Stochastic Modeling of Self-Evolving Botnets with Vulnerability Discovery

Takanori Kudo, Tomotaka Kimura, Yoshiaki Inoue, Hirohisa Aman, Kouji Hirata

PII: S0140-3664(17)31199-4
DOI: 10.1016/j.comcom.2018.04.010
Reference: COMCOM 5686

To appear in: *Computer Communications*

Received date: 20 November 2017
Revised date: 9 March 2018
Accepted date: 13 April 2018

Please cite this article as: Takanori Kudo, Tomotaka Kimura, Yoshiaki Inoue, Hirohisa Aman, Kouji Hirata, Stochastic Modeling of Self-Evolving Botnets with Vulnerability Discovery, *Computer Communications* (2018), doi: 10.1016/j.comcom.2018.04.010

Stochastic Modeling of Self-Evolving Botnets with Vulnerability Discovery

Takanori Kudo[a], Tomotaka Kimura[b,*], Yoshiaki Inoue[c], Hirohisa Aman[d], Kouji Hirata[e]

[a] *Faculty of Science and Engineering, Setsunan University, 17-8 Ikeda-nakamachi, Neyagawa, 572-8508 Japan.*
[b] *Faculty of Engineering, Tokyo University of Science, 6-3-1 Niijuku, Katsushika, 125-8585 Japan.*
[c] *Graduate School of Engineering, Osaka University, 2-1 Yamadaoka, Suita, 565-0871 Japan.*
[d] *Center for Information Technology, Ehime University, 3 Bunkyo-cho, Matsuyama, 790-8577 Japan.*
[e] *Faculty of Engineering Science, Kansai University, 3-3-35 Yamate-cho, Suita, 564-8680 Japan.*

Abstract

Machine learning techniques have been actively studied and achieved significant performance improvements in various kinds of tasks. While we benefit from such techniques in many ways, they can be a serious security threat to the Internet if malicious attackers become able to utilize them to discover unknown software vulnerabilities. This paper introduces a new concept of self-evolving botnets, where computing resources of infected hosts are exploited to discover unknown vulnerabilities in non-infected hosts and the botnets evolve autonomously. We provide a stochastic epidemic model for the self-evolving botnets, and show its behaviors through numerical and simulation experiments.

Keywords:
Botnet, computer virus, machine learning, continuous-time Markov chain

1. Introduction

We face threats of malware such as computer viruses, worms, and Trojan horses, due to the rapid growth of the Internet [19, 26]. One of the most serious security threats is the spread of botnets [17, 30], which are networks of hosts infected by malware. Such infected hosts are usually called zombie computers, and they are controlled to infect computers on the Internet with the botnet malware itself, via e.g., E-mail messages, websites, and social networking services (SNSs). Their attacks are usually performed through known vulnerabilities in software, so that they are basically effective only to non-updated hosts.

However, the threats of attacks become significant when an unknown vulnerability, called zero-day, is exploited. Because of its large impact to the cyber security, attackers make considerable efforts on *vulnerability mining*, i.e., discovering unknown vulnerabilities. Recently, some researchers have proposed algorithms of automatically discovering unknown vulnerabilities based on *machine learning techniques* [28, 34]. While the main purpose of these works is to develop efficient methods in protecting software, malicious attackers can also discover unknown security holes using such techniques and exploit them for illegal attacks.

Machine learning techniques with the state-of-the-art performance such as *deep learning* [23] require large computational resources, and it is known that distributed computing with a large number of inexpensive hosts can efficiently improve their performances [10]. It is then naturally expected that as an extension of [28, 34], high-performance vulnerability mining methods based on a large-scale distributed computing will be developed. If such learning methods are integrated with the self-rewriting capability of botnets [4, 7, 25], the threats of them will become far more serious than ever before.

Based on these facts, this paper introduces a new concept named *self-evolving botnets*. Self-evolving botnets exploit computing resources of zombie computers and perform distributed machine learning to discover unknown vulnerabilities, and they evolve autonomously so that discovered vulnerabilities can be utilized to infect other hosts.

The purpose of this paper is to evaluate the impact of self-evolving botnets on the cyber security, particularly with respect to their contagiousness. To that

*Corresponding author. Tel.: +81-3-5876-1717
Email addresses: t-kudo@ele.setsunan.ac.jp (Takanori Kudo), kimura@ee.kagu.tus.ac.jp (Tomotaka Kimura), yoshiaki@comm.eng.osaka-u.ac.jp (Yoshiaki Inoue), aman@ehime-u.ac.jp (Hirohisa Aman), hirata@kansai-u.ac.jp (Kouji Hirata)