地域戦略研究（東アジア）

CJK Cybersecurity from ‘Darknet’ observer’s perspective

2019-10-29

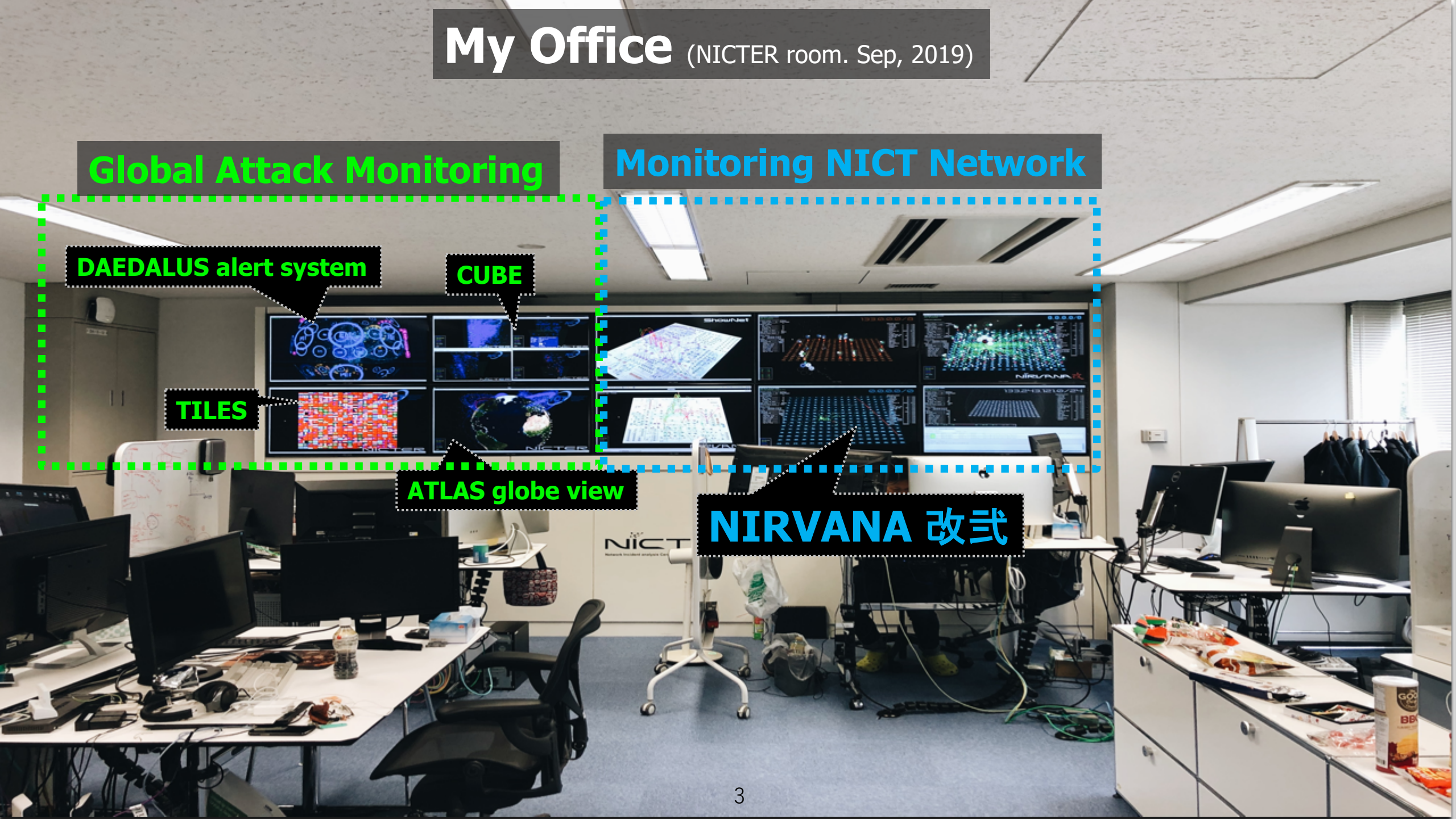
Graduate school of Media and Governance, Keio Univeristy

Masaki KUBO

About Me

- **Masaki Kubo (久保 正樹)**
  - Research Engineer @ NICT
- Career
  - National CSIRT (13 years) to **Cybersecuirty Research Institute** (2017-now)
- Areas of Work
  - Vulnerability Analysis & Coordination, Secure Coding, Darknet Monitoring, ISO/IEC standardization

My Office (NICTER room. Sep, 2019)



Q.

How do you measure cybersecurity of a country?

35,575 views | Aug 3, 2019, 02:31am

Chinese State Hackers Suspected Of Malicious Cyber Attack On U.S. Utilities

Zak Doffman Contributor ⓘ
Cybersecurity
I write about security and surveillance.

The notorious Chinese state-sponsored hacking gro

By Jack Martin

AUG 13, 2019

UN Report: South Korea Hardest Hit By North Korean Cyber Attacks

3670 Total views 90 Total shares Listen to article 1:51

The United Nations is investigating 35 North Korean cyberattacks across 17 countries, according to a report published Aug. 13 by the AP. This follows last week's leaked summary of the report, stating that $2 billion had been hacked by the nation thus far to fund weapons programs.

The Asahi Shimbun | Asia & Japan Watch

Search

TOP Japan News Politics Business Sports Culture Trave

The Asahi Shimbun > Politics > article

Politics

Japan, U.S. say cyber-attacks would be covered by security pact

BUN
:05 JST

Tweet Print
list

Measuring Cyber Attacks - WHAT

- **A cyber attack** is not so obvious
  - Different scale, different threat
    - Country, Sector, Organization, Devices
  - Different types of threat
    - DDoS, (Spear)Phishing, BEC, Targeted, Malware Infection
  - Security Event vs. Security incident
    - Attempt of an attack (security event), when confirmed, becomes incident
  - Closely related but different area: **cybercrime**

Measuring Cyber Attacks - HOW

- **How** do you measure?
  - Well, to measure something, you need a **measure**
  - Ex.
    - **# of malicious e-mails** sent to a government
    - **# of malware detection** by anti-virus software
    - **# of attack attempts** a single host received
    - …

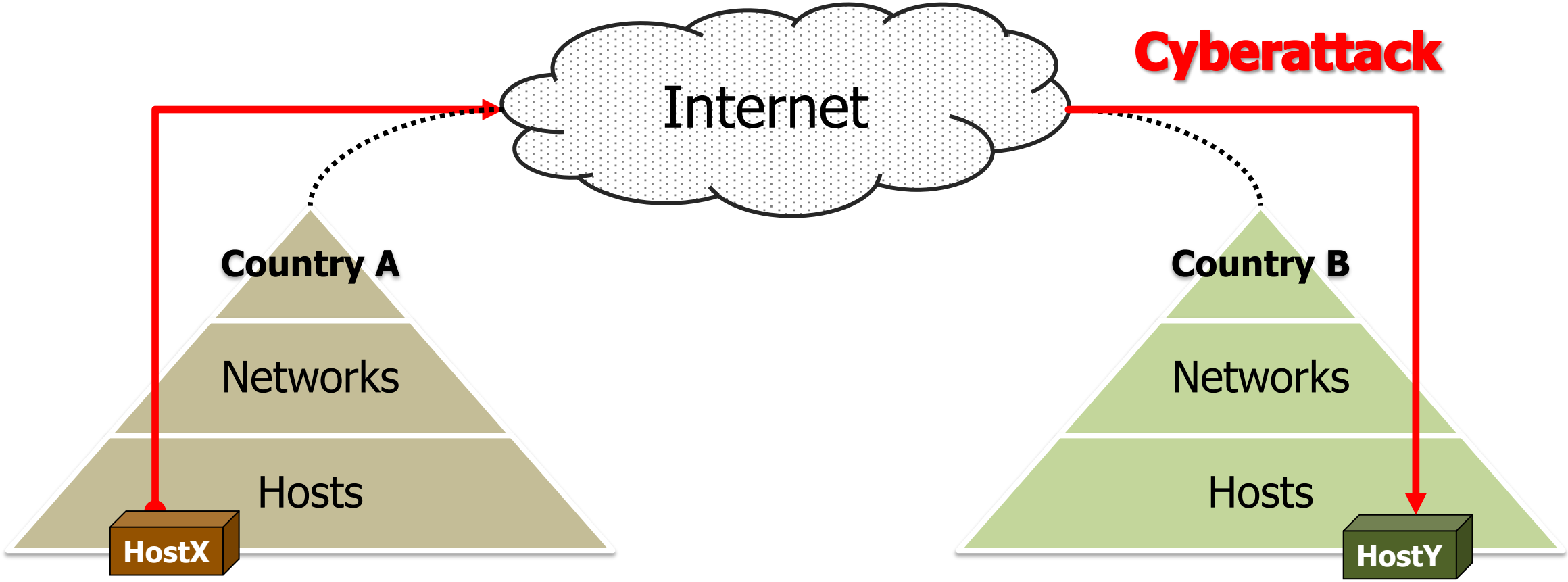
Measuring Cyber Attacks - WHO

- Cybersecurity of **A country?**
  - Cybersecurity ≒ Internet Security
    - ISO/IEC 27032:2012 – Guidelines for cybersecurity is now under revision with a new title: Guideline for Internet Security :-)
  - Geolocation vs. Internet address
    - Each IP address is assigned to a country
    - An attacker can use any country's host, off course
      - Hosting service, Botnet etc.

		Internet address allocation (million)
1	US	1500
2	CN	330
3	JP	200
4	GB	120
5	DE	110
6	KR	110
7	FR	90
8	CA	70
9	IT	50
10	BR	40
11	AU	40

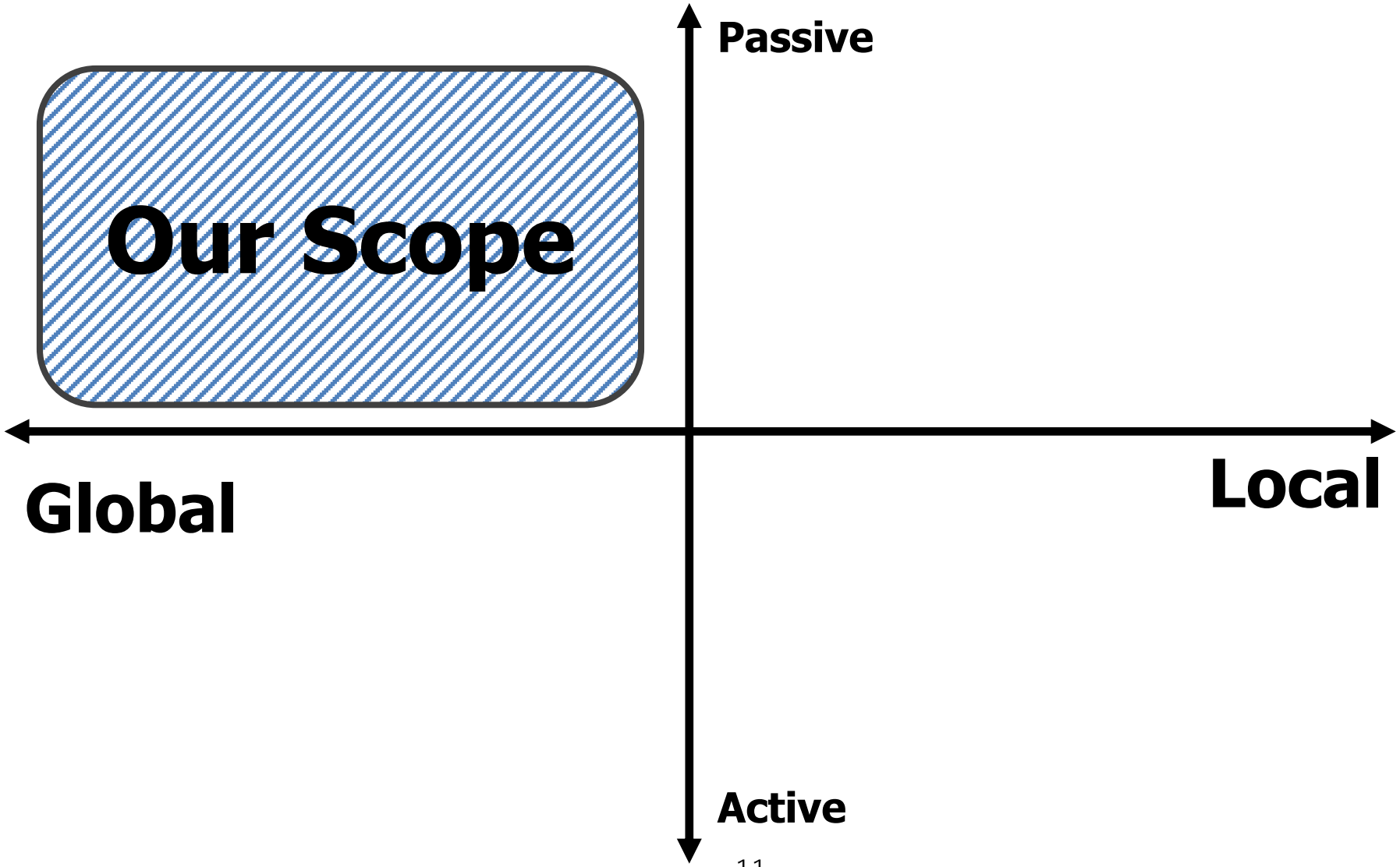
How Do We Observe Cyberattacks in Our Laboratory?

Our Scope



HostX of country A attacks HostY of Country B

Our Scope



Darknet Monitoring

Attacker

Network Scan Tools

Infected Hosts

HostX

Sensors

SYN

SYN + ACK

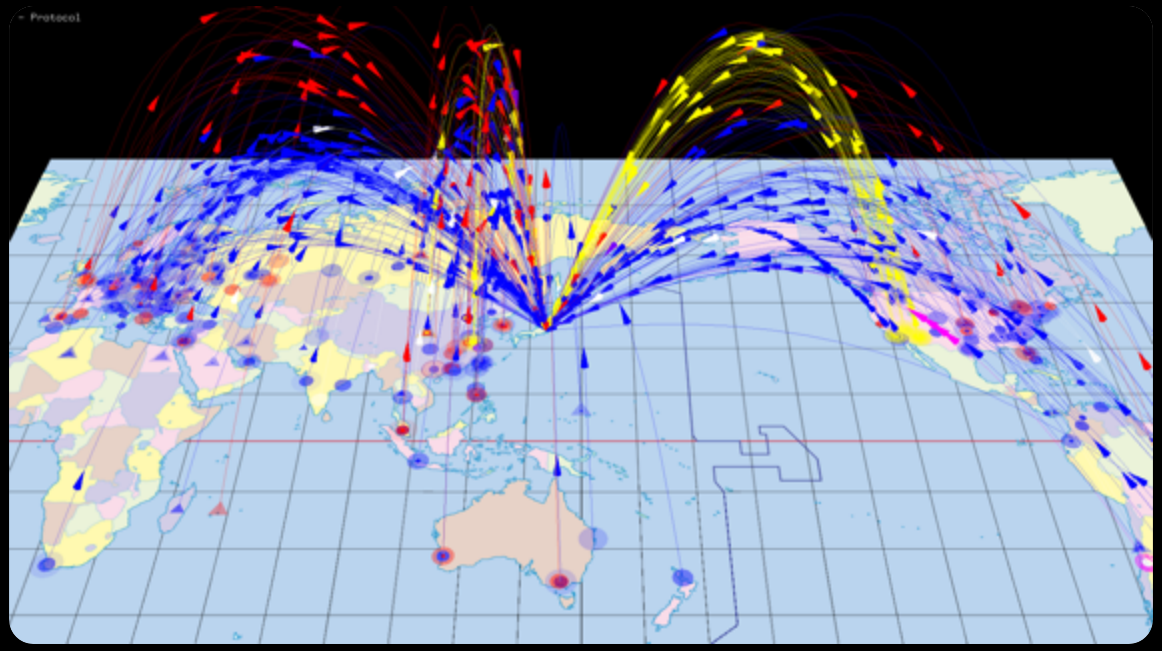
UDP

...

Our sensors will never respond.

Network scan of malware, research scan, reflection of DDoS attacks are observed

NICTER Atlas



- 30,0000 sensors (IPv4 addresses)
- Effective method for observing global, random attacks

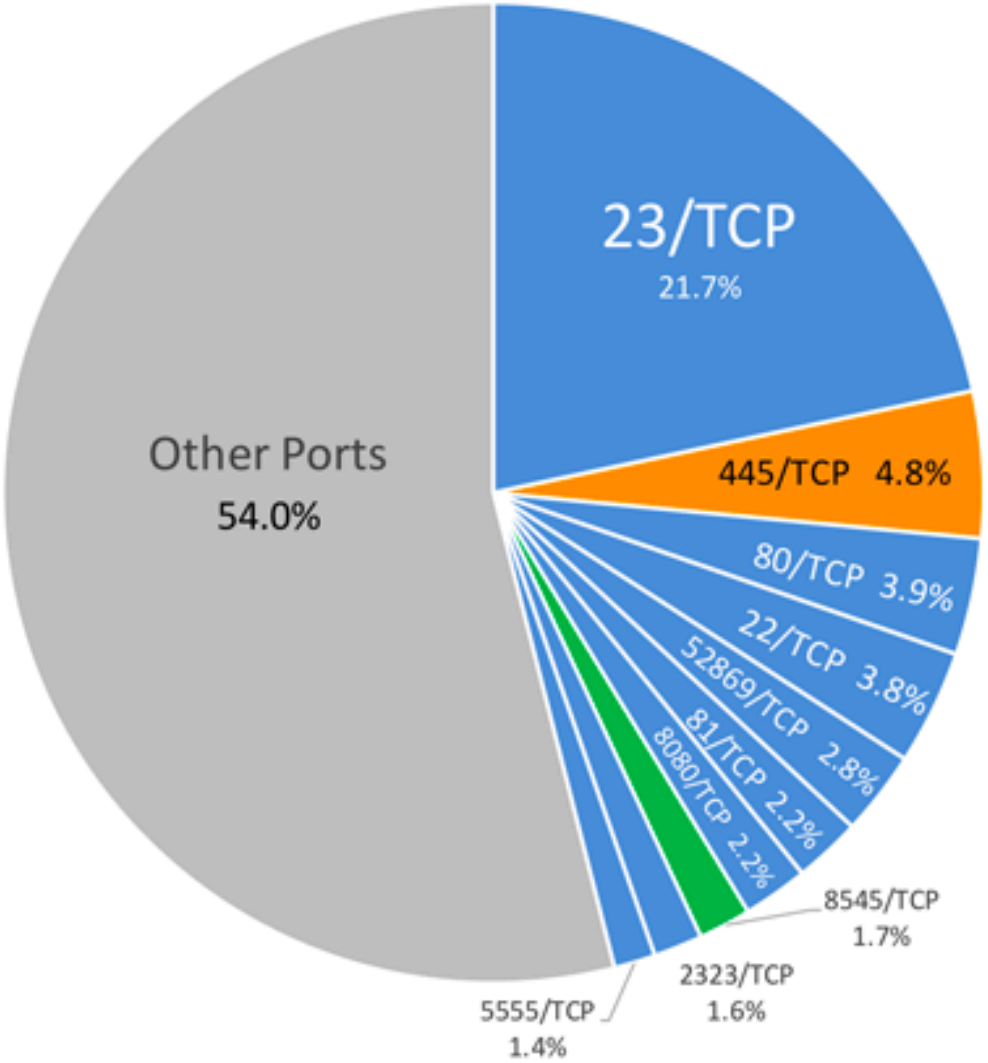

Global Trend

Total Yearly Attacks

Year	Total Packets	Sensor Addresses	Total Packets per sensor
2011	4.5B	120K	40,654
2012	7.78B	190K	53,085
2013	12.8B	210K	63,655
2014	25.6B	240K	115,323
2015	54.5B	280K	213,523
2016	128.1B	300K	469,104
2017	150.4B	300K	559,125
2018	212.1B	300K	789,876
2019 (estimate)	287.6B	300K	958,532

10X more attacks in the past 5 years

About Half of the Attacks Target IoT



ポート番号	攻撃対象
23/TCP	IoT機器 （Webカメラ等）
445/TCP	Windows（サーバサービス）
80/TCP	Webサーバ（HTTP） IoT機器（Web管理画面）
22/TCP	IoT機器（ルータ等） 認証サーバ（SSH）
52869/TCP	IoT機器（ホームルータ等）
81/TCP	IoT機器（ホームルータ等）
8080/TCP	IoT機器（Webカメラ等）
8545/TCP	イーサリアム（仮想通貨）
2323/TCP	IoT機器（Webカメラ等）
5555/TCP	Android 機器 （セットトップボックス等）

NICT National Institute of Information and Communications Technology

	Total Packet 2017	Total Packet 2018	Change	Increase (%)
Russia	11,562,849,149	49,314,675,237	37,751,826,088	426.5
China	**36,176,598,262**	**38,722,747,608**	**2,546,149,346**	**107.0**
U.S.A	22,767,104,642	25,459,602,115	2,692,497,473	111.8
Ukraine	2,655,374,113	12,131,652,686	9,476,278,573	456.9
Netherland	5,372,144,777	11,919,785,912	6,547,641,135	221.9
Chile	2,665,575,183	8,738,371,035	6,072,795,852	327.8
France	3,212,865,354	5,814,368,127	2,601,502,773	181.0
Brazil	6,887,435,973	5,663,397,123	-1,224,038,850	82.2
UK	2,130,203,730	4,853,576,338	2,723,372,608	227.8
Italy	1,642,265,277	4,335,502,372	2,693,237,095	264.0
Japan	**2,515,237,718**	**3,196,886,797**	**681,649,079**	**127.1**
Bulgaria	451,287,136	3,088,129,624	2,636,842,488	684.3
Korea	**6,236,288,185**	**2,629,346,857**	**-3,606,941,328**	**42.2**
Taiwan	4,472,008,096	2,181,762,030	-2,290,246,066	48.8
Vietnam	4,710,553,042	2,016,362,447	-2,694,190,595	42.8
India	5,917,768,114	1,808,629,544	-4,109,138,570	30.6
Argentina	3,122,746,805	635,832,252	-2,486,914,553	20.4

Why Russia is attacking so much?

Massive Global Increase of Espionage Scanning

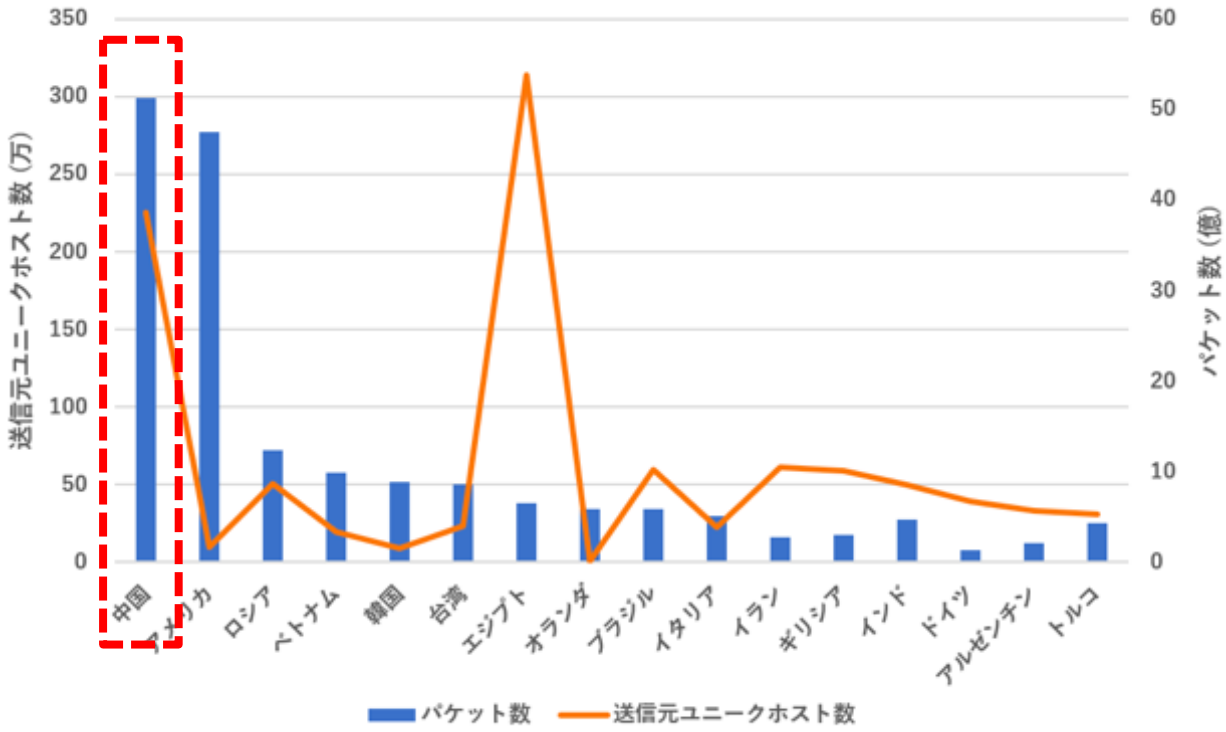
- A small number of host is scanning the Internet massively
  - The most active Russian host covered 1/400 of the total attacks in 2018
  - don't advertise themselves but possibly **espionage scanning**

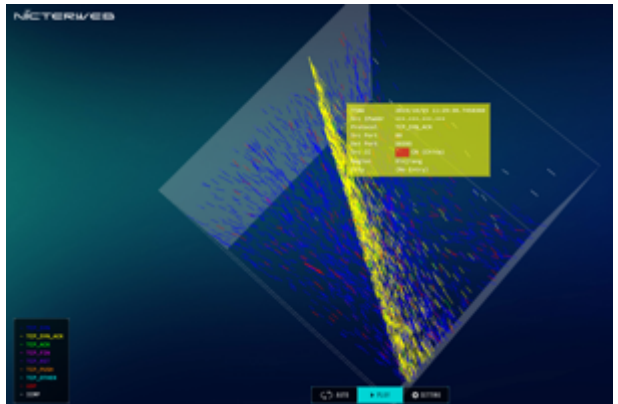
	2017	**2018**	2019 (1-2Q)
Total Packet	150B	**210B**	140B
From Large-scale Scanner	10B	**75B**	46B
% of Large-scale Scanner	6.8%	**35%**	32%

China

Trend of China

- The biggest host of **infected IoT devices**
  - Source of DDoS attacks
- **Vulnerability of Huawei's home router** has been a major target
- Occasionally victim of massive DDoS attack

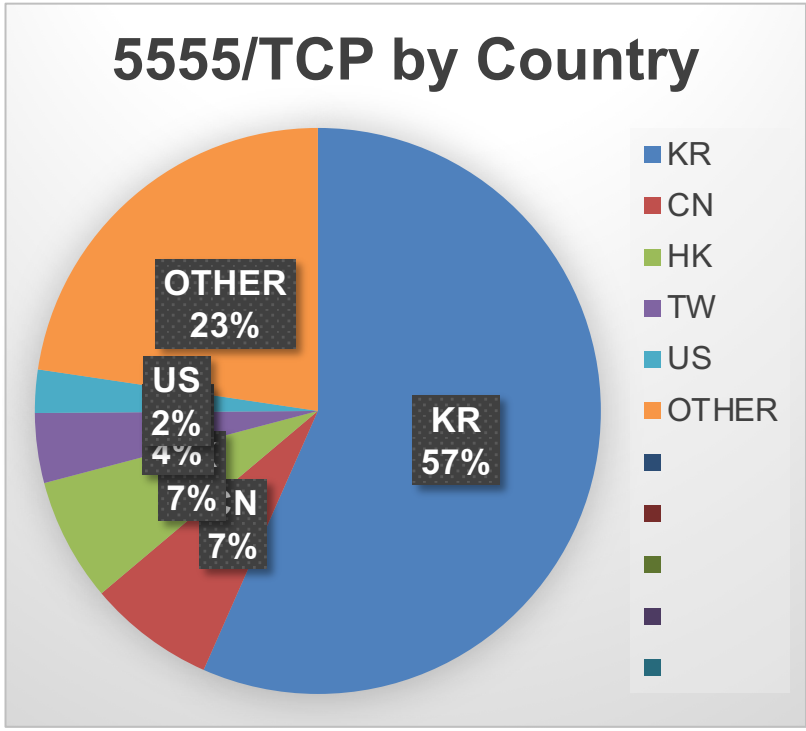




Korea

Trend of Korea

- The largest host of **vulnerable Android devices**
  - Android Debug Bridge is left open
  - Possibly Android Emulators for smartphone gamers
- Large unknown attack from SK Telecom
  - From about 600,000 hosts
  - Contacted SK but not response ☹



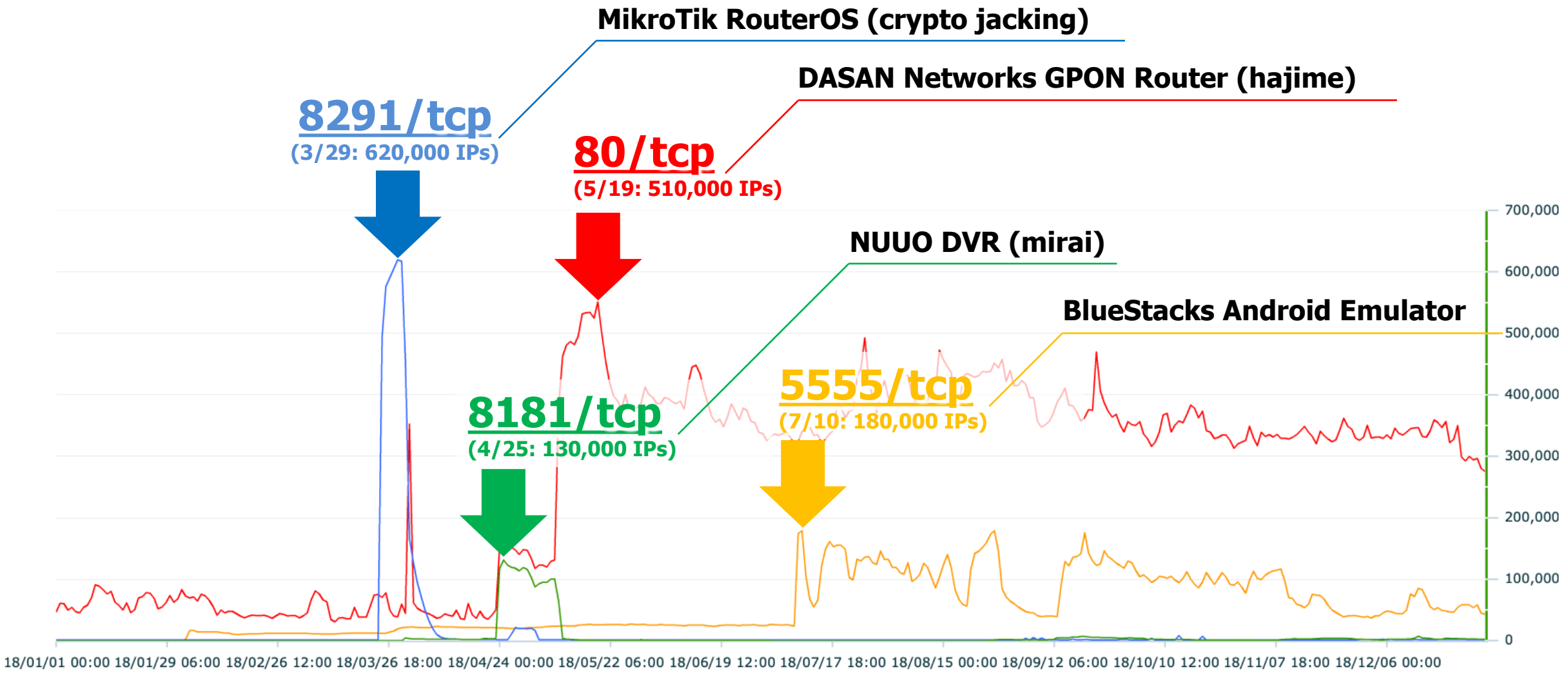
Japan

Trend of Japan

- Government (NICT) started scanning the internet of Japan and **try known ID/Pass** to find vulnerable IoT devices
  - Target: **100,000,000 address**
  - Could enter ID/pass: 98,000 hosts
  - Could login: **505 hosts**

- Cheap and not secure IoT devices
  - Long device lifecycle
  - Diverse user base
  - Not trivial to patch vulnerable system

Commonality of CJK Cybersecurity: IoT



Unique hosts / day (2018 Jan-Dec)