Zombie alert: assessing legitimacy of P2P botnet mitigation techniques

Karine e Silva[1] and Ruben Roex[2]

Background

Albeit dating from 1999[3], the cyber threat known as botnets has successfully adapted against countermeasures and ranked once again among the top cybersecurity concerns last year.[4] According to the explanatory memorandum of the Directive on attacks against information systems, botnets are "*networks of computers that have been infected by malicious software*". The combined power of all the individual infected computers (also known as zombies) through dedicated or dispersed command and control (C&C) structures is used by perpetrators to *inter alia* send out spam or execute distributed denial of service (DDoS) attacks.

While the threat has been recognised by most key stakeholders, botnet takedowns remain a very considerable challenge. Botmasters operate on a global scale, while government officials and even private companies need to pay due regard to jurisdiction issues. Furthermore, botnet technologies appear to evolve rapidly into structures that are very persistent and thus hard to disrupt. They are now increasingly decentralized networks operating via peer-to-peer (P2P) technologies,[5] where the C&C is spread among compromised machines. Because P2P bots do not receive orders from a singular C&C, but rather from other distributed bots, the botmaster may not be individually targeted or identified[6]. The change from central C&Cs to P2P fluid architecture without single point of failure strengthened botnet resilience and stability[7] against takedown and disruption attempts, while making detection even harder[8]. Contrary to what its name suggests, this advanced form of botnet is growing outside the limits of P2P networks and combining other infection means[9] such as email, mobile communications and cloud computing to recruit zombies. Only just recently a consortium consisting of Microsoft, Europol (EC3) and the FBI tried to take down the widely-spread ZeroAccess botnet[10], but were only partially successful.

---

[1] Legal Researcher at the Belgian Cybercrime Centre of Excellence for Training, Research and Education (B-CCENTRE), Interdisciplinary Research for Law and ICT (ICRI), KU Leuven, iMinds.
[2] Legal Researcher at the Belgian Cybercrime Centre of Excellence for Training, Research and Education (B-CCENTRE), Interdisciplinary Research for Law and ICT (ICRI), KU Leuven, iMinds
[3] Jan Gassen, Elmar Gerhards-Padilla and Peter Martini, Botnets: How to Fight the Ever-Growing Threat on a Technical Level, Springer, 2013, p. 49.
[4] European Network and Information Security Agency (ENISA), Threat Landscape 2013: Overview of current and emerging cyber-threats, 2013. Retrieved from http://www.enisa.europa.eu/activities/risk-management/evolving-threat-environment/enisa-threat-landscape-2013-overview-of-current-and-emerging-cyber-threats/at_download/fullReport
[5] Jan Gassen, Elmar Gerhards-Padilla and Peter Martini, op. cit., p. 56.
[6] Ibid.
[7] European Network and Information Security Agency (ENISA), Threat Landscape: Responding to the Evolving Threat Environment, 2014, p. 16. Retrieved from http://www.enisa.europa.eu/activities/risk-management/evolving-threat-environment/ENISA_Threat_Landscape
[8] European Network and Information Security Agency (ENISA), Threat Landscape 2013, op. cit., p. 20.
[9] Ping Wang et al., A Systematic Study on Peer-to-Peer Botnets, p. 2
[10] Microsoft, the FBI, Europol and industry partners disrupt the notorious ZeroAccess botnet, Microsoft News Center, December 5, 2013, Retrieved from http://www.microsoft.com/en-us/news/press/2013/dec13/12-05zeroaccessbotnetpr.aspx

The case did demonstrate, however, how international cooperation between law enforcement authorities and private actors is crucial in the takedown of botnets.

To fight this emerging threat, specific mitigation tools have been studied and deployed by security experts. These include index poisoning[11], Sybil-attacks[12], bare-metal[13], crawling[14]. Apart from the examination of the efficiency of such tools, law enforcement authorities (LEAs) and their private sector partners are faced with the challenge of whether these are legitimate means to gather intelligence about botnets and disrupt their operations.

Research aim, questions and methodology

The rise of P2P botnets and the need for effective countermeasures has revealed a lack of legal backing in the use of mitigation techniques. We aim to bridge this gap by examining whether popular P2P botnet mitigation tools classify as legitimate means to fight cybercrime in light of the applicable European framework.

From a legal perspective, the first questions arise with regard to data protection law. The zombie state is often unknown to the user of the machine and mitigation techniques operated by private actors are likely to interfere with their private communications as well as to access personal information and other types of protected data. In fact, the operations envisioned by many anti-cybercrime tools fall within the scope of the Data Protection Directive and e-Privacy Directive. In this context, we will be looking at the information flows, categories of processed data and legitimating grounds used by private sector in their fight against botnets. To this end, selected anti-botnet solutions will be scrutinized under the European data protection framework, implementing national laws, and related jurisprudence.

Additional questions are brought from a criminal procedural law point of view, as it is rather unclear whether gathering evidence through such tools will be upheld in court. From this angle, our research will focus on the question of how law enforcement authorities can access, search and seize material possibly to be used as evidence in ensuing legal proceedings. Starting out from the relevant provisions in the Council of Europe Convention on Cybercrime and the recently introduced Directive on attacks against information systems, we will look particularly into the national powers for LEAs to access, search and seize to see whether they are up to task of dealing with botnet takedown techniques.

To answer all these questions, we have narrowed our analysis down to selected countries, namely Belgium, the UK, the Netherlands and Spain. While the first have granted far-reaching investigative powers to their law enforcement agents for tackling cybercrime, the Netherlands has undertaken significant efforts to fight botnets by creating a specialised high-tech police unit and participated in the prosecution of the ZeroAcess botnet disruption. Furthermore, the latter jurisdiction has recently

[11] Ping Wang et al., op. cit., p. 2.
[12] Jan Gassen, Elmar Gerhards-Padilla and Peter Martini, op. cit., p. 77.
[13] Brent ByungHoon Kang et al., Towards Complete Node Enumeration in a Peer-to-Peer Botnet, 2009, p. 3.
[14] Christian Rossow et al., SoK: P2PWNED — Modeling and Evaluating the Resilience of Peer-to-Peer Botnets, p. 6.

introduced a proposal for a new law extending the powers of law enforcement officials in dealing with cybercrime quite considerably. Spanish authorities have also played an interesting role in cooperating with the private sector to takedown P2P botnets.[15] Each of these jurisdictions has created or is in the process of creating a national legal framework that to some extent can cope with the cross-border issues which one might expect when taking down a botnet. Finally, all countries are recognised for their defence of the right to privacy and stringent data protection legislation.

First, we will reach out to key stakeholders involved in the fight against botnets. Information will be gathered from interviews with contacts at EUROPOL (EC3), national CERTs, law enforcement authorities, research institutes (TU Delft, IViR, Oii and KU Leuven), and private sector (Microsoft). This step will serve to select a sample of the most common mitigation tools used by law enforcement, private sector and research institutes, gather information about the operation and deployment of solutions, and rank techniques according to their relevance, adequacy and purpose. An in-depth desk research and literature review on the functioning and deployment of the sample will follow.

Later, the deployment of P2P botnet solution will be confronted with the legal requirements enshrined by the applicable European framework, national laws and court rulings of Belgium, UK, the Netherlands and Spain. This will lead to a conclusive assessment of the legal requirements imposed to the use and development of P2P botnet solutions and result in recommendations for the appropriate deployment of such techniques by law enforcement and private sector.

At this stage, possible outcomes include findings on the illegitimate character of some of the sampled solutions as well as inadequacies in the existing national legal frameworks in dealing with the botnet threat. This can be due to: 1. inobservance of national data protection standards by private actors; 2. absence of clear powers given to LEAs to deploy invasive anti-botnet techniques; and 3. obstacles to the use by law enforcement of illegally collected evidence by a third party. Finally, the comparative analysis creates the risk that tools regarded as fair and lawful in one jurisdiction may receive a conflicting interpretation in a different country. If this hypothesis is verified, we will be facing an unlevelled playing field, where there may be an advantage for criminals to target users of Member State where a lesser degree of protection if offered to citizens.

References

Christian Rossow et al., SoK: P2PWNED — Modeling and Evaluating the Resilience of Peer-to-Peer Botnets, 2013 IEEE Symposium on Security and Privacy (SP), 2013.

Directive 2013/40/EC of the European Parliament and of the Council on attacks against information systems and repealing Council Framework Decision 2005/222/JHA

David Dittrich, So you want to take over a botnet, Proceedings of the 5th USENIX conference on Large-Scale Exploits and Emergent Threats, USENIX Association, 2012.

[15]El Grupo de Delitos Telemáticos (GDT) participa junto a SYMANTEC y MICROSOFT en la desarticulación de la BotNet BAMITAL, GDT Press Release, February 19, 2013, Retrieved from https://www.gdt.guardiacivil.es/webgdt/popup_noticia.php?id=1223

European Network and Information Security Agency (ENISA), Botnets: Detection, Measurement, Disinfection & Defence, 2011.

Jan Gassen, Elmar Gerhards-Padilla and Peter Martini, Botnets: How to Fight the Ever-Growing Threat on a Technical Level, Springer, 2013.

Ping Wang et al., A Systematic Study on Peer-to-Peer Botnets, ICCCN 2009, Proceedings of 18th Internatonal Conference on Computer Communications and Networks, 2009.