COMPUTERS & SECURITY 58 (2016) 180–198

Available online at www.sciencedirect.com

ScienceDirect

journal homepage: www.elsevier.com/locate/cose

Computers & Security

# Causality reasoning about network events for detecting stealthy malware activities [1]

Hao Zhang [a], Danfeng (Daphne) Yao [a,*], Naren Ramakrishnan [a], Zhibin Zhang [b]

[a] Department of Computer Science, Virginia Tech, Blacksburg, VA, USA
[b] Institute of Computing Technology, Chinese Academy of Sciences, Beijing, China

ARTICLE INFO

*Article history:*
Received 31 July 2015
Received in revised form 20 December 2015
Accepted 11 January 2016
Available online 21 January 2016

*Keywords:*
Network security
Anomaly detection
Stealthy malware
Traffic analysis
Dependence analysis
Machine learning classification

ABSTRACT

Malicious software activities have become more and more clandestine, making them challenging to detect. Existing security solutions rely heavily on the recognition of known code or behavior signatures, which are incapable of detecting new malware patterns. We propose to discover the triggering relations on network requests and leverage the structural information to identify stealthy malware activities that cannot be attributed to a legitimate cause. The triggering relation is defined as the temporal and causal relationship between two events. We design and compare rule- and learning-based methods to infer the triggering relations on network data. We further introduce a user-intention based security policy for pinpointing stealthy malware activities based on a triggering relation graph. We extensively evaluate our solution on a DARPA dataset and 7 GB real-world network traffic. Results indicate that our dependence analysis successfully detects various malware activities including spyware, data exfiltrating malware, and DNS bots on hosts. With good scalability for large datasets, the learning-based method achieves better classification accuracy than the rule-based one. The significance of our traffic reasoning approach is its ability to detect new and stealthy malware activities.



## 1. Introduction

Recent advancements in information technology have raised concerns on the security risks posed by the prevalence of malicious software. A study showed that a significant portion of computers worldwide is infected with malware conducting clandestine activities (Panda Security Report). Malware may spy on the victim user, cause data exfiltration, and abuse the computer for conducting bot activities (e.g., command-and-control). The initial infection vector of most malware is usually through exploiting vulnerabilities of common networked software, e.g., heap overflow vulnerability in a web browser or its plug-ins (Cova et al., 2010). Once the infection is successful (e.g., zero-day exploits), network requests from advanced malware may not exhibit distinct communication patterns. Because of this lack of signatures, pattern-based scanning is ineffective.

Compared to inspecting individual network requests, a more effective network security approach is to discover characteristic behavioral patterns in network event attributes. For example, BINDER (Cui et al., 2005) detects anomalous network activities on personal computers through analyzing the correlation in network events by the temporal and process information. BotMiner (Gu et al., 2008) performs a correlation

[1] The preliminary version of this work appeared in the Proceedings of the 9th ACM Symposium on Information, Computer and Communications Security (ASIACCS), Kyoto, Japan, June 2014 (Zhang et al., 2012) and in the Proceedings of 33th IEEE Symposium on Security and Privacy Workshops (SPW), San Francisco, CA, May 2012 (Zhang et al., 2014). This work was supported in part by an NSF grant CAREER CNS-0953638, ARO YIP W911NF-14-1-0535, and L-3 communications.

* *Corresponding author.* Tel.: +1 540 231 7787.
*E-mail address:* danfeng@vt.edu (D.(D.) Yao).

http://dx.doi.org/10.1016/j.cose.2016.01.002

analysis across multiple hosts of a network for detecting similarly infected bots. King et al. (2005) constructed directed graphs from logs to show network connections for dissecting attack sequences. However, none of these above solutions is designed for detecting general stealthy malware activities. Thus, they cannot be directly applied to our problem.

In this work, we describe a new *triggering relation discovery* problem to construct the request-level causality structure in network traffic. There have not been systematic studies on network-request-level causal analysis for malware detection. Existing dependence analysis work (e.g. Natarajan et al., 2012; Zand et al.) focuses on the network services and is not designed for malware detection. For example, NSDMiner (Natarajan et al., 2012) addressed the problem of network service dependency for automatic manageability and network stability. Rippler (Zand et al.) is proposed to actively perturb or delay traffic to understand the dependencies between service and devices. In comparison, we aim at achieving the *request-level* causality structure in network traffic. This finer granularity (request vs. flow) requires different relation semantics and more scalable analysis methods.

We introduce the problem of *triggering relation discovery* in network traffic and describe its application in solving challenging network security problems, such as stealthy malware detection. Triggering relations of events provide contextual interpretations for the behaviors of systems and networks, illustrating why sequences of events occur and how they relate to each other. We develop rule- and learning-based methods that detect network activities of stealthy malware activities through reasoning their causal relationship. We design a new method *pairing* that produces special pairwise features in the learning-based approach, so that the discovery problem can be efficiently solved with existing binary classification methods (e.g., SVM). By enforcing a *root-trigger* policy, we can identify the suspicious events that lack of valid triggers, and thus ensure an application's correct responses to user activities.

The higher-level information such as the underlying relations or semantics of events is useful for human experts' cognition, reasoning, and decision-making in cyber security (Green et al., 2008; Zhang et al., 2015). Thus, analyzing relations among network events provides important insights for identifying general stealthy malicious activities. The causality offers the logical interpretation to the vast amount of otherwise structureless and contextless network events. Our work demonstrates that triggering relations among cyberspace events enables the network assurance with structural evidence of the hosts.

Our contributions are summarized as follows.

1. We formalize the problem of triggering relation discovery in network requests, the data structure of triggering relation graph, and their applications for detecting stealthy malware activities.
2. We present two approaches for discovering the triggering relations among network events. First, we design a discovery algorithm based on empirically derived rules. In the rule-based approach, we inspect the temporal, semantic, and process-related attributes to reveal the causal relations among network requests. Then, we propose an advanced learning-based approach. A new feature extraction method is introduced as the *pairing* operation. It performs pairwise attribute comparisons, enabling the use of binary classifiers for our triggering relation discovery.
3. We adopt a new *root-trigger security policy* on discovered triggering relations for malware detection. This policy allows one to identify *vagabond events*, i.e., network events that do not have proper causes to justify their occurrences.
4. We extensively evaluate the classification and detection accuracy rates of our solution with DARPA dataset and real-world network traffic, including HTTP, DNS, and TCP traffic. Both rule- and learning-based methods are compared in identifying the dependencies and the learning-based one yields better prediction accuracy rates than rule-based one. We show that our dependence analysis is effective in detecting stealthy malware activities (e.g., HTTP-based malware and DNS bots).

Triggering relation discovery provides a new perspective for analyzing network traffic. It allows one to reason about the occurrences of network events, to detect unexplained network activities that are due to stealthy malware. The significance of our traffic reasoning approach is its ability to detect new and stealthy malware activities.

Major new results reported in this journal publication compared with previous conference papers (Zhang et al., 2012, 2014) are summarized as follows. We report the side-by-side comparisons of the rule-based and learning-based dependency analysis approaches. We perform new experiments evaluating the rule-based approach in discovering the triggering relations on HTTP traffic and in detecting HTTP-based malware (e.g., stand-alone data exfiltrating malware). We conduct new experiments on a DARPA dataset to evaluate our solution in detecting the stealthy malicious activities (exploits due to vulnerable applications). Last but not least, this journal version presents the rule-based and learning-based computation techniques under a unified triggering relation discovery framework. Such an abstraction can help motivate and inspire future research on causality reasoning for security.

### 1.1. *Organization*

We introduce the triggering relation graph and its security applications in Section 2. Then we present the rule- and learning-based methods in Sections 3 and 4, respectively. We illustrate the root-trigger policy and its use in Section 5. We systematically evaluation our solution with real-world malware and synthetic attacks in Section 6. Related work and conclusion are presented in Sections 7 and 8.

## 2. Model and overview

In this section, we introduce the concept of triggering relationship, define the problem of *triggering relation discovery*, and present the security applications.

### 2.1. *TRG definitions and properties*

*Triggering relationship* between event $e_i$ and event $e_j$ describes the temporal relation and causal relation between them, specifically $e_i$ precedes $e_j$ and $e_i$ is the reason that directly causes $e_j$ to occur. The specific semantics of triggering relation depend on the type of events and environment. An event may be defined