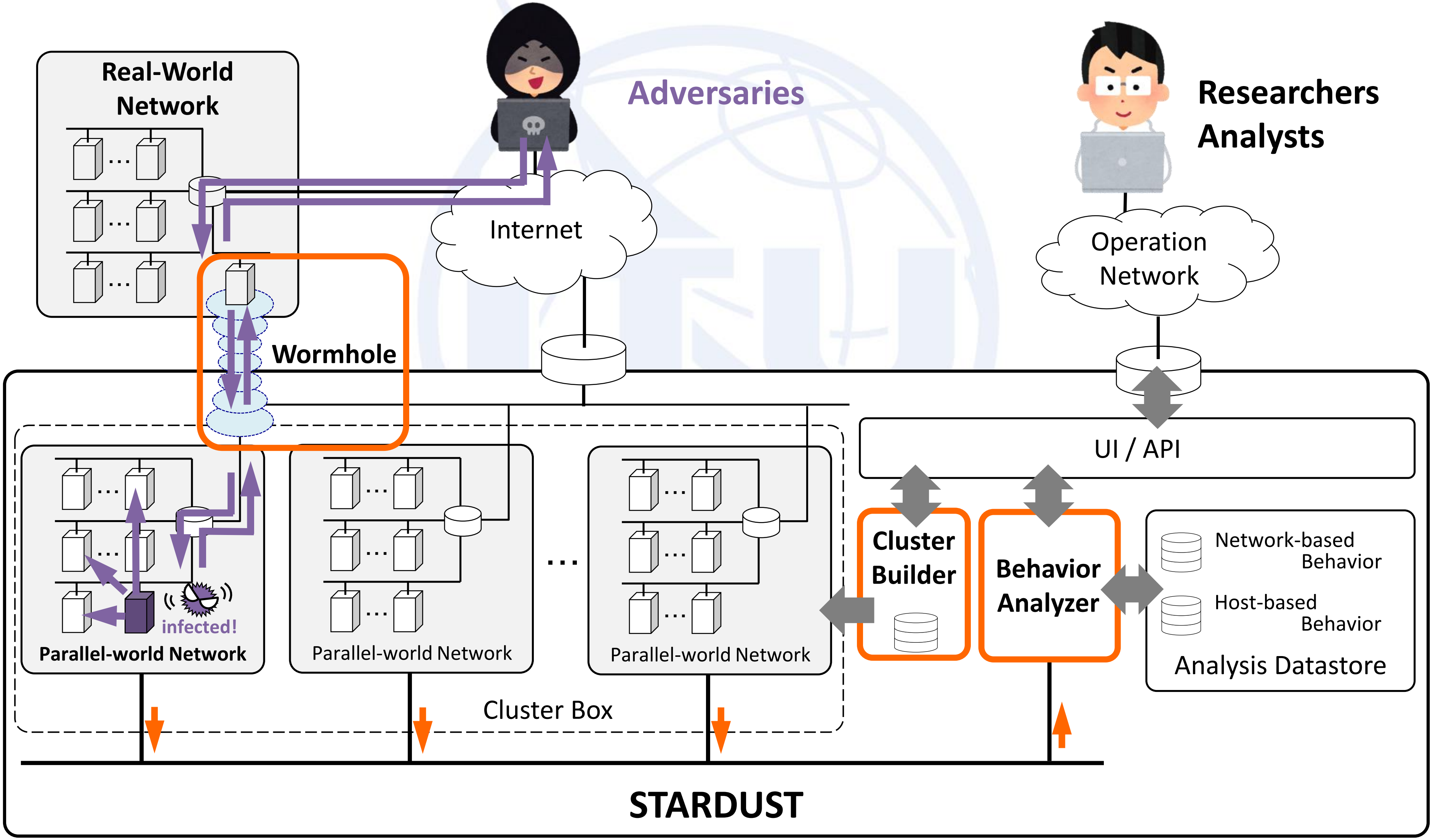
  etc...

We desire a large-scale infrastructure
to observe adversaries’ activities

What is STARDUST ?

- STARDUST is a large-scale infrastructure
  - for luring adversaries and
  - for observing their activities.
- By using STARDUST, we can
  - **flexibly (re)build** analysis environments called parallel-world networks.
    - A parallel-world network is a highly mimetic network based on a real-world network's configurations.
  - **stealthily observe** adversaries' activities on parallel-world networks.

Design Overview and Workflow



Case Study

- We analyzed APT groups, which targeted organizations in Japan.
  - vs. **Blue Termite**
    For preliminary testing, we used a **“clean”** parallel-world network.
  - vs. **DragonOK**
    We used a parallel-world network with **“lifelike settings (dirty)”.**
- Analysis workflow was the followings:
  1. Got C&C server’s domain by dynamically analyzing a malware.
  2. Resolved C&C domain, then checked connectivity of C&C.
  3. Executed the malware on a parallel-world network’s host.
  4. If C&C connection was broken, finished the analysis.

#	APT Group	Malware（MD5）	C2	Configurations of Parallel-world Network
0	Blue Termite	7af68ddba01ba2d69a8ef7c17430e5d0	JP	• Joined into AD domain AD = Active Directory
1	DragonOK	251c0f90bfe9a302c471bf352b259874	US	• Joined into AD domain • Set files and e-mail
2	DragonOK	acc2e5f8abd7426574712fe6a13c2342	SG	• Joined into AD domain • Set files and e-mail
3	DragonOK	c938690a0558d070528a7cab4de0e9b3	US	• Joined into AD domain • Set files and e-mail

Summary

- We proposed and implemented **STARDUST**.

- We observed similar activities in our case study
  - investigating networks/hosts
  - using regular expression
  - executing commands interactively because of some typo and
  - We could guess they had manuals to investigate targeting networks/hosts.
    - APT adversaries are not so advanced?

- Future Work
  - **Large-scale case study** by using STARDUST
  - **Sharing data** (adversaries' activities) that we observed
  - **Developing countermeasures** based on our observation.