工学部２号館ゲスト無線 LAN（bld2-guest）のサイバーセキュリティ研究目的での利用について

情報理工学系研究科・電子情報学専攻
准教授 落合秀也
2019 年 5 月 吉日

■ 背景

近年、ローカル・エリア・ネットワーク（LAN: Local Area Network）を対象としたサイバー攻撃が頻繁に発生している状況です。bld2-guest を対象とした LAN 内のマルウェア活動の分析を狙いとした研究を実施させていただきたく存じます。サイバーセキュリティ対策に関する研究は、実ネットワーク環境を用いることが絶対的に必要であり、ご協力をお願いします。

■ 研究方法

bld2-guest の LAN セグメント上でブロードキャストされる Ethernet フレームを、tcpdump コマンドにより取得、保存します。MAC アドレスを取り除いたうえで、ARP リクエストに関する解析を行うことで、ホスト間の通信関係や、その時系列的な変化を分析します。マルウェアが LAN 内に侵入して、LAN 内でのスキャン活動を行えば、その挙動を検出することができます。

■ 実施期間

2019 年 5 月 ～ 2021 年 3 月末

■ データの取り扱いについて

取得したデータは、サイバーセキュリティ対策の研究のためにのみ使うこととします。なお、ブロードキャストパケットの取得による方式のため、通常の通信の中身は原理的に読めません。そのため、bld2-guest で行われたユーザのデータ通信の中身を解読することはできませんし、ユーザへの不利益は生じません。なお、研究終了後、取得したデータセットは破棄いたします。

■ 本件に関するお問合せ

情報理工学系研究科・電子情報学専攻
工学部 2 号館 102C2 号室
准教授 落合 秀也

About the Use of “bld2-guest” Wi-Fi Network for Cyber-Security Research

Graduate School of Information Science and Technology.
Information and Communication Engineering,
Assoc. Prof. Hideya Ochiai,

* Background

In recent years, cyber-attacks to local-area networks (LAN) have been frequently happening. We would like to start research on bld2-guest network for studying malware activities inside a LAN. We would appreciate if you understand the necessity of the use of real operational networks for cyber-security related researches.

* Method

We capture and archive Ethernet frames broadcasted over the segment of bld2-guest by tcpdump command. After eliminating MAC address information, by mainly analyzing ARP requests, we analyze host-to-host connection patterns and its historical trend. If malware intrude inside the network and made scanning activity, we can detect such activity.

* Period

From March 2019 to March 2021.

* Data Management

We use the collected data only for cyber-security research. As it captures only broadcasted frames, we cannot read the communication contents of the users by its mechanism. Thus, we cannot read the user contents exchanged over bld2-guest. There are no disadvantages for users. We will destroy the dataset after the research.

* Contact

Assoc. Prof. Hideya Ochiai,
Information and Communication Engineering,
Graduate School of Information Science and Technology.