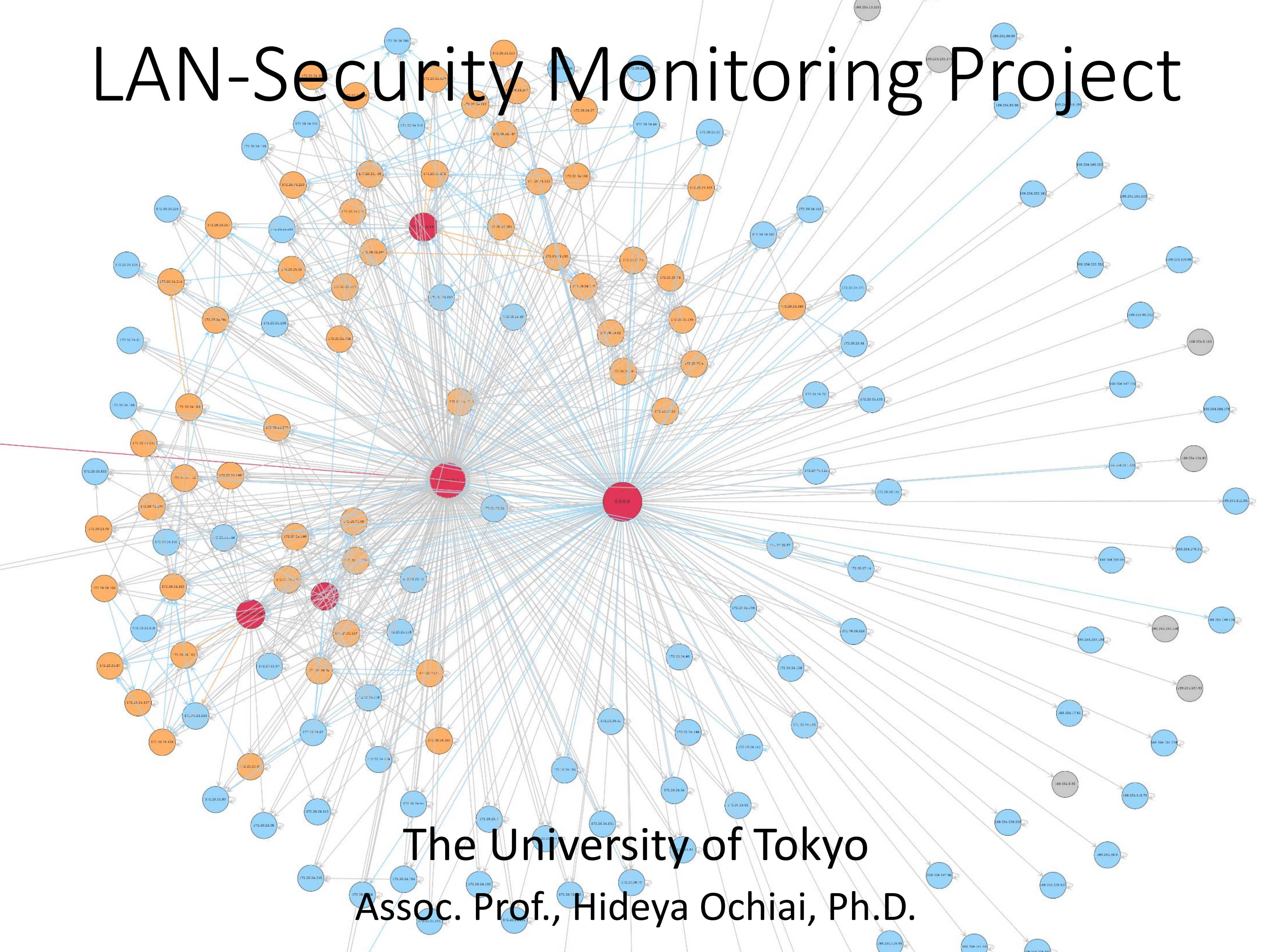
LAN-Security Monitoring Project



The University of Tokyo

Assoc. Prof., Hideya Ochiai, Ph.D.

Background: Cyber-Security Research

- Cyber-Security is now the major interest in network research community in Japan.
    - Decades Ago:
        - Development of Network Architecture, Routing, IoT Protocols, IoT Systems, Applications of IoT, Wireless Networks, etc…
    - Now and the Future:
        - Sustainability, Security, Management of Network/System Operation, Behavior of Networks, Reliability, etc…
- Issues 1: Computer Networks / Systems became so-complex and anyone (even engineers) cannot manage them.
- Issues 2: Legacy protection schemes such as Firewalls, Anti-Virus Software, etc., cannot protect them.
- Japanese Government raises the following topics for the researches of information technology.
    - Artificial Intelligence, Big Data, IoT, Cyber-Security

Background of “Research on LAN-Security”

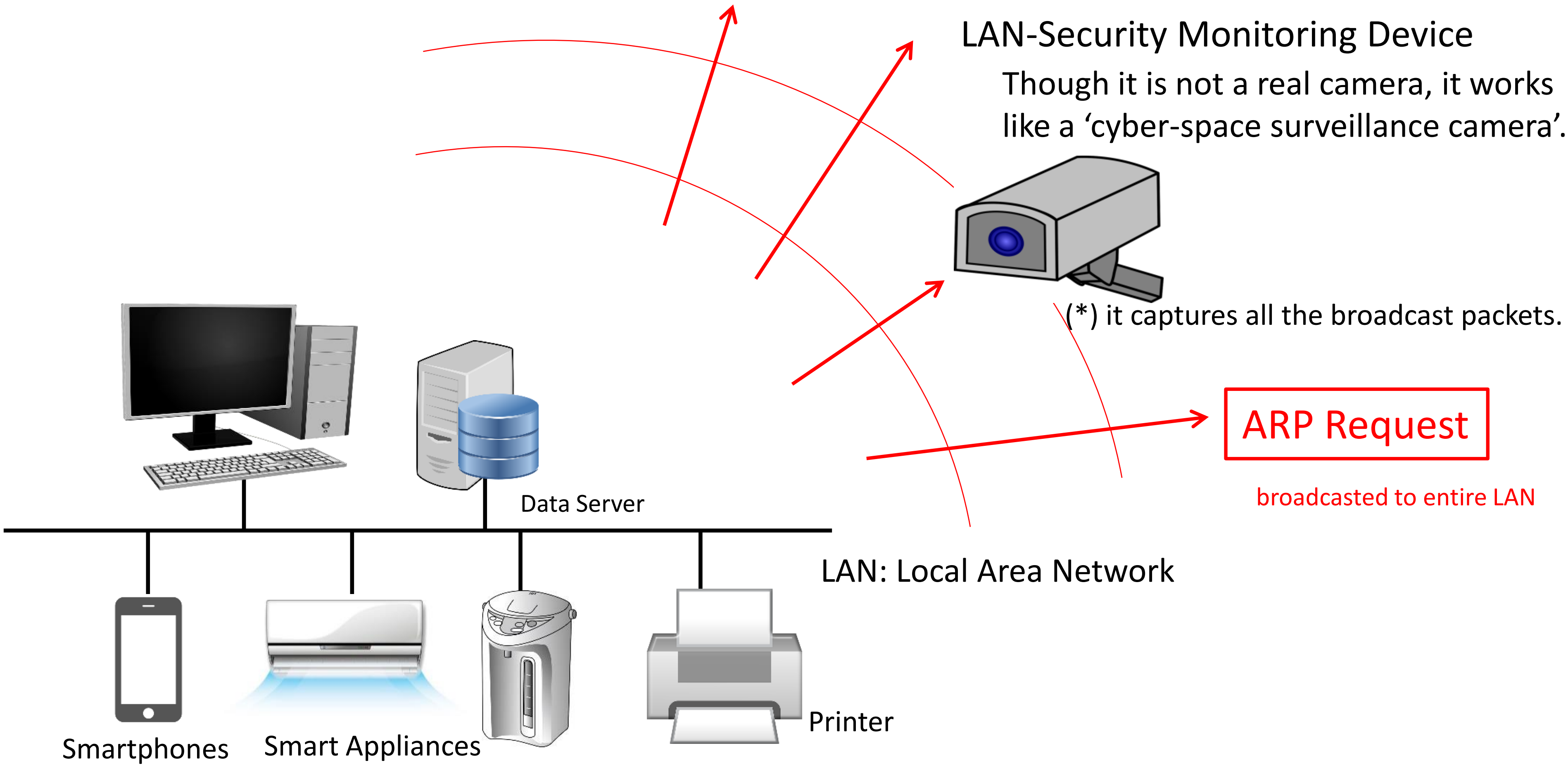
- Malware Intrusion into LANs
  - Malware Distribution by Phishing E-mails
    - Malware can be delivered into the hosts of LANs even if they have firewalls at the routers.
  - Connection of Malware-Infected Smartphones via Wi-Fi
    - Through Wi-Fi, malware can be spread from inside of the network.
- Vulnerabilities remain in LANs
  - Most of smart-home devices, smart-building devices, etc. can be easily accessed directly without authentication.
  - Support-expired operating systems are working without applying further patches (E.g. Windows XP).
  - Routers are deployed with default username/password for login from LAN-side.
  - Network cameras can be accessed with default username/password.

What happens if firewall becomes meaningless ??

LAN Security Monitoring Project

launched in Novermber 2018.

- Deployment of ‘LAN-Security Monitoring Device’ to capture malicious activities happens inside a LAN.

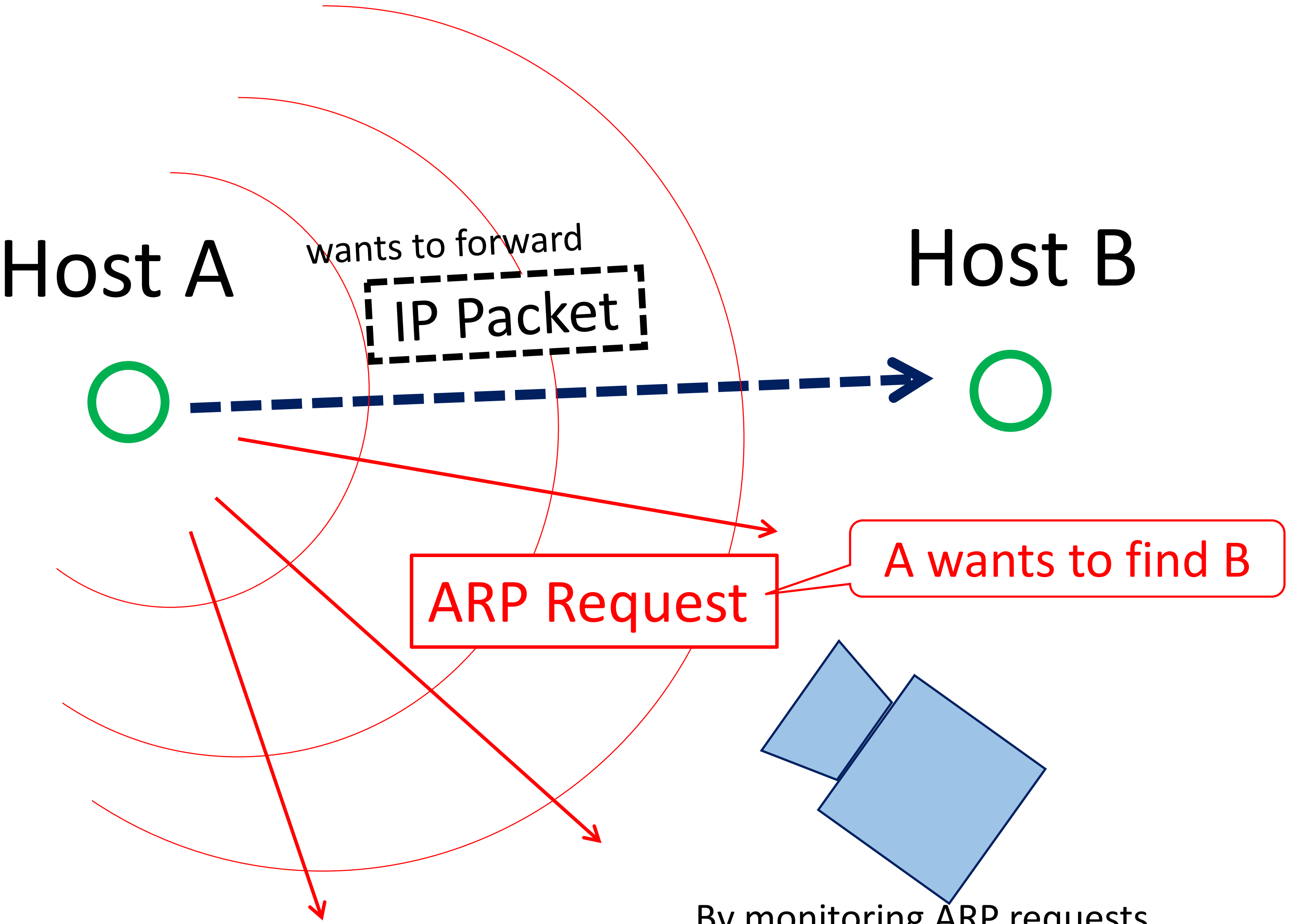


LAN-Security Monitoring Device

Though it is not a real camera, it works like a ‘cyber-space surveillance camera’.

(*) it captures all the broadcast packets.

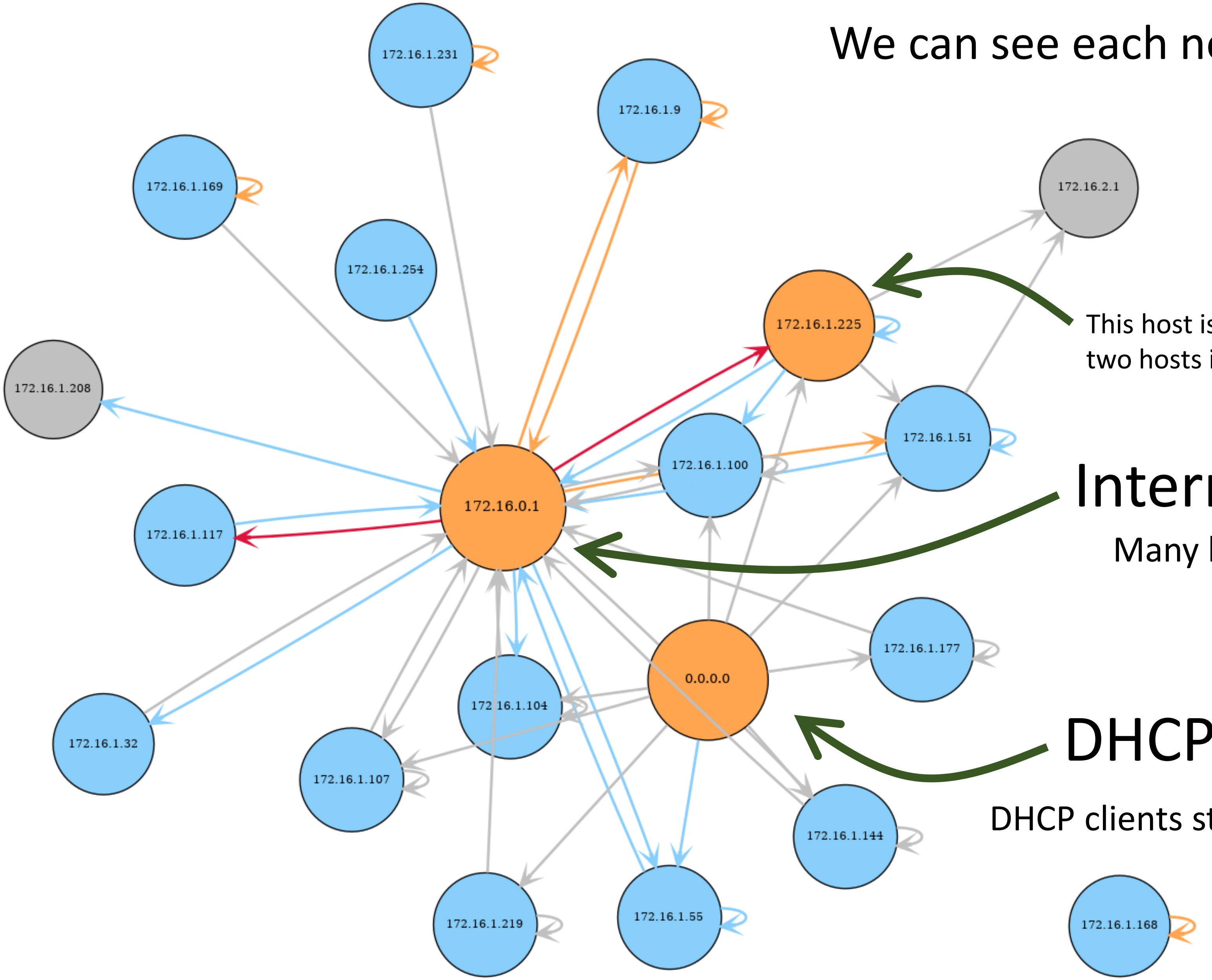
ARP Request prior to IP Packets



By monitoring ARP requests,
we can see that A wanted to communicate with B

Connection Graph generated in this way

We can see each node activity.



This host is directly talking to two hosts in the LAN

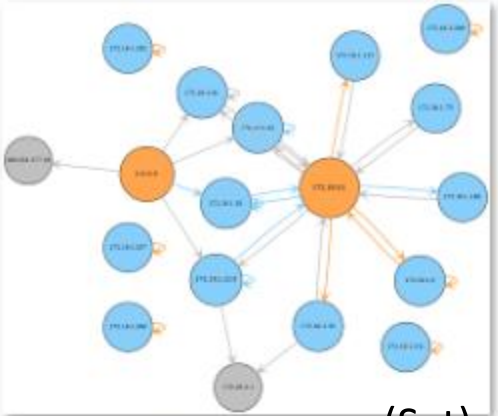
Internet GW

Many hosts use this.

DHCP client

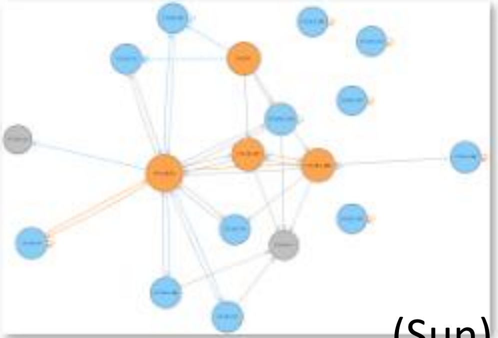
DHCP clients start from 0.0.0.0

Daily Connection Graph Changes (1/2)



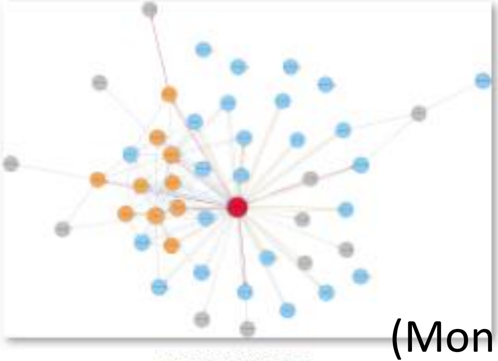
(Sat)

n019_20190629.png



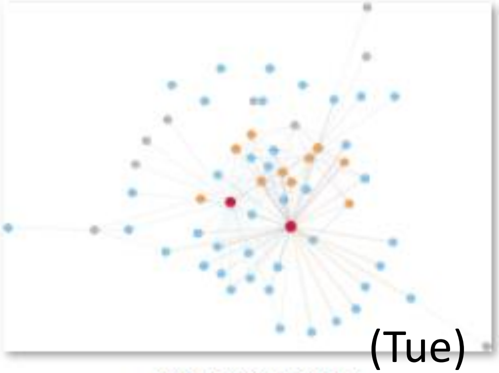
(Sun)

n019_20190630.png



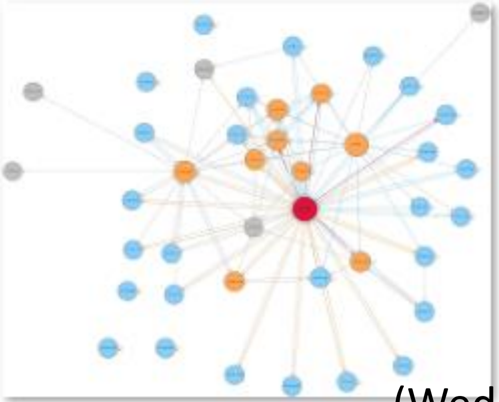
(Mon)

n019_20190701.png



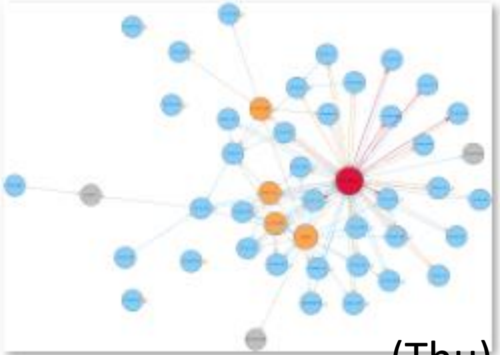
(Tue)

n019_20190702.png



(Wed)

n019_20190703.png

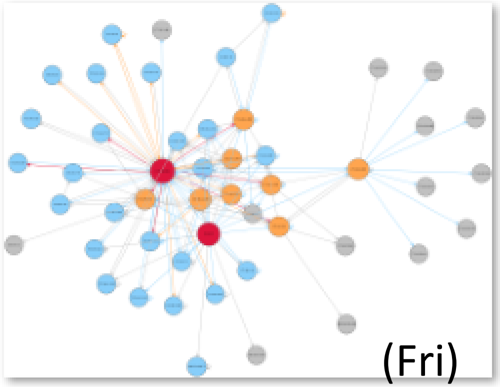


(Thu)

n019_20190704.png

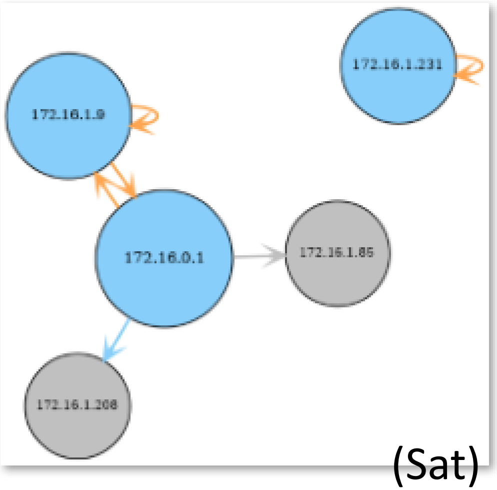
They contain nodes connectivity information : existence on the LAN.

Daily Connection Graph Changes (2/2)



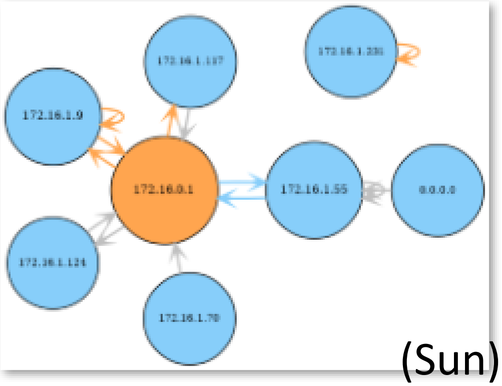
(Fri)

n019_20190405.png



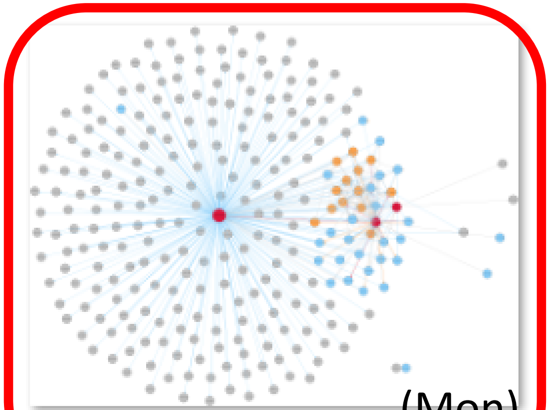
(Sat)

n019_20190406.png



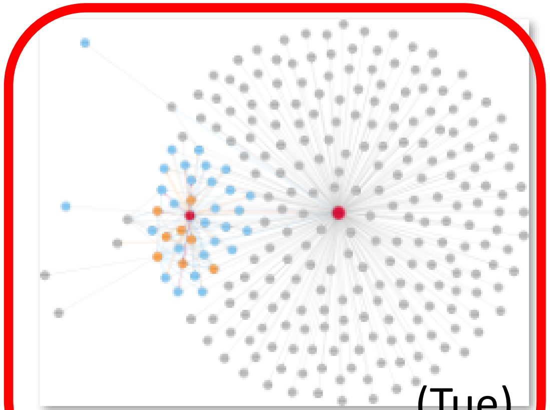
(Sun)

n019_20190407.png



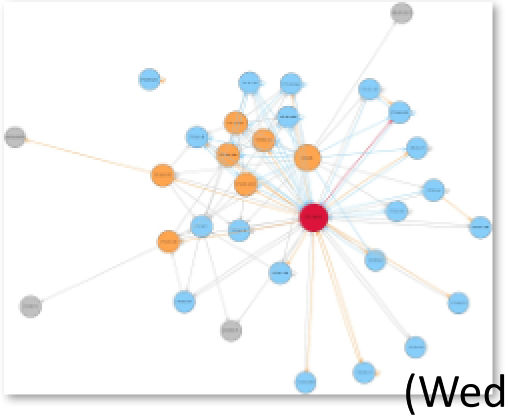
(Mon)

n019_20190408.png



(Tue)

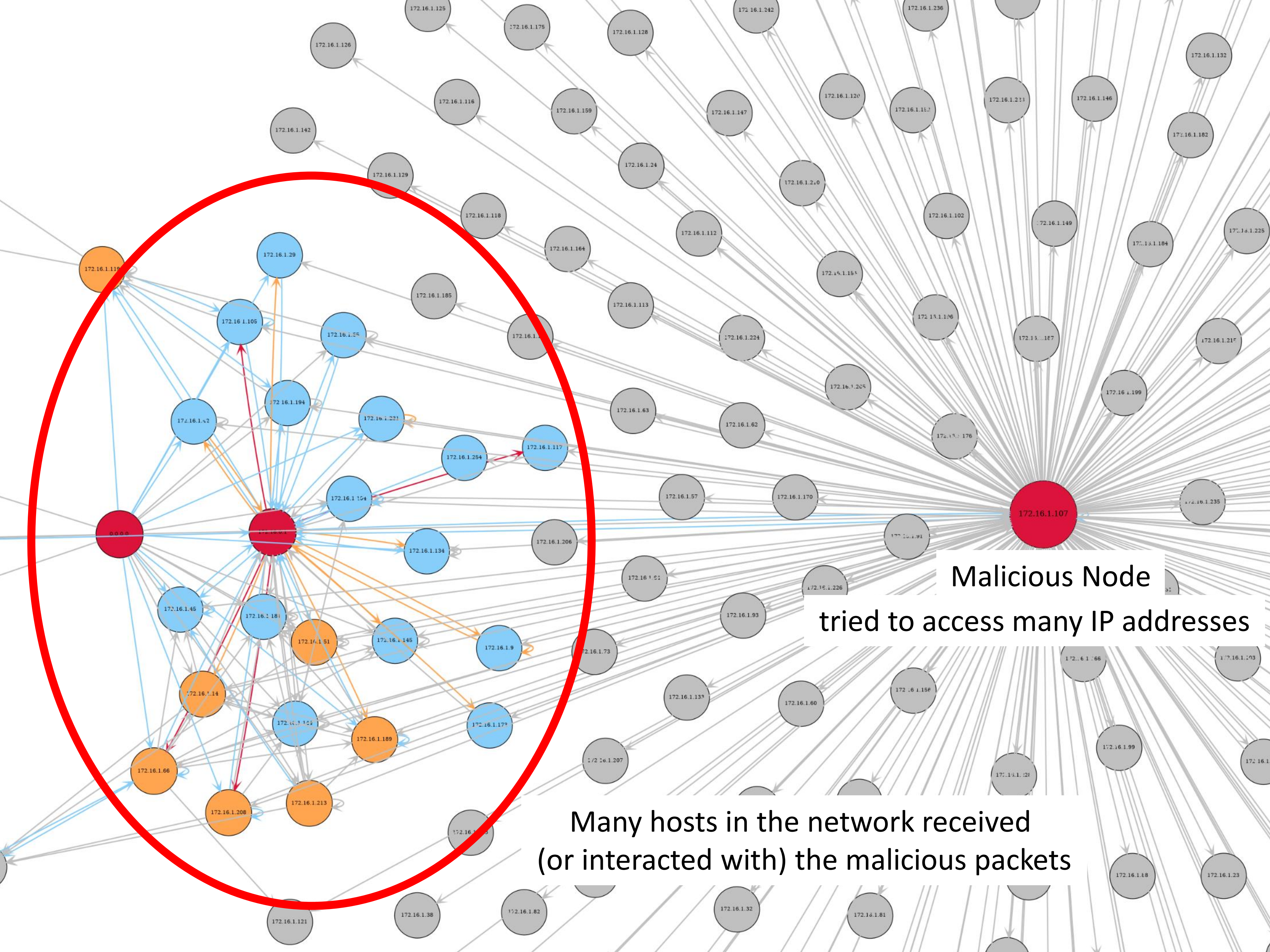
n019_20190409.png



(Wed)

n019_20190410.png

Anomaly Behavior



Malicious Node

tried to access many IP addresses

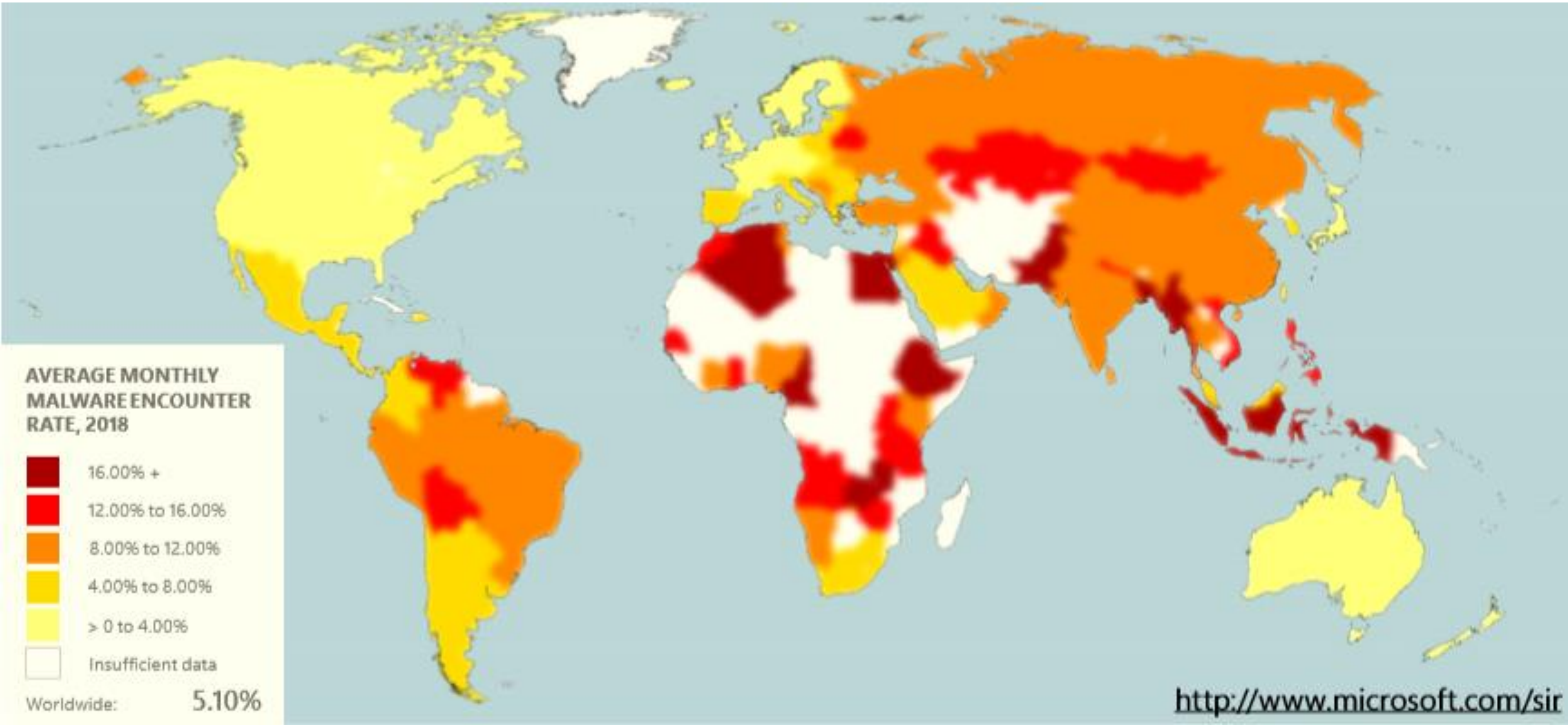
Many hosts in the network received (or interacted with) the malicious packets

LAN-Aware Malware

- Malware that spreads inside a LAN tries to find open TCP/UDP ports available -- for further intrusion.
    - It has to access hosts on the LAN, one-by-one, by sending IP packets to all the IP addresses.
- Spyware (that tries to intrude and retrieve data) may also work in the same way.
    - E.g., to find available database servers (MySQL, PostgreSQL), it sends IP packets to all the IP addresses.

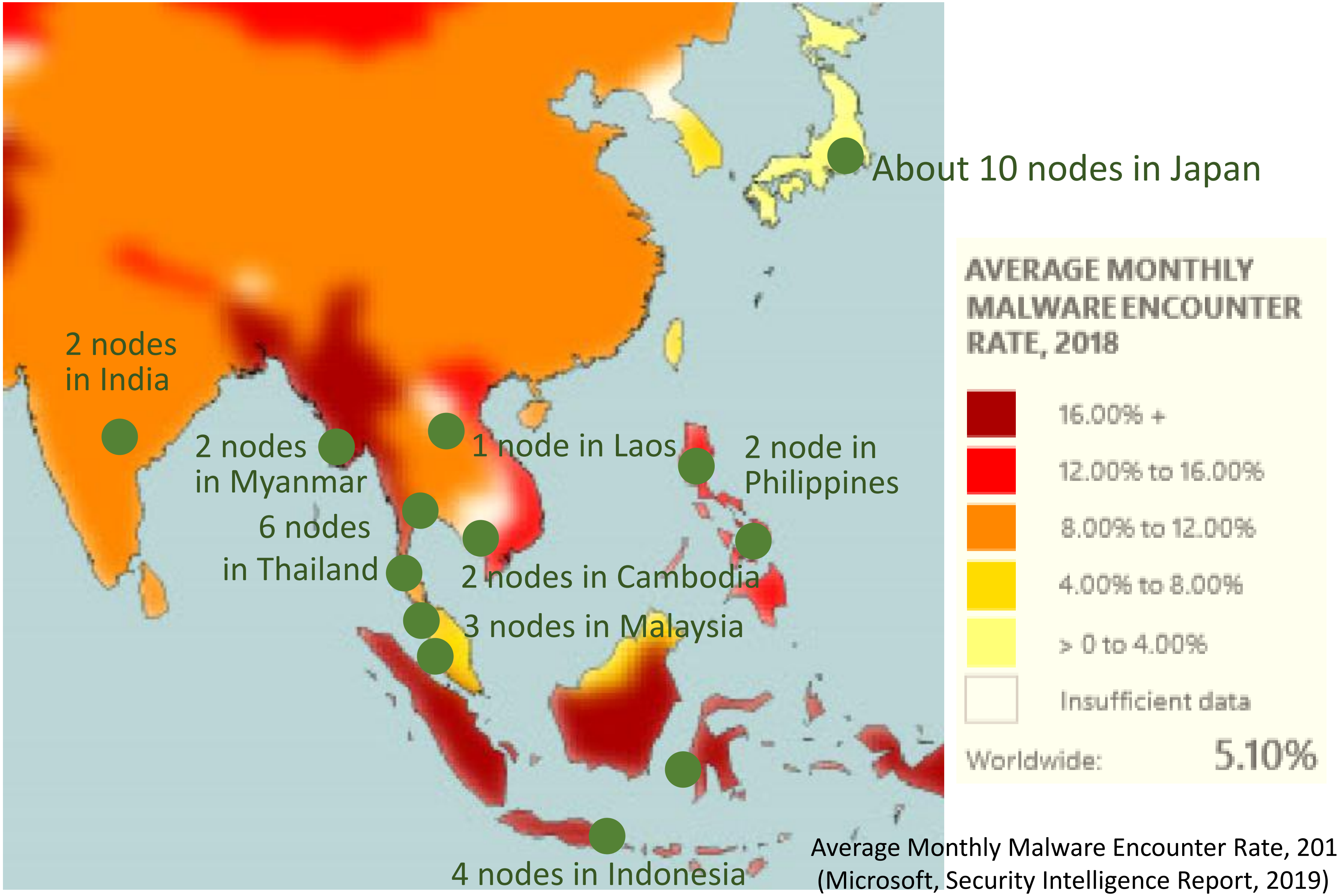
➔ “ARP Requests” to find the MAC address of the target IP address will be broadcasted from the malicious host to the entire local network.

Worldwide Malware Encounter Rate



Average Monthly Malware Encounter Rate, 2018
(Microsoft, Security Intelligence Report, 2019)

Collaboration with Asian Countries



Average Monthly Malware Encounter Rate, 2018
(Microsoft, Security Intelligence Report, 2019)

Joint Research Partners

(*) Alphabetical Order

Organizations of node installation (in progress) are listed.

ASEAN

- Cambodia
  - Institute of Technology of Cambodia
- Indonesia
  - Universitas Brawijaya
  - Universitas Hasanuddin
- Laos
  - National University of Laos
- Malaysia
  - Universiti Sains Malaysia
  - Universiti Tenaga Nasional
- Myanmar
  - University of Computer Studies, Yangon
  - University of Information Technology
- Philippines
  - ASTI
  - University of Philippines, Cebu
- Thailand
  - Asian Institute of Technology
  - Chulalongkorn University
  - Mahidol University
  - Prince of Songkla University
  - Thai-Nichi Institute of Technology
- Vietnam
  - Vietnam National University

East Asia

- Japan
  - Chiga Lab
  - Nara Advanced Institute of Science and Technology
  - United Nations University
  - Yamagata University
  - Individuals (Home Networks)

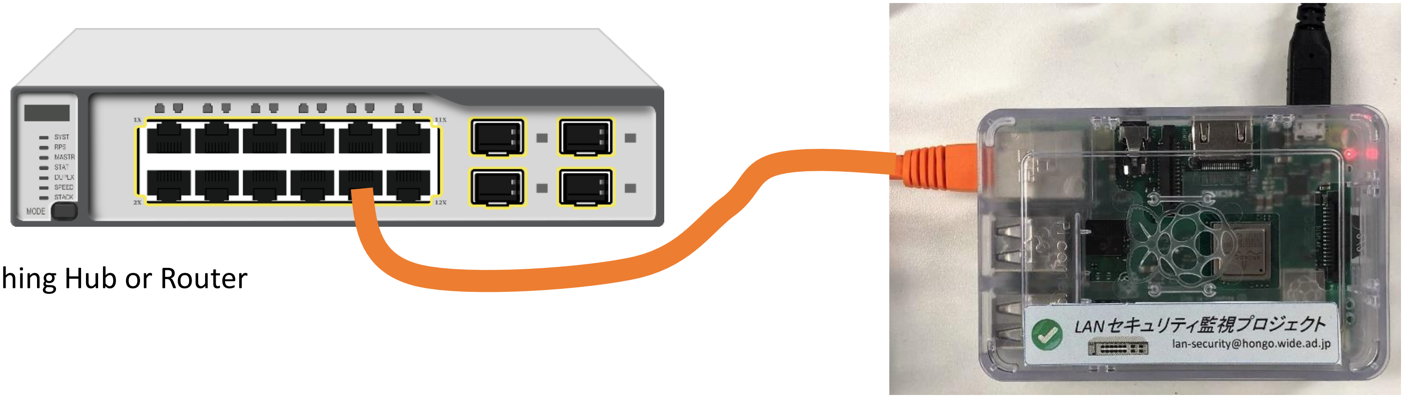
SAARC

- Bangladesh
  - Bangladesh University of Engineering and Technology
- India
  - Indian Institute of Technology, Hyderabad

คณะเทคโนโลยีสารสนเทศ
Faculty of Information Technology
泰日工業大学
IT
MT
BI
DC
MIT
วิทยาลัยการคอมพิวเตอร์
COLLEGE OF COMPUTING
COMPUTER SCIENCE
AND
INFORMATION MANAGEMENT
VIỆN TIÊN TIẾN VỀ KỸ THUẬT VÀ CÔNG NGHỆ
Advanced Institute of Engineering and Technology
IAN-Security Monitoring Project
UNIVERSITY OF INFORMATION TECHNOLOGY

Monitoring Device : How to Use

① Connect your ‘LAN-Security Monitoring Device’ to a LAN port of your switch hub or router.
(*) connecting to guest network is better (it is better not to deploy into critical networks).

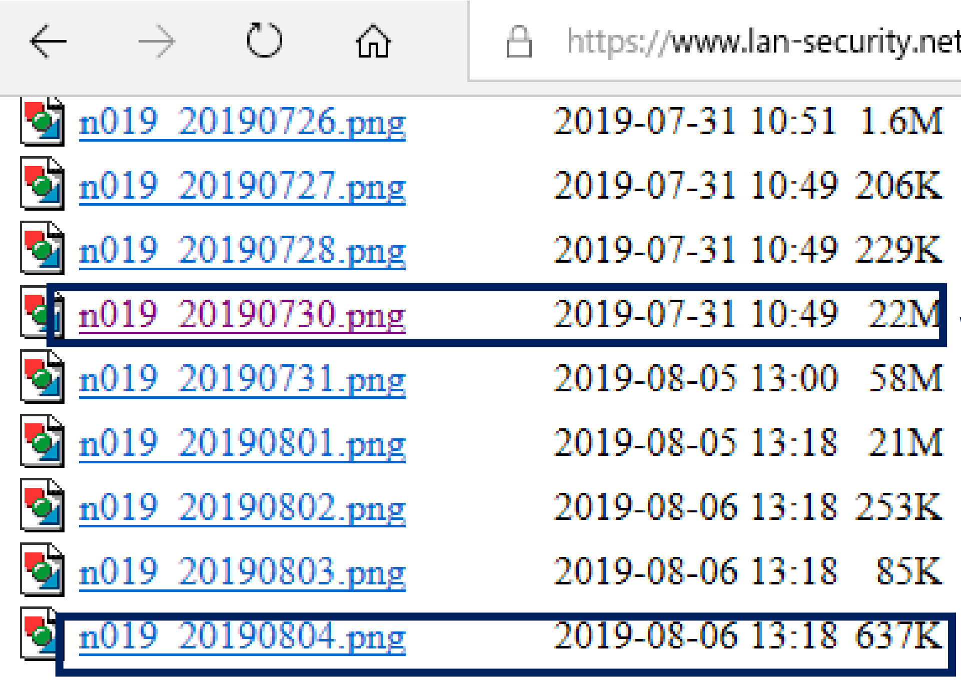

LANセキュリティ監視プロジェクト
lan-security@hongo.wide.ad.jp

Switching Hub or Router

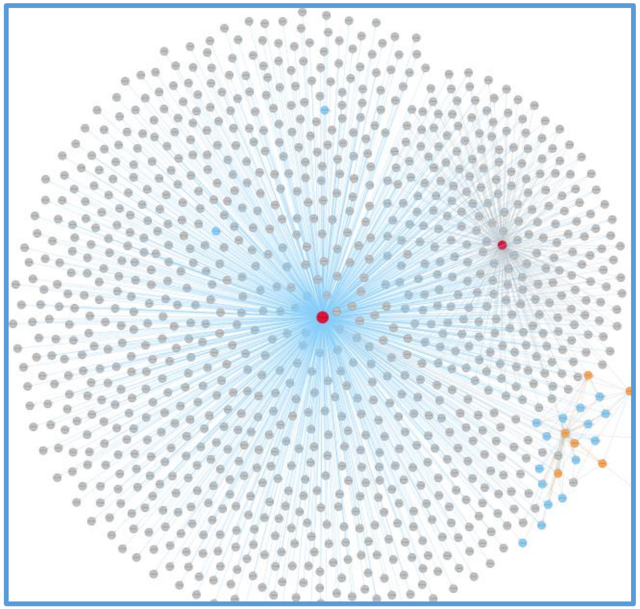
② Power on your ‘LAN-Security Monitoring Device’.

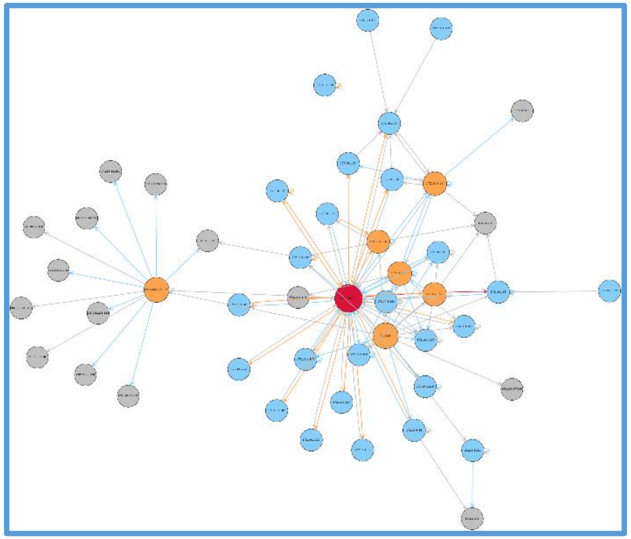
- As a surveillance camera `captures the view arrived at the device’, this device captures all the broadcasted frames in its LAN arrived at the device.
- The data shall be compressed, encrypted and transferred to the server securely-operated in the University of Tokyo through a secured channel at mid-night.
- If malicious activities are observed in the LAN, the server side program will detect its phenomenon, and notify to the network administrator.

Connection Graph Visualizer for Collaborators



```
https://www.lan-security.net/n019/
n019_20190726.png    2019-07-31 10:51  1.6M
n019_20190727.png    2019-07-31 10:49  206K
n019_20190728.png    2019-07-31 10:49  229K
n019_20190730.png    2019-07-31 10:49   22M
n019_20190731.png    2019-08-05 13:00   58M
n019_20190801.png    2019-08-05 13:18   21M
n019_20190802.png    2019-08-06 13:18  253K
n019_20190803.png    2019-08-06 13:18   85K
n019_20190804.png    2019-08-06 13:18  637K
```





Security Incident Notification to Network Administrator

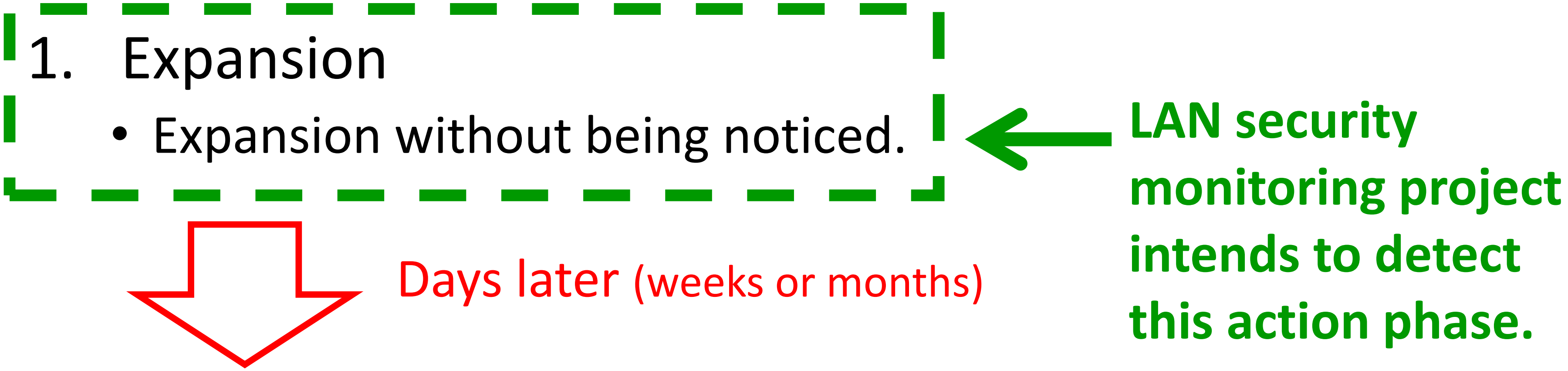
- If any malicious activities observed, the system will automatically generate incident report as follows and send to the network administrator.

```
1. Detected ARP scan from IP: 172.16.1.86 (MAC: d0:c6:37:83:48:89) on n019
It scans 256 IP addresses.
2019-07-11 10:36:08.416288      Who has 172.16.1.0 tell 172.16.1.86
2019-07-11 10:36:03.461982      Who has 172.16.0.1 tell 172.16.1.86
2019-07-11 10:36:08.416437      Who has 172.16.1.1 tell 172.16.1.86
2019-07-11 10:36:08.416759      Who has 172.16.1.2 tell 172.16.1.86
2019-07-11 10:36:08.417182      Who has 172.16.1.3 tell 172.16.1.86
2019-07-11 10:36:08.417548      Who has 172.16.1.4 tell 172.16.1.86
2019-07-11 10:36:08.417751      Who has 172.16.1.5 tell 172.16.1.86
2019-07-11 10:36:08.418137      Who has 172.16.1.6 tell 172.16.1.86
…

2. Detected 28 TCP SYN attacks from IP: 172.16.1.86 (MAC: d0:c6:37:83:48:89) during and after the ARP scan.
2019-07-11 10:36:08.426048 172.16.1.86:28837-->172.16.1.9:80
2019-07-11 10:36:08.938820 172.16.1.86:28837-->172.16.1.9:80
2019-07-11 10:36:09.824942 172.16.1.86:28837-->172.16.1.9:80
2019-07-11 10:36:10.826748 172.16.1.86:28849-->172.16.1.9:62078
2019-07-11 10:36:10.826750 172.16.1.86:28850-->172.16.1.9:445
2019-07-11 10:36:11.348420 172.16.1.86:28849-->172.16.1.9:62078
2019-07-11 10:36:11.348422 172.16.1.86:28850-->172.16.1.9:445
2019-07-11 10:36:11.860393 172.16.1.86:28849-->172.16.1.9:62078
2019-07-11 10:36:11.860395 172.16.1.86:28850-->172.16.1.9:445
…
```

Effectiveness of Malware Spreading Detection

* Malware Attack Phases in most of the cases



1. Expansion
   - Expansion without being noticed.

LAN security monitoring project intends to detect this action phase.

Days later (weeks or months)

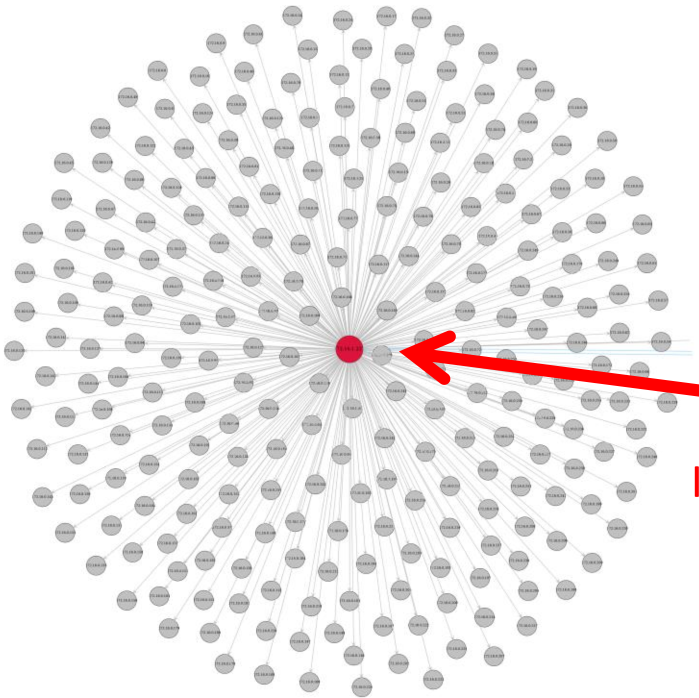
2. Action Simultaneously
   - Ransomware
   - DDoS Malware
   - Control over IoT devices
   - Video streaming from network camera
   - Information stealing malware

Advanced Topic: Honeypot-Enabled Monitoring Device

- By installing Honeypots in the monitoring device, it can make further interactions with the malicious node.
- Then, we can find its malicious level by observing the behavior.

Cowrie (SSH/Telnet Honeypot)
Dionaea (Samba, etc. Honeypot)

Setup

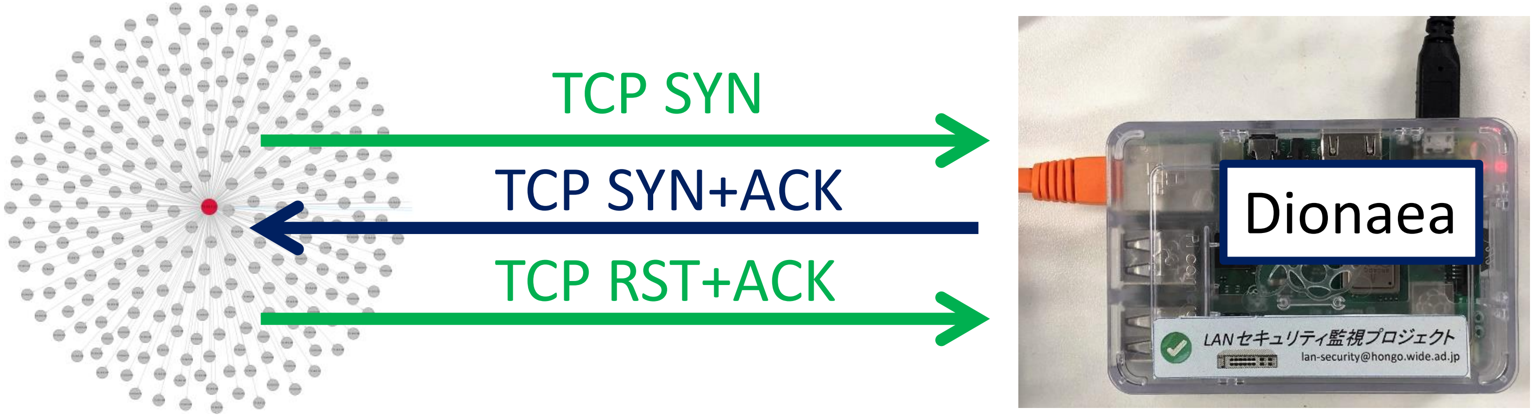


Interactions with the Honeypot

LANセキュリティ監視プロジェクト
lan-security@hongo.wide.ad.jp

Advanced Topic: Honeypot-Enabled Monitoring Device

- Vulnerability Testing Case: e.g., “nmap” case



TCP SYN

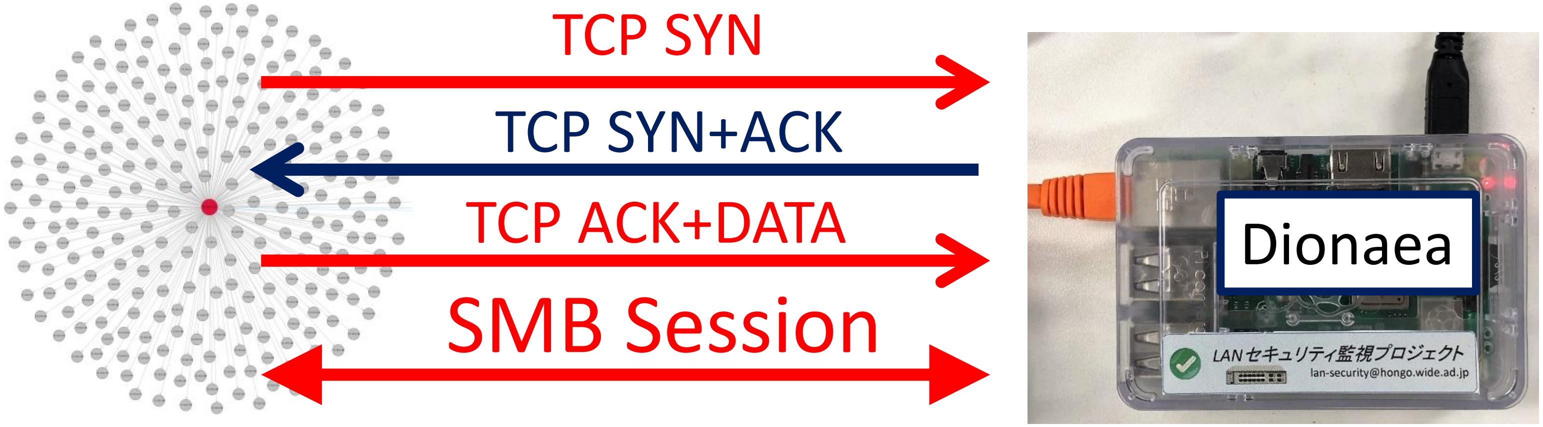
TCP SYN+ACK

TCP RST+ACK

Dionaea

LANセキュリティ監視プロジェクト
lan-security@hongo.wide.ad.jp

- Malware Attack Case: e.g., “WannaCry” case



TCP SYN

TCP SYN+ACK

TCP ACK+DATA

SMB Session

Dionaea

LANセキュリティ監視プロジェクト
lan-security@hongo.wide.ad.jp

Summary

- Cyber-Security research is the most advanced topic in network researches.
- By simply monitoring ARP requests, we can analyze malicious activities in the LAN.
    - Advanced topic : Honeypot-enabled monitoring
- The system of LAN-security monitoring project itself is useful for detecting malware expansion behavior.
- International collaboration is necessary to understand and overcome cyber-security problems.