17.02.2017, Wroclaw

Scientific Report: Short Term Scientific Mission in COST Action CA5127 RECODIS

1. STSM Details

STSM Title: Coordinated botnet attacks on critical network nodes

STSM Applicant: Wojciech Kmiecik

Home Institution: Wroclaw University of Science and Technology, Faculty of Electronics, Department of Systems and Computer Networks

Host Institution: Budapest University of Technology and Economics

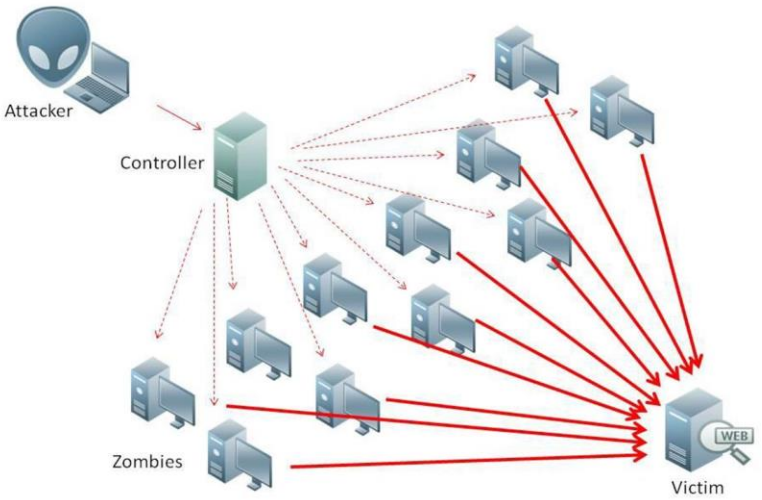
STSM Host: Dr. János Tapolcai

Period: 2017-02-03 to 2017-02-10

Working group: WG4

2. Purpose of the STSM

Communication networks, especially the Internet, once it became essential for everyday life for billions of people, also emerge more and more as the favorite attackers' land to launch a broad variety of threats. One of the most dangerous attacks is Denial-of-Service (DoS), a kind of volumetric attack where the target destination is overwhelmed by a huge number of requests, which eventually lead to the impossibility of serving any of the users. In its most powerful variant, the Distributed DoS (DDoS), such requests are produced in parallel by a botnet, a large net of robots acting cooperatively under the supervision of a botmaster. The bots may be either malicious users acting consciously, or legitimate users that have been preliminarily infected, (e.g., by warms and/or Trojans). [1] A different type of botnet attack is a distributed reflected denial of service attack (DRDoS), which involves sending forged requests of some type to a very large number of computers that will reply to the requests. Using Internet protocol spoofing, the source address is set to that of the targeted victim, which means all the replies will go to (and flood) the target.



Source: http://www.helpsec.net

Botnets attacks are now one of the biggest threats in the global network, especially given the fact that they can lead to huge revenue losses. *Dyn* (a company that controls much of the internet's domain name system DNS infrastructure) estimated that the attack that took place on October 2016 had involved '100,000 malicious endpoints', and the company said there had been reports of an extraordinary attack strength of 1.2 terabits (1,200 gigabytes) per second. The company was hit on 21 October and remained under sustained assault for most of the day, bringing down sites including Twitter, the Guardian, Netflix, Reddit, CNN and many others in Europe and the US [2]. Another example of huge revenue losses is the Avalanche network that was used as a delivery platform to launch and manage mass global malware attacks and money mule recruiting campaigns. It has caused an estimated EUR 6 million in damages in concentrated cyberattacks on online banking systems in Germany alone. The monetary losses are estimated to be in the hundreds of millions of euros worldwide. The international counter-cybercrime operation marks the largest-ever use of sink-holing to combat botnet infrastructures and was unprecedented in its scale, with over 800 000 domains seized, sinkholed or blocked [3].

Nowadays, botnets are used to attack mostly servers or websites of well-known companies in order to extort money (to stop the attack). Another potential targets of the botnets attacks are vital network nodes. In July 2016, Citibank employee knowingly transmitted a code and command to 10 core Citibank Global Control Center routers, and by transmitting that code, erased the running configuration files in nine of the routers, resulting in a loss of connectivity to approximately 90 percent of all Citibank networks across North America. That led not only to huge loss of clients trust but also millions of dollars [4].

The first goal of the STSM was to investigate topic of coordinated botnet attacks on critical network nodes and consult my ideas with János Tapolcai and his group. I believe the STSM gave me unique insight into the problem thanks to his experience in survivability and failure localization. Moreover, the topic of my STSM is placed within scope of the Working Group 4 of the COST RECODIS (Malicious human activities) and after finishing my work it will contribute to the objective of the WG4 – "to provide, e.g., new routing algorithms and link cost metrics (with the objective to decrease the vulnerability of important flows to attack-based disruptions), as well as methodologies of network topology update to decrease the topological vulnerability of networks to attacks.”.

The second goal of this STSM was to make new collaborations with researchers from Budapest University of Technology and Economics. Since I am a young postdoctoral researcher, making new connections and starting new collaborations is crucial for me as a researcher.

3. Description of the work carried out during the STSM

During the STSM, a visit to Dr. János Tapolcai’s Department of Telecommunications and Media Informatics, Faculty of Electrical Engineering and Informatics, Budapest University of Technology and Economics was conducted. I got to meet Dr. Tapolcai’s research team and give short presentation about my STSM entitled “Coordinated botnet attacks on critical network node”. Then, several topics related to my STSM subject were discussed. We narrowed them down to three main topics/questions:

- What are limitation of a hardware router in backbone network? Is it possible to take down node/router with a specific DDoS or other type of botnet attack?
- Are there any protection/restoration methods already in place by Telekom companies?
- If hardware routers are immune to all kinds of attacks, we should shift our focus to SDN routers and networks.

Besides the talks, I have studied thoroughly the subject of botnets, botnets attack and how to detect them and defend from them. It was crucial for me to better understand a subject that is new for me. A number of papers with important knowledge were identified and will be discussed in upcoming conference paper [5],[6],[7],[8].

Moreover, just after my STSM, I was able to give a presentation on my STSM topic during 3rd COST RECODIS MC/WG Meeting in Wroclaw, PL. That resulted in some great comments and remarks from the members of the WG4. As a result I will be consulting my ideas with Artemios Voyiatzis from Vienna. Olso, I’ve received contact to Matthias Gunkel from Deutsche Telekom and hopefully he will be able to answer my questions about hardware routers in the backbone.

4. Description of the main results obtained

Main results obtained during my STSM are as follows:

- A start of a collaboration between Dr. János Tapolcai’s research group and myself,
- Thorough state of the art literature study related to botnet and attacks,
- Presentation of my STSM topic where I could present my ideas,
- Discussion on the problem of protecting network from coordinated botnet attacks on critical network nodes which led to important questions that need to be answer before going forward with the conference paper,
- formulation of a working plan towards a conference paper.

Moreover, key findings/observations after my discussion with Dr. János Tapolcai and his research team are as follows:

- proposed research topic is relevant to WG4 and worthy following,
- even if hardware backbone routers can't be used in our research, this topic would be interesting to follow in the context of Software-Defined Networking,
- introducing new algorithms/methodologies for backbone/SDN networks taking into account possibility of the coordinated DDoS attack onto important network nodes is an important and up-to-date research topic

5. Publications/articles resulting from the STSM

I would like to continue a collaboration with Dr. János Tapolcai and his research team. First result of this collaboration will be a conference paper in RNDM, DCRN or other conference about resilient networks design and modeling. The paper will deal with problem of coordinated botnet attacks on critical network nodes and will propose new algorithms/metrics aiming to increase network survivability to such attacks.

References

[1] V. Matta, M. Di Mauro and M. Longo, "Botnet identification in randomized DDoS attacks," 2016 24th European Signal Processing Conference (EUSIPCO), Budapest, 2016, pp. 2260-2264.

[2] https://www.theguardian.com/technology/2016/oct/26/ddos-attack-dyn-mirai-botnetw.theguardian.com/technology/2016/oct/26/ddos-attack-dyn-mirai-botnet

[3]https://www.europol.europa.eu/newsroom/news/%E2%80%98avalanche%E2%80%99-network-dismantled-in-international-cyber-operation

[4] https://www.tripwire.com/state-of-security/featured/citibank-it-guy-deliberately-wiped-routers-shut-down-90-of-firms-networks-across-america/

[5] L. Zhang, S. Yu, D. Wu and P. Watters, "A Survey on Latest Botnet Attack and Defense," 2011IEEE 10th International Conference on Trust, Security and Privacy in Computing and Communications, Changsha, 2011, pp. 53-60.

[6] E. Stinson and J.C.Mitchell. "Towards systematic evaluation of the evadability of bot/botnet detection methods", Proceedings of the 2nd conference on USENIX Workshop on offensive technologies (WOOT'08). USENIX Association, Berkeley, CA, USA.

[7] C. Li, W. Jiang and X. Zou, "Botnet: Survey and Case Study," 2009 Fourth International Conference on Innovative Computing, Information and Control (ICICIC), Kaohsiung, 2009, pp. 1184-1187.

[8] P. Wang, S. Sparks and C. C. Zou, "An Advanced Hybrid Peer-to-Peer Botnet," in IEEE Transactions on Dependable and Secure Computing, vol. 7, no. 2, pp. 113-127, April-June 2010.