Risk analysis of botnet evolution

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

I. Who is the problem owner of the security issue as measured in your first assignment?

Botnet infection and evolution is a security issue that affects many parties in cyberspace, i.e. ISP, LAE, cloud and hosting providers, botnet victims and zombie machine owners. Each party receive a different kind of harm because of this security problem. However, not every party can visualize the real dimension or even be able to fight against the problem, since they may have a limited and narrow scope. We name the ISPs as the problem owner because they have a wider scope of the problem and they get direct consequences against their business model when a botnet evolves and propagate within their network.

II. What relevant differences in security performance does your metric reveal?

In this section we analize the output of the metrics proposed in [**?**]. Based on this output we compare the performance of the distinct Autonomos Systems (AS) 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 China.

A. BN propagation

It measures the number new IPs where the BNI attempts are being performed. It is useful to see the aggregate growth of the BN, and to help to infer a BNI rate. This metric can be used to measure the evolution of the botnet in side a network. Since each ISP know the number of clients this metric can be normalized using this value. If an external party would like to compute and compare its perfromance using this metric, the normalization can be performed using the number of IP available addresses.

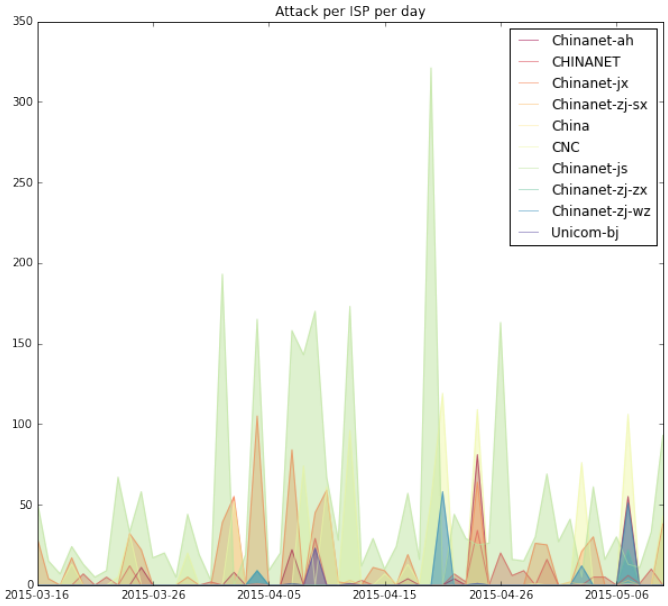
B. BNI attempts

It measures the number of attacks executed daily. We will use this data to analyze the BN activity. This metric could be useful to measure the effectiveness of mitigating controls. To analyze the security performance of the problem owner, we compare the activity comming from ISP networks and the activity comming from other service providers such as cloud providers and hosting providers. As we can see in figure 2 the majority of the activity is comming form ASs which belongs several ISP, however, as we can see in the before mentioned figure, the service providers also are suffering a misuse of their resourses.

In figure 1 we show the attemts to infect the ellastichoney honeypot that are coming form the top 10 most active AS that belong to ISPs.As we see the more infected ISP is Chinanet but within its network the AS called Chinanet-js, located in the province of Zhejiang. This metric is aimed to be used by the problem owners, since further normalization is needed to get more accurate information, i.e. the market penetration per ISP per region.

C. Network infection radio

Fig. 1: Attacks per day in diferent AS of the ISPs



D. BN geographical and digital location

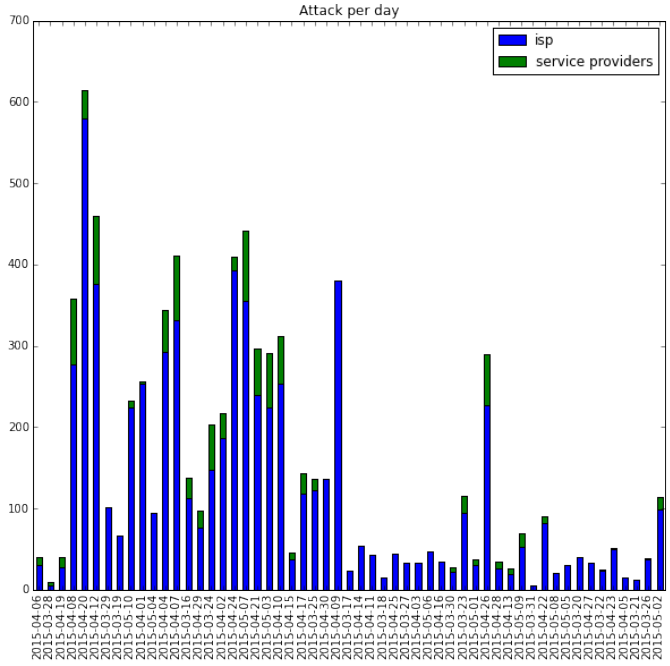
III. What risk strategies can the problem owner follow to reduce the security issue as measured in your first assignment?

In this section we describe possible risk strategies that the ISP can follow in order to reduce the security impact of botnet evolution.

a) To work with Industry and other stakeholders on developing a policy to implement:

b) Defense against attack by Bot: Security must be built-in during each phase of the system development and this can be done by using Intrusion Prevention System (IPS), Transport Layer Security (TLS)/Secure Sockets Layer (SSL) protocol and Correct coding of Web service/applications (without security flaws which makes it resistant to threats) [1].

Fig. 2: Activity coming from ISPs and other service providers



c) Monitoring, detection and studying of Bot: All users of computers and the system administrators should detect presence and/or activities of Botnet and prevent it from influencing upon the computers by constant following of the activities on the computers such as monitoring log files, detecting threats and finding counter measures [1].

- a registration component
- an awareness-raising component
- guidance on network management
- high-level advice on how to respond to threats
- a reporting component

Attempting to instruct users about how to shield themselves from installing malware and inadvertently transforming their PCs into bots is a key component to raise the level of security awareness [1].

d) To develop legislative punisment policy: 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 (legislative measures) along with legislative-punishment body to prevent the attackers from trying to carry the attacks [1].

Policy makers and ISPs must consider how best to implement authentication mechanisms that encourage reliable communications between ISPs, consumers and other actors.

e) The Addressing Layer: This involves strategies targeting the routing and the addressing layer of a botnet infrastructure. Bots in the local network cannot contact the original C&C server when intervened in addressing which usually take place in two steps.

In the first step, a site administrator can control the local DNS resolver(which handles the DNS requests forwards the request to an authoritative DNS server) and instruct to return a specially crafted response to specific queries. In the next step, local routers can be equipped with routing table entries to sinkhole certain addresses or redirect them to different hosts [**?**].

f) The Command Layer: This involves attacking the command layer of a botnet with the knowledge of the protocol used. An easy example would be an IRC-based network where a command like remove can instruct bots to uninstall themselves from infected systems [**?**].

g) Exploitation: Exploit based strategies make use of presence of bugs and programming flaws in bots that result in vulnerabilities which can be exploited to gain control either over a central component or over infected machines. An examples of such vulnerabilities would be security holes in software or remotely-exploitable buffer overflows [**?**].

IV. What other actors can influence the security issue as measured in your first assignment?

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

Vendors of Operating Systems / Softwares

V. Identify the risk strategies that the actors can adopt to tackle the problem

Government / Intelligence Agencies Ban Badware websites Effective Antispam and Cybercrime Laws and Regulation Dedicated laws on cybercrime Adapted to the paperless and cross-border nature of Internet crime Cross border jurisdiction established using a “country link” concept Capacity Building among relevant policy stakeholders Framework for local enforcement of Cybercrime and Botnet Mitigation Development of watch, warning and incident response centres Broad based education initiatives on Internet safety and security Facilitation of secure ICT access for users Capacity Building for Policy Stakeholders Framework for Efficient Cross Border Enforcement in Cybercrime Prosecutions Automated Detection and Reporting of Botnet Hosts Network Telescopes - Darknets and Flow Based Analysis Collection and Analysis of Anonymized Server Log Files from Participating ISPs

High Level Domain owners Registrar Detection and takedown of malware or botnet domains Phish tracking and repository sites such as Netcraft and Phishtank Trusted block lists such as Spamhaus and CBL Identification of IP Space Controlled by an ISP: Whois and Rwhois Records Real Time Feeds of DNS Block Lists that Target Malware Activity Fast

Flux Hosting and Rock Phishing Whois Privacy and Domain Takedowns

Others Capacity building for e-commerce and online transaction providers Network Telescopes - Darknets and Flow Based Analysis

VI. Pick one of the risk strategies identified previously and calculate the Return on Security Investment (ROSI) for that particular strategy

References

[1] S. Stankovic and D. Simic, "Defense strategies against modern botnets," *arXiv preprint arXiv:0906.3768*, 2009.