Management of LAN Security with Cloud-Based Intrusion Detection

-- 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 November 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
broadcasted to entire LAN

Cloud

Analysis (i.e., Intrusion Detection) is made in Cloud

LAN: Local Area Network

Smartphones
Smart Appliances
Printer

Data Server
By monitoring ARP requests, we can see that A wanted to communicate with B.
Connection Graph generated in this way

Internet GW
Many hosts use this.

DHCP client
Hosts starts from IP 0.0.0.0.

This host is directly talking to two hosts in the LAN.
They contain nodes connectivity information: existence on the LAN.
Daily Connection Graph Changes (2/2)

(Fri)  
(Sat)  
(Sun)  
(Mon)  
(Tue)  
(Wed)  

Anomaly Behavior
tried to access many IP addresses

Many hosts in the network received (or interacted with) the malicious packets
Attacks: Changing IP address of the node (192.168.x.a/24, x=0,1,2,3), and scan for all IP in 192.168.x.0/24.

Assigned Network Segment

10.100.0.0/22

192.168.142.0/24

192.168.95.0/24

192.168.20.0/24
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

- About 10 nodes in Japan
- 1 node in Malaysia
- 1 node in Laos
- 5 nodes in Thailand
- 4 nodes in Indonesia

1 node in Myanmar

Average Monthly Malware Encounter Rate, 2018: 5.10%

(Microsoft, Security Intelligence Report, 2019)
Joint Research Partners

- Chulalongkorn University, Thailand
- Thai-Nichi Institute of Technology, Thailand
- Asian Institute of Technology, Thailand
- Prince of Songkla University, Thailand
- Mahidol University, Thailand
- National University of Laos, Laos
- University of Information Technology, Myanmar
- Universiti Kuala Lumpur, Malaysia
- Universiti Tenaga Nasional, Malaysia
- Universitas Hasanuddin, Indonesia
- Universitas Brawijaya, Indonesia
- Bangladesh University of Engineering and Technology, Bangladesh
- Bangladesh University of Professionals, Bangladesh
- Indian Institute of Technology Hyderabad, India
- Nara Advanced Institute of Science and Technology, Japan
- United Nations University, Japan
- University of Philippines, Cebu, Philippines
- Individuals (for Home Networks)
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).

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 will be serviced from the end of July 2019.

(*) You can see about your own devices only.
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.

   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 10:36:08.418137 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
   ...

   2019-07-11 10:36:08.938820 172.16.1.86:28837--->172.16.1.9:80
   ...

...
Effectiveness of Malware Spreading Detection

* Malware Attack Phases in most of the cases

1. Expansion
   • Expansion without being noticed.

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

Days later (weeks or months)

LAN security monitoring project intends to detect this action phase.
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

• Connection graph visualization service will start from the end of July 2019.

• The system of LAN-security monitoring project itself is useful for detection of malware expansion behavior.

• International collaboration is necessary to understand and overcome cyber-security problems.