IL-002

【既発表論文紹介】

Tracking Attack Sources based on Traceback Honeypot for ICS Network

阿部 真吾[†‡]　　洞田 慎一[†]
Shingo Abe　Shinichi Horata

出典： Proceedings of the SICE annual conference 2017, pp. 712-723.

本講演では，国際会議 SICE 2017 にて発表した，産業制御システム (Industrial Control System (ICS)) における，ネットワークセキュリティ上の脅威を検知するための応答型ハニーポットシステム (Traceback Honeyot System (THS)) について説明します．一般的に，ICS 機器はセキュリティ上の脅威を発見することを目的にログを出力しているとは限らず，マルウエアに感染した機器が発するパケットや，攻撃者による遠隔操作といったセキュリティ上の脅威を ICS 機器に残るログから発見することは一般的には困難であると考えられます．そのため脅威を発見することを目的として ICS ネットワーク内にハニーポットを設置し，攻撃者からのパケットを待ち受ける分析手法が提案されています．THS はこれを拡張し，ICS 機器の応答を模倣する機能や，ハニーポットへ到達したパケットに応答する機能を強化し，攻撃元に関する情報を収集することを目的に研究・開発を行いました．ICS ネットワークに対する既知のマルウエア (例 Havex RAT) について，感染端末は特定の機器に対するスキャンを行うことが分析において判明しており，応答型ハニーポットはそのような探索に対して，感染端末の特定を効率的に実施できると考えられます．そのため，応答型ハニーポットで得られた情報から，感染端末を切り分け，ICS ネットワーク上に存在する他の機器への感染拡大を防止するためにアクセス制限を行うなどの事前防御に活用することが可能であると考えます．本論文では，応答型ハニーポットの機能や動作について説明を行い，その有効性について考察を示します．

† 一般社団法人 JPCERT コーディネーションセンター, JPCERT/CC
‡ 名古屋工業大学

Copyright © 2018 by
The Institute of Electronics, Information and Communication Engineers and
Information Processing Society of Japan All rights reserved.