Metric design for Botnet Infection problem

Santiago Aragón, Daniel Meinsma, Pallavii Jagannatha, Owais Ahmed
University of Twente, Nederlands

I. Introduction

Internet Service Providers are the problem owners of the security issue as measured in our first assignment. It is of primary interest to them to avoid having unwanted traffic in their network due to botnets. This is undesirable as it would exhaust their resources and cost them money.

II. title

In this section we analize the output of the metrics proposed in [**?**]. Based on this output we compare the performance of the distinct network owners. We detail how the security performance can me compared using applying the metrics to a subset of the the problem owners i.e. ISPs in Beijing.

A. BN propagation

B. Network infection radio

C. BN geographical and digital location

III. State-of-the-art metrics

a) To work with Industry and other stakeholders on developing a policy to implement: ISPs are in a better position to understand the issues associated with botnets and can act on the botnet threat. They stand a better chance at formulating the solution with internationally co-ordinated policy efforts which involves all stakeholders.

b) Promote public participation: When voluntary codes of practice are received to battle botnets, ISPs must be urged to openly advance their cooperation in the project. They must likewise be urged to show how they are accomplishing consistence with the code.

c) The code of conduct should contain: a) a registration component, b) an awareness-raising component, c) guidance on network management; d) high-level advice on how to respond to threats and e) a reporting component.

d) Privacy protections should be included in policies for botnet responses: The measures taken to fight botnet might possibly affect a person's privacy, contingent upon the appropriate lawful structure and variables, for example, how contaminated machines are recognized. These dangers can be diminished through the privacy-sensitive design of systems and hierarchical procedures and in addition appropriate supervision.

e) Devise mechanisms for reliable and verifiable communications during notification: Policy makers and ISPs must consider how best to implement authentication mechanisms that encourage reliable communications between ISPs, consumers and other actors.

f) Consider multi-channel notification method: ISPs should consider to depend on various channels of correspondence to inform users about the vicinity of bots.

g) Design policies using effective metrics: The consolidation of good measurements into frameworks and empowering the reporting of measures to pertinent powers would be a helpful step. Metrics must be universally practically identical to assist members with recognizing best practices across borders and urge different nations to advance such activities.

h) Measures for prevention should be taken: Attempting to instruct users about how to shield themselves from installing malware and inadvertently transforming their PCs into bots is a key component of a thorough methodology.

i) Go for worldwide interoperability: Worldwide cooperation amongst national governments, specialized bodies and authoritative foundations is significant if the botnet danger is to be foiled.

j) Financial aid for policy development to implement: Government offices must contribute both towards start up and introductory operational expenses wherever conceivable and work with ISPs to discover reasonable methods for covering the long term operational expenses.

IV. title

Cloud Providers Cloud providers enable sharing of computing resources like storage, services, servers, networks, and application. They are provided with minimum management efforts and very quickly. With this background, attackers can use their cloud bots for distributed password-cracking, click fraud, or denial of service attacks that flood target websites with junk traffic. Because the cloud services offer far more networking bandwidth than the average home computer possesses, their botnet can funnel huge attack traffic at any given target which is undesirable for cloud providers.

LAE

Affected parties (DOS spam victims)

V. title

VI. title

References