Progress Report on the research project

Mohammad-Reza Memarian

December 4, 2014

1 DDOS Subtype selection

One of The uses of Botnets in large networks is to conduct DDOS attacks. Based on top cloud threat CSA report [1], DDOS is one of the prevalent threats to security of Cloud computing that is conducted by getting advantage of cloud computing on demand resources. On demand resources of cloud computing leads to abuse use of cloud services that is another cetegory of threats in cloud computing. DDOS attacks have various subcategories. SYN flood, Smurf, Ping of death, Reflected/spoofed attack are all subcategories of DDOS. The botnets that are used for conducting DDOS attacks are referenced as DosNet.

In [2], Verisign observerd DDOS trends in second quarter of 2014 which is April 1st to end of Jun. In the mentioned period, the notable observation results are in following: 41% of attacks were directed against IT services, cloud and SaaS verticals which show Cloud service providers are one of the primary attack targets. Also it is important to note multi-vector attacks are on rise. In other word, attackers tend to change their attack vectors continuosly by conducting sophisticated TCP and UDP floods. TCP and UDP floods are easy to conduct attacks with high impact on the victim. So attack may have more impact with smaller number of zombies in shorter time slot. The primary attack vector in 2nd qurter of 2014 was UDP flood by NTP reflection attack that generates a significant damage to victims such as online business services. The attacks that were observed were short in duration and high in intensity. Verisign predicted Amplification attacks using techniques such as DNS reflection, NTP or SNMP are becoming more prevalent.

In [3], Verisign observed DDOS trends in third quarter of 2014 which is July 1st to end of September. In the mentioned period, the notable observation results are in the following: UDP flood attack were still the prevalent attack vector. But apart from NTP, SSDP got to be the new protocol trend for UDP flood attacks too. But NTP reflection continued to form majority of UDP flood attacks. Also There is an increase in deploying Linux DDOS malware as critical and vital server systems are moslty deployed using linux systems.

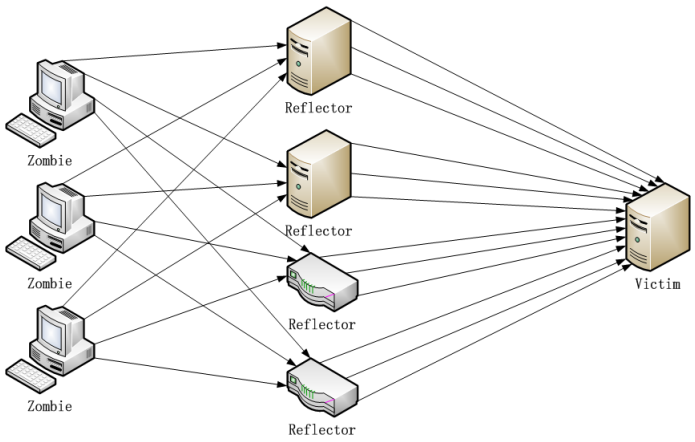

Figure 1: process of a reflection attack

1.1 Description of the attack

The NTP service supports a monitoring service that allows administrators to query the NTP server for traffic counts of connected clients. This information is provided via the monlist command. The basic attack technique consists of an attacker sending a get monlist request to a vulnerable NTP server, with the source address spoofed to be the victims address. The attack relies on the exploitation of the monlist feature of NTP, as described in CVE-2013-5211. The detail of the vulnerability is mentioneed in US National Vulnerability database [4] [5]. This command causes a list of the last 600 IP addresses connected to the NTP server to be sent to the victim that causes the victim to be overwhelm with unwanted legal traffic. Due to the spoofed source address, when the NTP server sends the response, it is sent instead to the victim. Because the size of the response is typically considerably larger than the request, the attacker is able to amplify the volume of traffic directed at the victim. Additionally, because the responses are legitimate data coming from valid servers, it is especially difficult to block these types of attacks. The primary solution is to disable monlist within the NTP server or to upgrade to the latest version of NTP (4.2.7) which disables the monlist functionality.

Protocols involved in amplification attack have bandwidth amplification factor. For example based on [6], SSDP has bandwidth amplification factor of 30.8 meaning that a search command on this protocol will return a response 30.8 times size of the request.

1.2 Attack map

Openstack is collection of open source projects working and collaborating together. Although on the same machine, but in a operational environments each

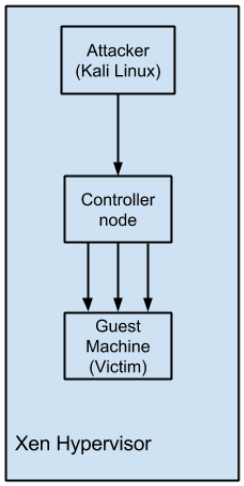

Figure 2: Designed attack map

of the projects should be configured separately. For the sake of simplifying configuration job for developers, Openstack contributers introduced a set of scripts called devstack that configures whole openstack projects together (controller node) on a Virtual machine. So development can be done easily on that VM. Controller node that hosts most of the openstack services, acts as the brain of the cloud platform. Local NTP service is offered by the controler node to the rest of the entites in the cloud. So in UDP flood attacks using NTP amplification, controller node acts as one of the amplifiers.

US-CERT (United states computer emergency readiness Team) has mentioned NTP amplification attacks in CVE-2013-5211 in [5]. All the NTP versions prior to 4.2.7 are vulnerable to this attack. NTP protocol is one of the protocols that do not receive update so much. And looking from administrative view, when it is configured, configuration is not reviewed so often. As We configured NTP server on the controller node, by default it installed NTP version 4.2.6 which is a vulnerable version.

2 Direction ahead and discussion

NTP reflection is only one of the UDP flood attacks on rise. Other protocols such as DNS and SSDP are frequently used in this kind of attacks too. But the negative point about NTP reflection is that NTP has the Highest Amplification factor compared to other protocols. So In scenarios that NTP is envolved,

Smaller Botnets are required that makes it ptorocol of choice. As mentioned earlier, botnets are moving toward being multipurpose and not just act in one direction. The proposed milestone to reach for days ahead in order are in following:

1- Finilize the attack to empower the Motivation: Working with Kali linux and Openstack is a bit complicated, So I am trying to get to know them as fast as possible as conduct the desired attack. I have done some DOS attacks from Kali to the victim shown in Figure 2 using spoofed IP of controller node, but I must do it with NTP reflection to say that this attack is also deployable in cloud context.
2- Target System Identification: In the attack scenario the zombies are Guest VMs, Reflectors are NTP and DNS servers and victim can be any VM either server or guest VM.
3- Symptom Determination: Identifying Malwares that are recently used to conduct NTP reflection attacks. There are for Malware which were announced in Symantec DDOS trend 2014 report. They were designed for DDOS attacks but I just must figure out which one was designed for NTP reflection attack and determine sysmtoms based on some official static analysis reports.
4- Determination of suitable Machine learning Algorithm: One of the strong points of our work can be usage of some machine learning algorithms in our work for high and correct detection rate that may not be found in typical existing systems.

References

[1] , "The notorious nine cloud computing top threats in 2013," Cloud Security Alliance, Tech. Rep., .

[2] ——, "Verisign distributed denial of service trents report, 2nd quarter 2014," Verisign, Tech. Rep., .

[3] ——, "Verisign distributed denial of service trends report, 3rd quarter 2014," Verisign, Tech. Rep., .

[4] ——. () Vulnerability summary for cve-2013-5211. [Online]. Available: http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2013-5211

[5] ——. () Ntp amplification attacks using cve-2013-5211. [Online]. Available: https://www.us-cert.gov/ncas/alerts/TA14-013A

[6] C. Rossow, "Amplification hell: Revisiting network protocols for ddos abuse," in *NDSS 2014*.