# POSTER: Reflected Attacks Abusing Honeypots

Martin Husák
husakm@ics.muni.cz

Martin Vizváry
vizvary@ics.muni.cz

Masaryk University
Institute of Computer Science
Botanická 554/68a, 602 00 Brno, Czech Republic

## ABSTRACT

We present the observation of distributed denial-of-service attacks that use reflection of the flooding traffic off reflectors. This type of attack was used in massive attacks against internet infrastructure of Czech Republic in March, 2013. Apart from common hosts in the network, honeypots were abused as the reflectors. It caused the false positive incident detection and helped attackers. Honeypots, which are by default set to accept any incoming network connection, unintentionally amplified the effect of reflection. We present an analysis of the attack from the point of view of honeypots and show the risks of having honeypots respond to any incoming traffic. We also discuss the possibilities of attack detection and mitigation and present lessons learned from handling the attack. We point out a lack of communication and data sharing during the observed attack.

## Categories and Subject Descriptors

C.2.0 [**Computer-communication Networks**]: General—*Security and protection*

## Keywords

DDoS attack; reflection; honeypot; mitigation; data sharing; communication

## 1. INTRODUCTION

Denial-of-service attacks are a major threat to today's networks. They are relatively easy to perform, hard to defend against, and the attacker is rarely traced back due to common usage of IP spoofing techniques and a distributed form of the attack.

The Distributed Reflected Denial-of-Service (DRDoS) attacks do not contact the victim directly, they rather spoof source IP address of the victim and use bouncing of traffic off reflectors instead. The spoofing of victims' IP address causes the reflectors to appear as the attackers while the real attacker is often above suspicion. Reflectors do not need to amplify an attack, response with the same or even smaller amount of data is sufficient for a successful attack. In addition, any host in the network can be abused as a reflector, i. e., server, workstation or honeypot.

We have observed a situation where honeypots unintentionally helped the attacker. Honeypots, by their nature, are not meant to be accessed by legitimate users. If a network traffic of a honeypot is monitored and a honeypot is abused as a reflector, we can see an attempt to contact it and mark the source IP as a potential attacker. This is natural and legitimate procedure of malicious behavior detection but, in case of DRDoS, we have marked spoofed address as an attacker. Even though any network traffic destined to honeypot is suspicious, we cannot be sure if we have detected the real attacker or a victim.

The involvement of honeypots in DRDoS is often ignored, as we have observed in several attacks recently. To name a few, abuse of honeypots was associated with the massive DDoS attacks against Czech Republic in March, 2013. Another example of this type of attack was an incident from April, 2013, when we detected an IP address, which was part of a DDoS mitigation service. In both cases, the actual victim was reported and as an attacker initiating unsolicited connections to honeypots.

This paper is organized in six sections. We recount the recent DDoS attacks and the role of honeypots in them in Section 2. We point out the importance of proper configuration of honeypots to eliminate the reflection in Section 3. The possibilities of detection and mitigation of the attacks and handling issues for which organizations should be prepared are described in Section 4 and 5. The paper is concluded in Section 6.

## 2. DDOS ATTACKS AGAINST CZECH REPUBLIC

In March 2013, Czech Republic was a target of DDoS attacks which lasted 4 consecutive days. It was the first time the entire country had to face an attack of this volume. Online media, banks and mobile operators were gradually under DDoS attacks from Monday, March 4 to Thursday, March 7 in working hours between 8 AM and 5 PM (CET). The attacker used two types of DDoS attack with volume up to 1 Gbps [1] and initiated the attack with the knowledge of the Czech internet. The reason for the attack is unknown but it has shown how prepared the Czech community is for these attacks.

The attacks started with a SYN flood attack on Monday and Tuesday and were aimed against more than a dozen on-

line media virtually hosted on a few servers, and the most popular Czech search engine *Seznam.cz*. According to DDoS attacks taxonomy [5], it was a brute-force attack using randomly spoofed source IP addresses with fluctuating rate. Even though the attack was simple and the bandwidth was low, overload of the virtual hosting denied access to many web pages. We believe that the goal of these attacks was to attract the attention of media.

On Wednesday and Thursday the attack continued with reflected SYN flood attack. The attacks were aimed against websites of major Czech banks and two mobile operators. According to the taxonomy [5], it was a brute-force attack using fixed spoofed source IP address with fluctuating rate known as the DRDoS attack. As shown in Figure 1, it is a form of a DDoS attack that bounces the flooding traffic off of reflectors by spoofing requests from the victim to Internet hosts that will send replies to the victim [6]. These attacks are based on willingness of improperly configured servers and computers to respond to incoming packets. Reflected attacks due to their nature are harder to trace and filter. According to CESNET, the Czech NREN[1], 68 % connections on random destination port were accepted and responded to with SYN+ACK. It was approximately 1.5 million packets per 5 minutes.

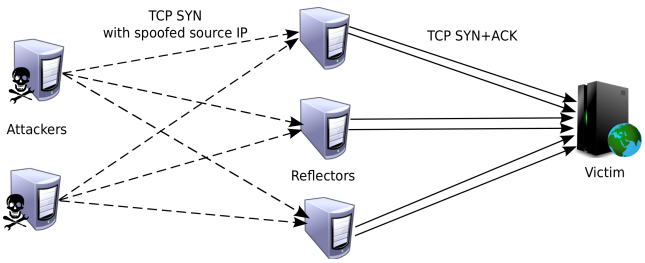


**Figure 1: Schema of the reflected attack**

Honeypots became great reflectors for the DRDoS attack. We observed that honeypots from another Czech university reflected 93 % of all incoming packets. Hosts in the network of Masaryk University reflected approximately 5 % of incoming packets while honeypots alone reflected 16 % of incoming packets. Figure 2 shows a traffic peak from honeypots that was stopped shortly after the false positive detection and filtering of the actual victim.

## 3. HONEYPOT SETTINGS AND VULNERABILITIES

Traditionally, there are two approaches to honeypot implementation, high-interaction and low-interaction honeypots [2]. These implementations differ in a level of possible interaction between a honeypot and an attacker. High-interaction honeypots are usually deployed as the virtual machines with a real operating system and applications. They do not differ from the real hosts on the network and they are not often deployed in large numbers. The low-interaction honeypots are usually emulators of systems or their parts. The settings of these honeypots are limited as well as the possible countermeasures while they are cheap to deploy and often deployed in large numbers.

[1]National Research and Education Network

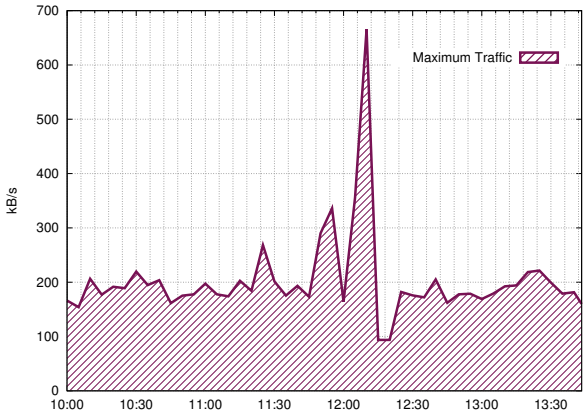


**Figure 2: Incoming and outgoing TCP traffic on honeypots – Thursday, March 7, 2013 from 10 AM to 2 PM**

There are popular tools among the honeypot community, a low-interaction honeypot *honeyd* [7] and a tarpit *LaBrea* [4]. Honeyd is a small daemon that creates virtual hosts in the network. There are two potential vulnerabilities in its deployment, the number of emulated hosts and settings of their port actions. Any port on any host (including defaults) emulated by honeyd can be set in three ways, 1) *open* responds with TCP SYN+ACK packet, 2) *reset* responds with TCP RST packet and 3) *block* is not responding. Honeypots are generally configured to accept any incoming connection, e. g., *open*, to capture potential attacks including zero-day exploits. The problem is that honeypots accept and respond also to spoofed packets. The ports open by default are the reason why honeypots reflect more traffic than common hosts in the network. Next, tarpits like LaBrea include additional potentially hazardous ability. They establish a TCP connection and keep it open for as long as possible without sending much data. This ability is supposed to deplete the resources of an attacker. However, in case of reflected attack the tarpit is actually depleting the resources of the victim.

The risk of having all ports opened is multiplied by the number of emulated hosts. For example, honeyd can emulate up to 65,536 addresses. As for our own honeypots, we use honeyd emulating slightly more than 200 IP addresses. Even this number of emulated hosts would be enough for the attacker to execute DRDoS attack. The only limitation of the reflected traffic is bandwidth of a singe host running the honeyd.

The attacker does not need to know if the reflectors are common hosts or honeypots. It can be a coincidence to abuse honeypots as reflectors, although favorable for the attacker.

The easy abuse of honeypots can be turned into honeypot detection mechanism. Scanning for highly responsive network segments reveals good reflectors that are likely to be honeypots, especially when they reply with the SYN+ACK flags on many unusual ports. Suppressing this behavior corresponds with the strategy of making honeypots indistinguishable from common network hosts [2].

# 4. DETECTION AND MITIGATION OF THE ATTACKS

The DRDoS attack is based on IP spoofing and if we could detect spoofed IP packets, we would be able recognize an attack. Elimination of IP spoofing would make DRDoS attacks impossible and would enable defense mechanisms against many other kinds of DDoS attacks [5]. The BCP38 [3] deals with network ingress filtering that disables sending of forged traffic with a spoofed source IP address. Since the filtering is still not always put in place we have to rely on a research in source address validation.

Once we have detected an attack reflected of our network, we can mitigate the attack at least by dropping the connections from and to the victim. Next step should be sending a report of reflected traffic to the abuse contact of the victim with data pointing to the source of the spoofed traffic on uplink level ISP. This informs the victim that we act as a reflector and not the actual source of attack and gives enough information to trace the actual attacker.

It is worth noting that attackers rather succeed in saturation of the link or active nodes such as firewalls, load balancers etc., than overloading the end server. The port is irrelevant when it comes to link saturation, however the port 80 is more likely to be accepted by firewalls. This port is not the only option, well-known ports are most likely to be used.

# 5. COMMUNICATION AND DATA SHARING

Significant part of the mitigation of attacks is based on communication and sharing of data between organizations involved in a DDoS attack. As it turned out from recent attacks, researchers and security teams are focused mainly on detection of attacks and their processing in a local context. This approach is sufficient enough for attacks on small scale focused on one organization. However, attacks that go across several organizations, which could act as both victims and attackers, needs more than simple detection.

There is the best practice to use a list of official abuse emails and out-of-band contacts to eliminate the delay and a risk of losing contacts due to personal changes in organizations. Recent events in March showed lack of systematic communication between organizations which communicated mostly ad-hoc and based on good relations between the involved organizations. There were conference calls put in place and personal contacts were used.

Sharing of data is very closely related to communication. It helps tracing the source of attack and speeds up the analysis of attack. A shared database of detected anomalies and incidents could make the detection and mitigation of attacks faster and more accurate. Moreover every organization should have summarizing information about the status of own network, i. e. used bandwidth, count of open connections, etc. This could detect involvement in attack as reflector or botnet zombies. Every mitigated attack to the victim could lower the impact of attack, particularly if the bandwidth of the reflector is higher than victims'. The legislative adjusting the work and access to personal data and network records has to be taken into consideration, though.

There is also the need to usefully visualize the shared data gathered during an attack. Visualization is currently oriented simply on amount of traffic between nodes or subnets. It would be helpful to correlate the results of detection methods and visualize them on upper levels of network hierarchy. This could help to react faster to early warnings and changes in ongoing attack.

# 6. CONCLUSIONS

In this paper, we pointed out that there is a risk in using honeypots. However, we do not want to discourage readers to use them. We still see the benefit of honeypots being deployed in the network but we advice against them being as open as possible. Honeypots are still useful even for reflected traffic, because they point to malicious behavior, although in this particular case, they are reporting victim and not the attacker. We have shown that honeypots are capable of reporting false positives, although they were believed to be free of false positives.

We have supported our conclusions by the observation and analysis of real large-scale DRDoS attacks. Honeypot settings and vulnerabilities were presented on an example of widely-known low-interaction honeypots participating in the attack. We also discussed the problems related to incident handling and communication during the attack. Not only false positive detection, but overall information sharing needs to be revised to replace observed ad-hoc solutions.

Finally, we presented lessons learned in the area of both honeypots and attack handling, including prevention of honeypot abuse and proper handling of security incidents. We believe there is still room for improvement in communication and data sharing associated with mitigation of attacks.

# 7. REFERENCES


[1] P. Bašta. DDoS - lessons learned - technical aspects. `http://www.afcea.cz/img/clanky_next/ITTE/Basta_DDOS.pdf`, 2013.

[2] European Network and Information Security Agency (ENISA). Proactive Detection of Security Incidents II - Honeypots. `http://www.enisa.europa.eu/activities/cert/support/proactive-detection/proactive-detection-of-security-incidents-II-honeypots`, 2012.

[3] P. Ferguson and D. Senie. Network Ingress Filtering: Defeating Denial of Service Attacks which employ IP Source Address Spoofing. RFC 2827 (Best Current Practice), May 2000. Updated by RFC 3704.

[4] T. Liston. Welcome to My Tarpit: The Tactical and Strategic Use of LaBrea, 2001.

[5] J. Mirkovic and P. Reiher. A taxonomy of DDoS attack and DDoS defense mechanisms. *SIGCOMM Comput. Commun. Rev.*, 34(2):39–53, Apr. 2004.

[6] V. Paxson. An analysis of using reflectors for distributed denial-of-service attacks. *SIGCOMM Comput. Commun. Rev.*, 31(3):38–47, July 2001.

[7] N. Provos. A virtual honeypot framework. In *Proceedings of the 13th conference on USENIX Security Symposium - Volume 13*, SSYM'04, Berkeley, CA, USA, 2004. USENIX Association.