Reflected Attacks Abusing Honeypots

Martin Husák
Institute of Computer Science
Masaryk University
Brno, Czech Republic
husakm@ics.muni.cz

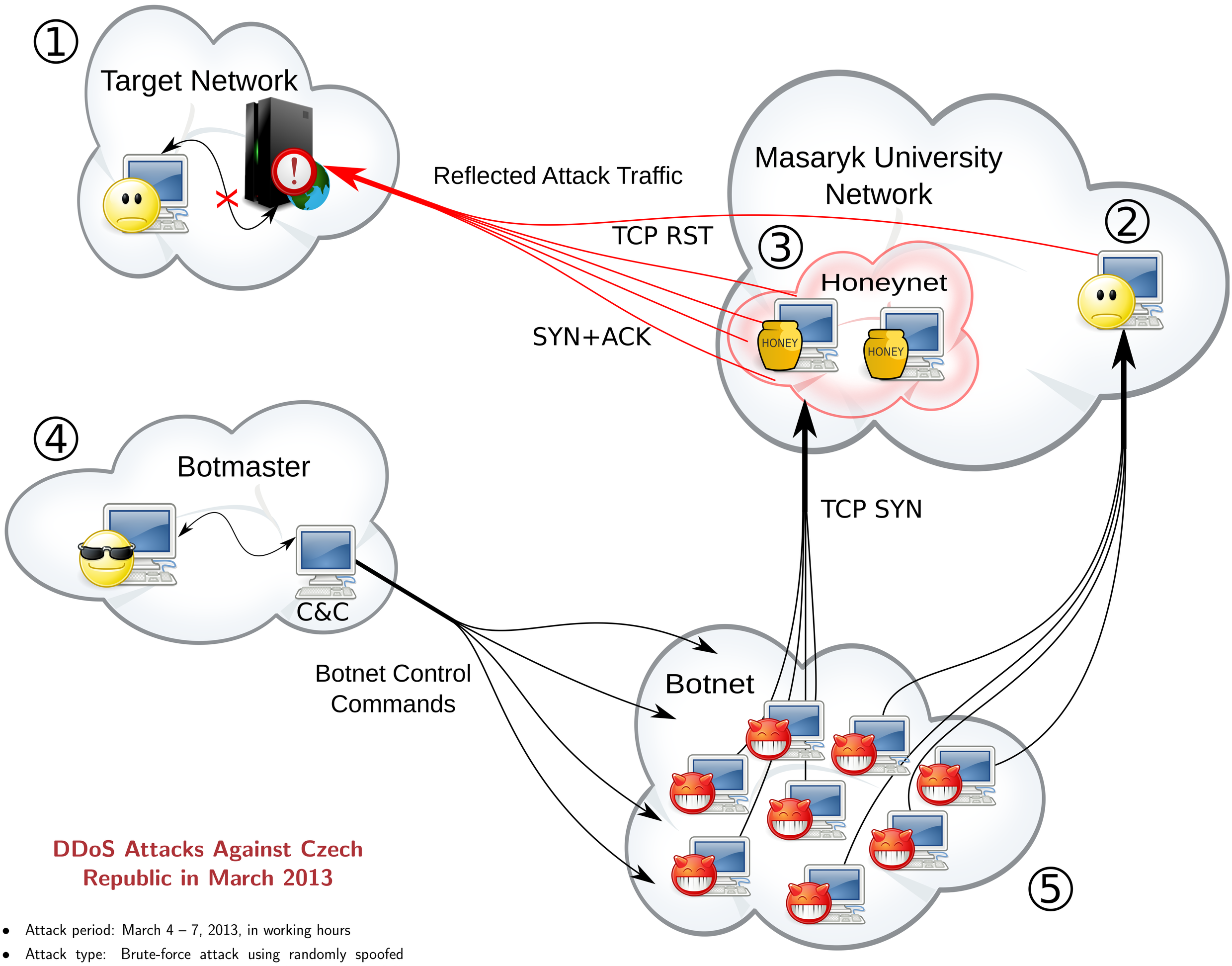
Martin Vizváry
Institute of Computer Science
Masaryk University
Brno, Czech Republic
vizvary@ics.muni.cz

We present the observation of a distributed reflected denial-of-service attack abusing honeypots as reflectors. This type of attack was observed during massive attacks against internet infrastructure of Czech Republic in March, 2013.

Explanatory notes to the attack schema:

1. Target network is under attack! The flooding traffic is reflected so the victim suspects the random network hosts that were abused as reflectors while the attacker is hiding.
2. Random hosts are abused as reflectors to bounce off the flooding traffic.
3. Honeypots are abused as reflectors too, but due to their settings they respond to any incoming packet and reflects almost all the flooding traffic.

   Possible response to incoming SYN packet is to drop it or respond with either SYN+ACK or RST. Honeypots are most likely to respond with SYN+ACK on any port to attract the attackers.
4. Attacker controls the botnet and sends commands to start the attack.
5. Botnet is a network of zombies controled by the attacker that generates the flooding traffic.



DDoS Attacks Against Czech Republic in March 2013

- Attack period: March 4 – 7, 2013, in working hours
- Attack type: Brute-force attack using randomly spoofed source IP address with fluctuating rate (see taxonomy [2]) with volume up to 1 Gbps [1]
- SYN flood attack on Monday and Tuesday
- Reflected SYN flood attack on Wednesday and Thursday
- CESNET, the Czech NREN, recorded high number of accepted TCP connections on random ports
- $\mathbf{68\,\%}$ of connections (approximately 1.5 million packets per 5 minutes) were accepted and responded to with SYN+ACK
- Hosts in the network of Masaryk University (including honeypots) reflected approximately $\mathbf{5\,\%}$ of incoming packets
- Honeypots in the network of Masaryk University reflected $\mathbf{16\,\%}$ of incoming packets
- Honeypots from another Czech university reflected $\mathbf{93\,\%}$ of incoming packets

Conclusions

There is a risk in using honeypots. We still see the benefits of deploying honeypots but we advice against them being as open as possible.

Honeypots are capable of reporting false positives although they were believed to be free of it.

We present lessons learned in area of both honeypots and handling of security incidents.

Our conclusions are supported by the observation and analysis of real high-scale reflected DDoS attacks.

Overall information sharing needs to be revised to replace observed ad-hoc solutions.

There is still room for improvement in communication and data sharing associated with mitigation of attacks.

Acknowledgements

This work has been supported by the project "Cybernetic Proving Ground" (VG20132015103) funded by the Ministry of the Interior of the Czech Republic.

References

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

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