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.

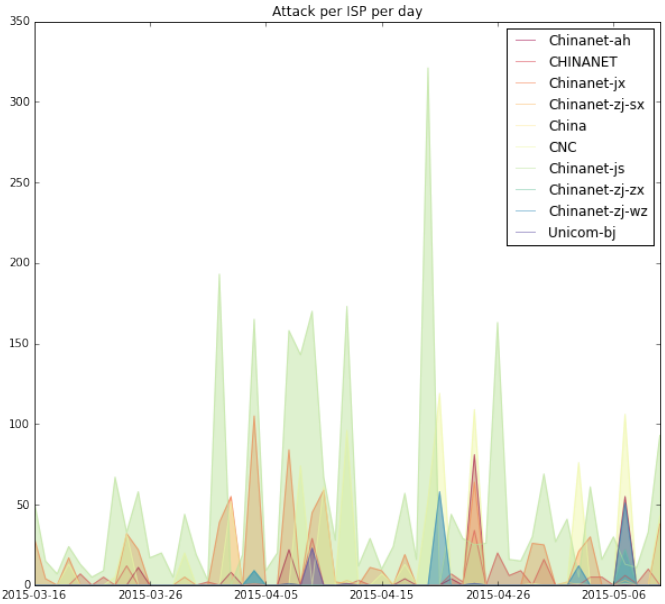
B. BNI attempts

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



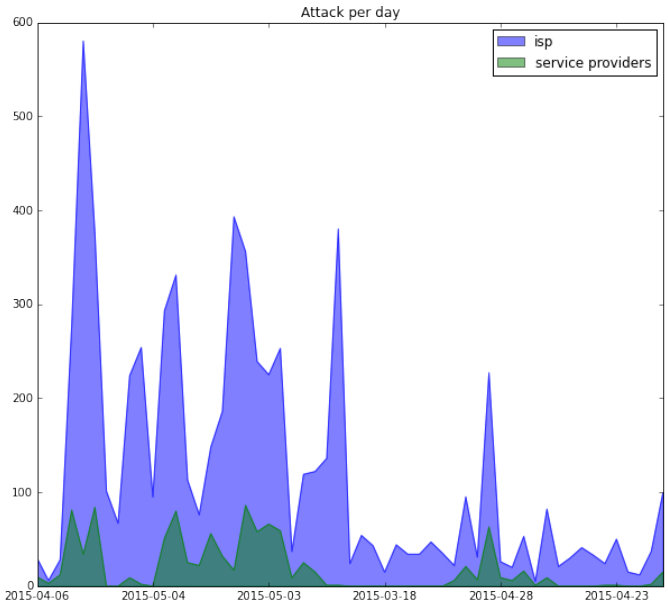
D. BN geographical and digital location

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

a) To have the connection between Command & Control server and its bots disconnected: ISPs should make sure that bots in the local network will not be able to contact the original C&C server. This can be done by intervening the 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 [**?**].

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



b) To have effective countermeasures(to fight botnets) on the infrastructure level: ISPs should make use of the knowledge of the protocol which can be used to attack the command layer of a botnet .

An easy example would be an IRC-based network where a command like remove can instruct bots to uninstall themselves from infected systems. [**?**].

c) To take the botnet down using the inherent flaws in botnet: ISPs can 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. This is aid in bringing the botnet down. An examples of such vulnerabilities would be security holes in software or remotely-exploitable buffer overflows [**?**].

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

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

e) To build an anti-bot friendly network: Security can 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].

f) To learn from the activities of the bot to predict its actions: 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].

g) To develop legislative punishment 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.

h) 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 [**?**].

i) 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 [**?**].

j) 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 [**?**].

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

l) 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 [**?**].

m)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 to raise the level of security awareness [**?**].

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

o) Financial help 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 [**?**].

OECD (2012), "Proactive Policy Measures by Internet Service Providers against Botnets", OECD Digital Economy

Papers, No. 199, OECD Publishing

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

Vendors of operating systems should provide tools that provide on-demand and real-time scanning of systems to help remove viruses, spyware, and other malicious software. These valuable applications should be bundled with the operating systems as part of the effort to mitigate the risks from botnet infection attempts. They cannot be a complete replacement to antivirus and antispyware applications used that scan and monitor known viruses and spyware, however they can be a vital resource to provide ongoing protection from a trusted source. An effective and up-to-date software firewall at the OS level can be an effective protection barrier between the users system and the Internet. OS Vendors should provide a sandbox environment to run unverified programs that may contain malicious code downloaded from unverified solution providers, untrusted users and untrusted websites. Software providers that provide email, social networking and instant messaging facilities should enforce strong filtering of content and attachments to mitigate the risk of botnet infections delivering malware that are presumed to be pictures or movies by the end users. Users should be limited to restricted access to applications and OS features, unless all security settings are hardened and the systems are patched with the most current updates.

Domain registrars can be effective against blocking compromised domains for hosting phishing sites, command and control servers, poisoned and malware delivery sites. To establish every network connection to a particular host, computers have to preform DNS lookup. Domain registrars can use methods such as packet filtering to filter traffic towards banned IPs by blocking access to certain servers from a list of banned or suspected bad domains. Attackers abuse the DNS system to avoid detection by using devious tricks such as fast-flux. In the fast-flux technique, bots continuously register and deregister their IP addresses for a particular domain. Each request by a user to access a malicious site will result in accessing a different bot and possibly different ISP. The only option to combat fast-flux is for the registrar to suspend the bad domain, which has its own positive and negative incentives in doing so. Another proactive approach that registrars can adopt is automated abuse handling and actively responding to external domain suspension requests from financial service providers and other authentic sources of information like intelligence agencies and ISPs.

Most major vendors like Microsoft are providing free tools to remediate the effects of botnet infections, and help users to combat against cyber criminals for their online privacy and security. However, there is a need for more user awareness for better protection and prevention from botnet infections. With ever growing incentives and motives behind spreading infections to run large networks of distributed botnets, the techniques and technologies are changing rapidly with time. Vendors of security services such as antivirus solution providers should put more effort on research and develop solutions to detect, prevent and mitigate the impact of botnet infections. Although the existing practices, tools and techniques to mitigate botnet infections are being tackled to a greater extent compared to the past, however attackers are coming up with clever new ways of exploiting vulnerabilities to spread their networks via botnet infections. Many infections are quite hard to remove, as they may disable windows update, as well as block access to the websites and update servers of antivirus and security software vendors.

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.