# 第19部

# ネットワーク管理とセキュリティ

Glenn Mansfield Keeni,　Hiroshi Tsunoda

## 第１章　Introduction

The WIDE-Netman WG has been carrying out research and development to make the Internet more manageable and secure. The WG is working on analyzing real darknet traffic. Its purpose is to effectively identify Internet-wide scanning for research purposes in darknet. The WG is doing research and development on characterizing the behavior of network hosts by analyzing traffic traces. With an eye on Zero Trust to achieve enhanced security, the WG is working on developing a framework that expands the scope of information available for monitoring and management and is cost-aware, too. As a community-support effort, the WG is working on development of tools to facilitate cyber patrolling of social networking services (SNSs).

## 第２章　Analyzing Internet-wide scanning for research purposes in darknet

Darknet refers to reachable but unused IP address spaces which sees mainly suspicious traffic to non-existent targets. Analyzing this traffic is crucial for understanding cyberattack trends on the Internet. In recent years, the traffic caused by Internet-wide scanning activity for research purposes (ISRP) has been increasing. Correspondingly, the component of ISRP traffic in the darknet has increased and made it difficult to distinguish cyberattack patterns in darknet traffic. Therefore, identifying and filtering ISRP traffic is important. Several metrics have been proposed to identify the sources of ISRP traffic. But, there has been no comparative analysis of these metrics. To understand the characteristics and limitations of existing metrics, the WG analyzes real darknet traffic data using various metrics and visualizes the results. The progress of this work is presented in [84][85][86] and the paper [85] received FIT encouragement award and FIT young researcher award.

The WG will continue to develop appropriate metrics to automate the identification of potential research scanning activities. Additionally, the WG plans to investigate the impact on darknet analysis when excluding both slow-scanning traffic and large-scale research scanning traffic from darknet traffic data.

## 第３章　Profiling hosts in intranets

The WG is doing research and development on characterizing the behavior of network hosts.

To understand the activities of every host, the WG is focusing on utilizing eBPF (extended Berkeley Packet Filter) technology to identify the source applications of network packets. This year, the WG developed an eBPF-based packet capture system that can embed the application metadata into each packet when it is stored in a file. Such metadata is expected to be useful for efficient network forensics. The progress of this work is presented in [87][88]. The WG also explored the possibilities of an application-based access control system using SDN (Software-Defined Networking) technology. The progress of this work is presented in [89].

The WG has been engaged in research and development for detecting devices in an intranet. This year, the WG focused

on identifying the types of detected devices. Specifically, the WG developed a system that analyzes the content of the administrative WebUI of devices using an LLM (Large Language Model) to identify the devices. The progress of this work is presented in [90].

## 第 4 章 Towards Zero Trust: achieve increased transparency by expanding the scope of information available to management systems.

To make the network secure, it is necessary to implement the concepts of Zero Trust, which essentially requires checking and confirming every facet of the network and in every possible detail. This would require exhaustive monitoring and management, which, considering the practicalities of cost, is a very difficult target. As a first step towards Zero Trust, we expand the scope of transparency of interactions in the intranet and with the Internet, while keeping an eye on cost and complexity.

o the scope of information on intranet interactions is expanded from the MAC and IP addresses of connected hosts to include the MAC and IP addresses of the (attempted) peer connections.

o the scope of information on Internet interactions is expanded from traffic volume (counters for protocols, ports, hosts, destinations, etc.) to include the IP addresses (hosts/domains) and ports of the network flows seen at the entry point of the intranet.

The increased transparency provides a significantly deeper insight into the network behavior of the hosts in the intranet. For instance, an attempted access/connection from a user terminal to another user terminal maybe considered suspicious and worth further examination. On the other hand, an access to a network in a domain or country may raise the level of suspicion and call for further investigation if not, blocking and/or quarantining the corresponding host in the intranet.

The (attempted) peer connections in an intranet may be detected by a single sensor in the intranet from broadcast packets, and the Internet interactions may be monitored by a single flow monitor at the entry point of the intranet. From the cost and complexity point of view, that looks reasonable.

Zero Trust implies implementing a framework which has 100% or, "total" auditing or auditability. Towards this end, we explore the facets that can be covered in totality. For example,

a. monitoring the point(s) at which the intranet connects to the Internet we have a coverage of all Internet traffic from and to the intranet.

a-1 packet dumps can be taken to provide 100% auditabiliy of all Internet traffic.

a-2 every flow between the intranet and the Internet can be monitored. A new or "unusual" flow can be detected in (near) real-time

a-3 all DNS query requests and responses can be monitored.A new country, TLD, domain, or sub-domain access can be detected in (near) real-time.

Interestingly, the above features may be used to detect "unusual" communications within the intranet and between the intranet and the Internet. The "unusual" communications in turn provide significant clues to abnormality in the network e.g. malware attempting to infect other network devices in the intranet, malware attempting to contact its command and control server in the Internet, malware trying to steal information/data etc. Further, by mapping the IP address of a flow to a country, TLD, domain, or sub-domain the flows of interest may be narrowed down to flows destined to or sourced from "interesting" and/or "unusual" countries, TLDs, domains, or sub-domains. This year the WG conducted experiments to closely observe the flows between the intranet and the Internet and analyzed them based on DNS query information. The progress of this work is presented in [91][92].

## 第 5 章 Development of tools for efficient cyber patrolling

SNSs foster quick and easy communication among people, but there is a downside too. There are posts offering to sell illegal drugs, soliciting child prostitution and the like. In the country, prefectural police headquarters are seeking the help of civilian volunteers to "cyber patrol," i.e. find and report harmful SNS posts. The WG has been looking at supporting cyber patrols by developing tools that will make cyber patrolling easier.

The WG has developed a push-based system asking volunteers to judge whether a post should be reported. The developed system conducts keyword searches on Twitter to find posts with harmful words. The system scores the harmfulness of posts based on machine-learning technology and sends posts with high degrees of harmfulness to volunteers. They make a final judgment. Since 2022, the WG has been providing the developed system to volunteers and conducting a pilot study to evaluate its effectiveness.

This year, we have wrapped up these pilot-study results and the overall system development process into a journal paper [93].

## 第 6 章 Plans for 2025.

The WIDE-Netman WG will continue investigating data collection on a large scale and from small devices. We will continue working on

a. analyzing Internet-wide scanning for research purposes in darknet
b. profiling hosts in intranets
c. developing a cost-aware framework that expands the scope of monitoring and management, leads to enhanced transparency of the network dynamics and realization of the Zero Trust concept.
d. development of tools for efficient cyber patrolling