Contribution ID: **187** Type: **Paper presentation**

From Incident to IOC - An Automated Malware Investigation Pipeline

Thursday 18 September 2025 12:40 (15 minutes)

Incident response teams and security engineers are often overwhelmed by the large number of compromised artifacts requiring investigation and mitigation within short timeframes. This critical demand for speed and scalability emphasizes the important role of automation in modern post-incident processes.
This paper presents an automated forensic investigation pipeline specifically designed for malware detection and threat intelligence analysis for compromised QCOW2 disk images. The pipeline has three stages - extracting potential indicators from the affected targets, confirming their malicious nature, and sharing threat intelligence with the interested parties. The key tool for automating the analysis process is Dissect. Dissect is used to programmatically acquire system information and potentially infected artifacts. Once extracted, the indicators are triaged against a malware database. Finally, validated indicators of compromise (IOCs) are disseminated using MISP, a threat intelligence platform.
We validated this workflow by analyzing a substantial volume of compromised QCOW images collected from an SSH honeypot, showcasing its effectiveness in accelerating the analysis process. This work contributes to automating post-incident analysis by providing a modular pipeline that transforms raw forensic data into threat intelligence. This approach reduces the manual burden, ensures analysis reproducibility, and is easy to extend.

Authors: OCĂNOAIA, Andreia-Irina (National University of Science and Technology POLITEHNICA Bucharest); MIHAILESCU, Maria-Elena (National University of Science and Technology POLITEHNICA Bucharest, Romania); Mr NĂSTASE, Vlad-Iulius (National University of Science and Technology POLITEHNICA Bucharest); JUMAREA, Stefan Dorin (National University of Science and Technology POLITEHNICA Bucharest); CARABAŞ, Mihai (National University of Science and Technology POLITEHNICA Bucharest); DAGILIS, Lukas Vytautas (NRD Cyber Security); SANDU, Dragos (Revel Business Group)

Presenter: OCĂNOAIA, Andreia-Irina (National University of Science and Technology POLITEHNICA Bucharest)

Session Classification: Cloud Computing and Network Virtualisation

Track Classification: Network Security