# Dragging Attackers to Honeypots for Effective Analysis of Cyber Threats

**Martin Husák and Jan Vykopal**
Institute of Computer Science, Masaryk University,
Brno, Czech Republic
husakm@ics.muni.cz, vykopal@ics.muni.cz

## Introduction

- Honeypots, tools for attack analysis and zero-day exploit discovery, are passive in waiting for an attacker. Attracting more attackers is beneficial.
- We propose a novel approach to the effective utilization of honeypots based on cooperation between honeypots and the network in which they are deployed.
- We **map the attack vectors** and decompose the process of an attack into a series of simple events.
- Once we know the attack sequence, we can **detect its early phase and predict further intrusion**.
- Malicious network traffic is redirected to a honeypot for further analysis using a concept of a **network funnel**.

## Research Questions

I. **How does an attacker search for targets?**
We need to map the attack vector, the ways an attacker learns about new targets and picks the target to attack. Knowing the enemy's next move is the first step in taking appropriate countermeasures.

II. **How can we identify the attacker early and predict the attack?**
Once the attack vectors are mapped, we can detect events preceding the attack and predict the intrusion phase of the attack. Formal description and modeling of the attack may significantly improve the detection and prediction capabilities.

III. **How can we prevent the attack and still be able to analyze it?**
Common security measures, e.g., blocking, prevents the attacker from accessing the network but also prevents an analysis of the attack. The redirection of the malicious traffic to the honeypot for further analysis is a suitable solution.

## Mapping the Attack Vector

**Research question I.**
**How does an attacker search for targets?**

We observed and analyzed the attacks to learn in depth about the security threats. Host-based and network-based data were used to gain an overview of the attack process. The attacks can be decomposed into a sequence of events from network reconnaissance to an intrusion itself.

### Tools of the trade

- Honeypots are excellent source of host-based data.
- Network monitoring provides overview of the whole intrusion process including network reconnaissance and target discovery.
- NetFlow, IPFIX – usable in large-scale and high-speed networks.

### Related problem – honeypot advertising

- Attackers have to learn about honeypots. It is necessary to attract them.
- Common approaches include assigning domain names, running various services, providing eye-catching content, etc.
- Some approaches are out of scope of technology, e.g., black market exchange, information on hacking fora.

## Early Detection and Prediction of the Attack

**Research question II.**
**How can we identify the attacker early and predict the attack?**

The observed attacks are decomposed and described as a sequence of causal events. Prediction of an attack is based on detection of its early phases described by events.

### Decomposition of the attack

- Well-defined sequence of simple events is used to describe an attack.
- Simple events are easily detectable using flow-based network monitoring.
- The events include network reconnaissance as well as intrusion.

### Causality of the events in an attack

- Scanning for TCP port 22 commonly takes place before SSH brute-force attack.
- Can we study these events in reverse order? Are these events causal?
- Does SSH brute-force attack takes place after scanning for TCP port 22?

### Formalization of the attack

- Causal network is a suitable formal modeling language.
- Formal description of attacks serves as a prediction model.

### Attack prediction and early redirection

- The attack can be predicted if a sequence of events leading to an intrusion is detected.
- The suspicious network traffic is blocked from production network.
- Traffic can be redirected to honeypot instead, see Network Funnel.
- The attack is deflected before it can cause any harm.

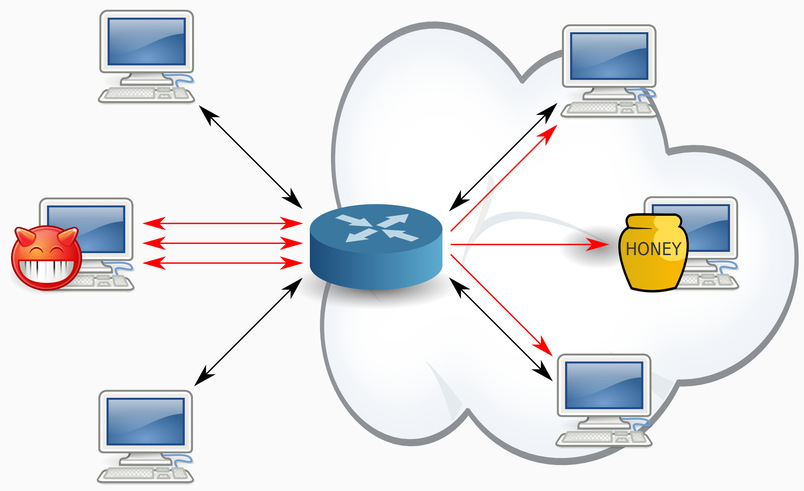
## Acknowledgement

This paper is supported by the Czech Ministry of Interior under Identification code VF2013201531.

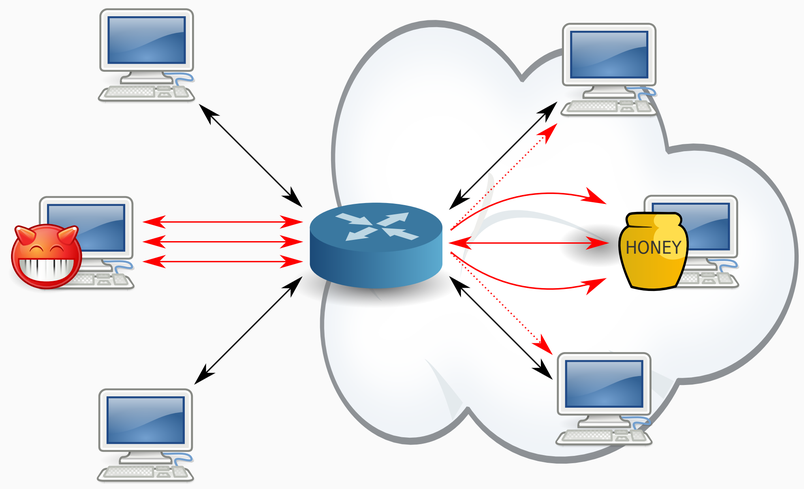
## Network Funnel

**Research question III.**
**How can we prevent the attack and still be able to analyze it?**

We cannot analyze the intrusion if we block the attack. Meanwhile, honeypots are passively waiting for an attacker. We propose an idea of a network funnel to redirect suspicious traffic to a honeypot to protect production network and analyze the attack.




The attacker is searching for targets, network monitoring tools detect suspicious activity (e.g., scanning) and pass the attacker's IP address to a network funnel controller.




Network funnel redirects any traffic from the attacker to a honeypot, which is mimicking regular hosts in the network. The attacker cannot access production network and we can analyze the attack using the honeypot.

Network funnel provides transparent traffic redirection, network address translation, and tunneling of the traffic between edge routers and honeypots.

## Conclusion

- We propose the utilization of network monitoring to extend data sources for attack analysis and to identify malicious network traffic early.
- We propose a concept of a network funnel in which the malicious traffic is transparently redirected to a honeypot.
- The redirection prevents the attacker from accessing the production network while the honeypots have a chance to analyze the intrusion.
- We can drag more attackers to a honeypot to analyze the attacks, learn about trends in network attacks, and possibly catch more zero-day attacks.
- We no longer have to passively wait for an attacker to access a honeypot, we actively drag them to a honeypot instead.