2016 European Intelligence and Security Informatics Conference

The Role of Internet Service Providers in Botnet Mitigation

Jeroen Pijpker [a,b]

Harald Vranken [a,c]

[a] Faculty of Management,
Science & Technology
Open Universiteit
Heerlen, The Netherlands

[b] School of Media & Entertainment
Management and Technology
Stenden University of Applied Sciences
Emmen, The Netherlands

[c] Faculty of Science
Radboud University
Nijmegen, The Netherlands

***Abstract*—We studied how Internet Service Providers (ISPs) are involved in botnet mitigation in the Netherlands. Although Dutch ISPs on average perform very well with respect to botnet mitigation, botnets still are a significant threat and many end-user systems are infected by bot-malware. We created a reference model which summarizes measures for botnet mitigation from scientific literature that ISPs can take. Our model is structured according to the five stages in the anti-botnet lifecycle: prevention, detection, notification, remediation, and recovery. We validated our reference model in an empirical study by means of semi-structured interviews with a representative sample of Dutch ISPs. Our study identified which measures actually have been taken by ISPs, and why other measures have not been taken (yet). It became clear that ISPs spend most effort on prevention and notification towards customers, thereby focusing on individual bots. ISPs currently have little incentive to implement further measures for detection, remediation, and recovery. Although ISPs are well capable of applying advanced detection and follow up actions, they do not apply such measures mainly due to privacy concerns of customer data. Furthermore, although ISPs do cooperate in various ways, there still is room for improvement, particularly in the sharing of information on botnet infections and mitigation practices with stakeholders and peer ISPs.**

***Keywords*—botnet; botnet mitigation; internet service provider; cyber security; anti-botnet lifecycle**

I. Introduction

Botnets are self-spreading and self-organizing networks of compromised devices (‘bots’) that can be used to perform malicious activities in a coordinated way under control of a botmaster. The bots are infected by malware and receive commands through command-and-control (C&C) channels from a botmaster to carry out malicious activities against bots inside the botnet (internal attacks) or computer systems outside the botnet (external attacks). Examples of malicious activities are stealing sensitive data such as passwords, committing click fraud, manipulating online banking transactions, mining cryptocurrencies, compromising new hosts to extend the botnet, performing distributed denial-of-service attacks, and sending spam or phishing e-mails.

The security threat caused by botnets is huge and worldwide. In this paper, we focus on the situation in the Netherlands. The Netherlands are among the countries with the highest broadband internet coverage and quality in the world, both wired and wireless. Unfortunately, the Netherlands are also an important player in the world of cybercrime and a prime target for botnets. It was estimated that at least 5 to 10 percent (but probably significantly more) of Dutch broadband subscribers suffered an infection that made their computer part of a botnet during 2009 [23]. Subsequent editions of the Cyber Security Assessment Netherlands by the Dutch government have shown that botnets remain a significant cyber security threat [12].

Botnet mitigation should ideally be addressed by both public and private organizations. We previously studied the capabilities and legal authority of organizations in the Netherlands involved in botnet mitigation in 2012 [19]. At that time we focused mainly on public organizations, although we acknowledged the importance of private organizations such as Internet Service Providers (ISPs) and organizations active in vital sectors. In this paper we extend our previous study by focusing entirely on the role of (Dutch) ISPs in botnet mitigation.

It is generally acknowledged that ISPs can play an important role in botnet mitigation, since ISPs − in the role of internet access providers − are well positioned to detect malicious traffic in their networks generated by infected computers of end users and to subsequently disconnect them from the internet or put them into quarantine [10][15][20]. Measures that address end users directly, such as awareness raising and information campaigns, have been proven useful but insufficient. In search for more effective mitigation, the focus has shifted from end users to internet intermediaries, particularly ISPs, as they can undertake mitigation more economically than end users [24]. Besides ISPs, also other parties provide internet access, such as national research networks (NRENS), hosting providers, and corporate and government networks. ISPs nevertheless cover a large part of the IP address space and their customers, such as home users, are most vulnerable to malware infections. In [24] is shown that the bulk of infected systems is actually located in the networks of large ISPs, although there are some significant differences across countries.

978-1-5090-2857-3/16 $31.00 © 2016 IEEE
DOI 10.1109/EISIC.2016.12

IEEE computer society

Numerous botnet mitigation measures for ISPs to take have been proposed in literature, however questions on how effective such measures in reality are, and what measures actually are taken by ISPs, are not widely attributed. In the Netherlands, the Delft University of Technology has been researching the role of ISPs in botnet mitigation, mainly by means of quantitative analyses [3][4][11][23][24]. In the present paper, we complement this research by a qualitative analysis of the role of ISPs in the Netherlands.

The goal of this paper is to enhance the knowledge on the role of ISPs in botnet mitigation. Our contributions are threefold: we provide (i) an overview of both technical, organizational and legal measures that ISPs can take in botnet mitigation, (ii) an overview of which measures are actually applied by ISPs in the Netherlands, and (iii) recommendations on how ISPs can further improve botnet mitigation.

The paper is organized as follows: In section II we first clarify our research method, which consisted of a literature study and an empirical study. In section III and IV we review prior work on botnet mitigation by ISPs: in section III we explore incentives for ISPs to mitigate botnets, and in section IV we address best practices and (Dutch) initiatives for botnet mitigation in which ISPs are involved. In section V and VI we present our key results: in section V we give an overview of botnet mitigation measures taken by ISPs, and in section VI we provide results of our empirical study and show what measures are actually applied by Dutch ISPs. Finally, we conclude the paper with conclusions in section VII and recommendations in section VIII.

II. Research Method

We conducted our research in two phases: a literature study followed by an empirical study. The goal of our research was to examine what measures for botnet mitigation actually have been taken by (Dutch) ISPs, what measures they could have taken (but did not take because such measures are either ineffective or inefficient, or suffer from technical, organizational, or legal issues), and what measures they plan to take in the near future.

We started with an extensive literature study on botnet mitigation and the role of ISPs in botnet mitigation, as outlined in Fig. 1. We identified relevant features of botnets and their C&C-structures and looked at how they affect botnet mitigation methods. Next, we studied technical, organizational and juridical measures that ISPs can take when applying these mitigation methods, which we summarized in a 'reference model'.

Next, in our empirical study, we conducted semi-structured interviews to validate the results from our literature study (i.e., the reference model). We restricted this empirical study to the Netherlands. We interviewed security officers and services managers at five Dutch ISPs during April to September 2015. These five ISPs are a representative sample of the ISPs active in the Netherlands, including some of the largest ISPs operating nationally and some smaller ISPs operating regionally, which together cover about two-thirds of the Dutch broadband internet market. Four of these five ISPs are member of the Abuse Information Exchange (see also section IV), while the fifth ISP is planning to join. In addition, we interviewed an advisor at the Dutch National Cyber Security Centre (NCSC) to identify and prioritize botnet mitigation measures for ISPs in general.

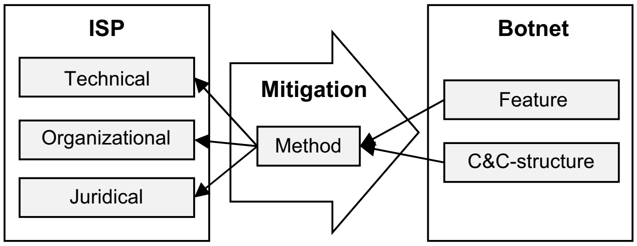

Fig. 1. Approach of literature study.

III. Incentives for ISPs towards Botnet Mitigaction

The fact that ISPs as internet access providers are well positioned to mitigate botnets, does not imply that they actually do or should do so. ISPs may be reluctant to take actions since they are not the root cause of botnets and costs are involved when supporting their customers for dealing with botnets. Initial studies identified various incentives for ISPs that either improve botnet mitigation or have only limited impact [5][10][18][22][25]. The recent quantitative analyses in [24] and subsequently in [4] nevertheless show clearly that ISPs do make a difference in botnet mitigation, which is attributed to organizational and institutional incentives. We summarize their findings in the following subsections.

A. Organizational Incentives

Relevant organizational factors for ISPs to address botnet mitigation include the size of their customer base, the internal organization of their abuse desk, and the cost spend on various security measures. These factors can be controlled directly by ISPs to a large extend.

Absolute figures indicate that the larger the ISP, the larger the number of infected systems in its network. In fact, the majority of infected systems is located at larger, well-established ISPs in well-governed jurisdictions. Such absolute figures however are misleading, since relative figures indicate that larger ISPs in general have fewer infections per customer. Larger ISPs have automated processes for identifying, notifying, and mitigating infected customers, which makes botnet mitigation more economically efficient on a larger scale.

Although larger ISPs in general perform better, still considerable variations in infection levels, up to two orders of magnitude, have been observed for similarly sized ISPs. Also characteristics of ISP customers matter: higher usage rates of pirated software are associated with higher botnet activity, while higher education levels, as an indication of technical competence, are associated with lower levels of botnet activity. On the other hand, average connection speed of customers and average revenue per customer appeared to be unrelated to security performance of ISPs.

B. Institutional Incentives

Relevant institutional factors include the legal and regulatory context in which ISPs operate, and market settings (such as the ISP market structure, the associated competitive pressures, and conditions in related markets such as for security technology). Institutional factors are either imposed by policymakers or by market conditions, which ISPs can only control indirectly.

According to [21] most cyber security incidents should be mitigated at a national level. Therefore national initiatives for clearing networks from botnets should be encouraged and good models should be circulated how to do this successfully.

Regulation is an effective incentive [4]. ISPs have been pushed increasingly to contact customers and clean up infected computers, both by industry groups such as the IETF (Internet Engineering Task Force) [9], country regulators such as the FCC (Federal Communications Commission) [7], and international organizations such as the OECD (Organisation for Economic Cooperation and Development) [16]. As a result, codes of conduct for ISPs and anti-botnet initiatives have been established in several countries. Such initiatives include national anti-botnet centres that act as call centres for infected users, and joint mitigation schemes such as centralized clearing houses that collect and channel infection data to ISPs and their customers. In [4] is shown that having a national anti-botnet centre correlates with lower ISP infection rates in general.

In [10] is suggested that an ISP's arrangements with its peer ISPs might be endangered if the ISP's customers produce too much bad traffic. IP addresses may be blacklisted, which restricts internet access of ISP customers. This is however of less concern for large ISPs because peer ISPs cannot afford to block them. It therefore has been suggested that policymakers should give large ISPs a stronger incentive for taking action, for instance by means of fixed statutory damages against ISPs that act too slowly after being notified of infected computers on their networks [2].

C. Relations between Incentives

Organizational and institutional incentives are interrelated in many ways. ISPs often take organizational measures in response to institutional incentives. For instance, large botnet infection rates may lead to regulation that enforces ISPs to take security measures, which in turn increases cost for mitigation at the organizational ISP level. On the other hand, institutional initiatives such as national anti-botnet centres stem from public–private cooperation, which reduces mitigation cost for ISPs.

In [24] is shown that, although the behaviour of ISPs is largely driven by institutional incentives, ISPs perform very differently under comparable institutional incentives and economic circumstances. This suggests that institutional incentives, while useful and necessary, should also address organizational incentives and realign both. How ISPs react on incentives, depends on their business model. Commercial ISPs will primarily respond to economic incentives, which holds less for non-profit ISPs or cooperatives.

IV. Botnet Mitigation: Best Practices and Initiatives

We previously studied the capabilities and legal authority of Dutch organizations involved in botnet mitigation [19]. Our findings were that no single organization is solely capable or has the authority to effectively mitigate botnets, and therefore organizations – including ISPs – cooperate in structural and ad hoc ways.

This also holds for other countries and numerous organizations, both public and private, cooperate in many ways across the world to address botnet mitigation (see e.g., [21] for a brief overview). An example of international cooperation is the publication of best practices on botnet mitigation by organizations such as APWG (Anti-Phishing Working Group), CSRIC (Communications Security, Reliability and Interoperability Council), ENISA (European Network and Information Security Agency), ETIS (IT Association for Telecommunications), M3AAWG (Messaging, Malware and Mobile Anti-Abuse Working Group), and OTA (Online Trust Alliance). In Europe, the ACDC (Advanced Cyber Defence Centre) project is an example of cooperation in which ISPs, CERTs, law enforcement agencies, IT providers, NRENs, academia and critical infrastructure operators participate. ACDC aims to improve the prevention, detection and mitigation of botnets by offering an infrastructure of interconnected support centres across Europe that are linked to a central clearing house.

In the Netherlands, the largest ISPs joined in a covenant in 2009 that expressed their commitment to botnet mitigation [6]. This covenant addresses gathering and sharing of information by ISPs and dealing with botnet infections in their own networks. Two notable aspects in this covenant are (i) that ISPs explicitly exclude active monitoring of network traffic from customers, and (ii) that ISPs take immediate action upon detection of an infected customer system by completely or partially disconnecting the system from the internet. In 2012 the Abuse Information Exchange was established, an association of Dutch ISPs and other stakeholders with an aggregated market share of over 90 percent. A tangible achievement of this association, although partially funded by the Dutch government, is the AbuseHub system that became operational in 2013. AbuseHub is a central system to collect, analyse and correlate information on botnet infections and other internet abuse from various national and international sources ('reliable notifiers'), such as the ShadowServer Foundation and Microsoft. Notifications on botnet infections are fed directly into the automated incident response processes of Abuse Information Exchange members, who can subsequently warn their customers. The members of AbuseHub cover 78% of the Dutch IPv4 address space and their customers are largely retail users who are most vulnerable to infection.

A study in 2015 evaluated the impact of ISPs on botnet mitigation in the Netherlands by quantitative analysis [11]. It showed that Dutch ISPs on average perform among the best in the world with respect to botnet mitigation and have low infection levels. The same study also evaluated the impact of AbuseHub on botnet mitigation. The preliminary conclusion is that member ISPs already have on average such low infection rates that new initiatives like AbuseHub hardly contribute to further improvement. There are however some differences among ISPs. Also, ISPs that are member of Abuse Information Exchange have improved faster than non-members. The most infected non-members are smaller ISPs.

V. Reference Model for Botnet Mitigation Measures

In this section we present our reference model in which botnet mitigation measures for ISPs, as identified in scientific literature, are summarized. The reference model, as shown in Table I, is structured according to the five stages of the anti-botnet lifecycle as defined by the Online Trust Alliance (OTA). The OTA defined an anti-botnet ecosystem model in 2012 [13], which identifies five stages for botnet mitigation: prevention, detection, notification, remediation, and recovery. The sequence of these five stages constitutes an anti-botnet lifecycle [14], as shown in Fig. 2. When considering specifically the role of ISPs in this anti-botnet lifecycle, these five stages imply the following:

- Prevention: proactive activities initiated by an ISP that can reduce the vulnerability of a user's device.
- Detection: actions/activities with the aim of identifying threats on the network of an ISP.
- Notification: actions/activities conducted by an ISP to inform a customer.
- Remediation: actions/activities initiated by an ISP to remove malicious software from a compromised device.
- Recovery: actions/activities supported by an ISP to resolve the impact of an attack.

The most prominent stage is to prevent that systems get infected by malware and become part of botnet: an ounce of prevention is worth a pound of cure. If systems nevertheless get infected, the first action is to actually detect the infection and subsequently to take further actions by means of notification, remediation and recovery to cure the infection and restore its impact.

We derived botnet mitigation measures for each lifecycle stage from scientific literature. We also identified for each mitigation measure taken by an ISP whether the measure is targeted towards the ISP's customers, other stakeholders (such as peer ISPs), or the ISP itself, and whether the measure addresses technical, organizational, or legal aspects. We summarize our findings in the following subsections. We first elaborate on botnet mitigation measures, and next focus on each lifecycle stage in more detail.

A. *Botnet Mitigation Measures*

Ashgari extracted botnet mitigation measures in 2010 from several industry driven efforts (APWG, ENISA, ETIS, M3AAWG, OECD) and came up with a set of over 200 best security practices [3]. These measures include both technical, organizational and legal aspects, which can be categorized into: active abuse handling; proactive detection of malicious activity; filtering malicious traffic and content; user education and awareness; client security and quarantining; using updated network protocols and servers; participation in security community; management and administrative procedures; legal measures. Since 2010, some best practices have been renewed and also new best practices have been published (as discussed in section IV), which we also incorporated in our reference model.

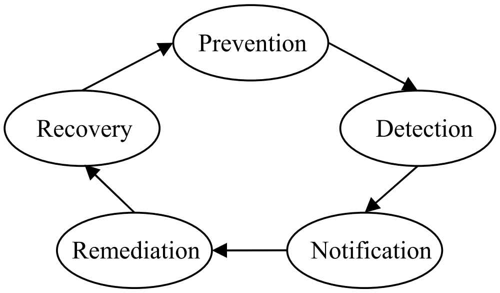

Fig. 2. Anti-botnet lifecyle [14].

Botnet mitigation is an international effort that crosses borders. Agreements between countries are needed to prosecute cybercrime in a consistent and coordinated way [20]. Within each country, botnet mitigation measures should respect local laws. Public telecom providers in the Netherlands must abide by article 11.3 of the Telecommunications Act. According to this act, ISPs are required to take technical and organizational measures to protect their customers against cybercrime. ISPs are also required to inform their customers on the risks (such as botnets) associated with the use of internet services offered by the ISPs, and what customers can do themselves in order to reduce these risks. Hence, ISPs have obligations towards their customers of technical, organizational and informational nature. The act however does not state explicitly what an ISP should do whenever a botnet is detected in its networks. Hence, actions by ISPs against botnets are currently taken more voluntarily rather than obliged by law.

B. *Prevention*

A first measure that ISPs can take to prevent that customer systems get infected with malware and become part of a botnet, is to proactively provide end-point security solutions to their customers (P-1). For example, ISPs can provide anti-virus software or secure routers to their customers. Another important measure in prevention is customer education (P-2). ISPs can educate their customers about the threats imposed by botnets and what customers should do and not do to avoid malware infections. Examples are awareness training and information campaigns that teach customers how to recognize phishing e-mails and that urge them to apply end-point security solutions and to frequently back-up their data.

ISPs can collaborate with other stakeholders by sharing information on botnet mitigation (P-3). For example, ISPs can share lessons learned and procedures about botnet mitigation with other parties, such as peer ISPs or a national cyber security centre. ISPs can also actively participate in botnet mitigation initiatives (P-4), of which the Abuse Information Exchange in the Netherlands is an example.

TABLE I. REFERENCE MODEL

Target group	*Aspect*	*Description*	*Technical*	*Organizational*	*Legal*
PREVENTION					
Customer	P-1	ISP provides end-point security solutions to its customers	x	x	
	P-2	ISP actively educates its customers on botnet threats and mitigation	x	x	x
Other	P-3	ISP collaborates by sharing information on botnet mitigation		x	
	P-4	ISP collaborates in initiatives for botnet mitigation		x	
ISP	P-5	ISP applies Intrusion Prevention System (IPS)	x		
	P-6	ISP applies technical measures against botnet infections	x		
	P-7	ISP keeps up with latest trends regarding botnet mitigation	x	x	
	P-8	ISP has implemented customer support processes		x	
	P-9	ISP offers Service Level Agreements (SLAs)		x	
	P-10	ISP conforms to security standards		x	
DETECTION					
Customer	D-1	ISP provides self-identify portal		x	
	D-2	ISP receives information about potential botnet infection from customers		x	
Other	D-3	ISP communicates about detected (botnet) infections		x	
	D-4	ISP receives information about possible infections from external parties		x	
	D-5	ISP receives information about possible infections from AbuseHub		x	
ISP	D-6	ISP applies honeynet	x		
	D-7	ISP applies Intrusion Detection System (IDS)	x	x	
	D-8	ISP actively validates infections	x		
	D-9	ISP has abuse team		x	
NOTIFICATION					
Customer	N-1	ISP notifies infected customers		x	
	N-2	ISP provides notification with remediation tools	x	x	
Other	N-3	ISP notifies other providers about infections		x	
REMEDIATION					
Customer	V-1	ISP isolates infected customers	x	x	
	V-2	ISP shares information about solutions to mitigate possible (botnet) infection	x	x	
	V-3	ISP provides links for customer to get professional help in case of infection		x	
Customer/other	V-4	ISP shares information about walled garden procedure		x	
Other	V-5	ISP shares best practices about removal of infections		x	
RECOVERY					
Customer	H-1	ISP activates customer’s internet connection	x	x	
	H-2	ISP supports customer in recovery process		x	
	H-3	ISP informs customer on effects of recovery on personal data and accounts		x	
	H-4	ISP actively gives information about recovery to customers		x	

ISPs can also take measures that affect their internal operation and infrastructure. Technical measures that ISPs can take are applying an Intrusion Prevention System (IPS) (P-5), or applying other technical measures such as securing their DNS servers (P-6). Organizational measures imply keeping up with the latest trends regarding botnet mitigation (P-7), implementing customer support processes (P-8), offering Service Level Agreements (SLAs) with respect to botnet mitigation (P-9), and conforming to security standards such as ISO 27002:2005 and ISO 27006:2007 (P-10).

C. Detection

When customer systems nevertheless get infected and become part of a botnet, this should be detected as soon as possible. Botnet detection methods can be classified in various ways. For instance the taxonomy in [8] considers detection methods that focus on either bots, C&C-servers or botmasters. ISPs however focus primarily on detection of bots. An alternative view is given in [1], where botnet detection techniques are classified as either active by means of honeynets, or passive by means of an Intrusion Detection System (IDS) using DNS-based, host-based, network-based or hybrid detection.

Our reference model includes nine aspects that cover these detection methods (D-1 to D-9). Towards customers, ISPs can offer a web portal or related resource that enables customers to self-identify a potential bot-malware infection (D-1). ISPs can also receive information about possible botnet infections from their customers by other means (D-2), for instance when a customer contacts its ISP to report a possible infection.

In relation with other stakeholders, ISPs can share information about detected infections (D-3), for instance with other ISPs. ISPs can also receive information about possible infections from external resources (D-4). In the Netherlands the AbuseHub system provides ISPs with information about possible infections (D-5).

With respect to their internal operation and infrastructure, ISPs can apply honeynets (D-6) or IDSs (D-7) in their network to detect infections. When an ISP detects an infection, it should validate whether the detected infection is indeed accurate and decide on appropriate measures against the infection (D-8). An ISP should have an abuse team in place to handle infections (D-9).

D. Notification

Upon detection, an ISP should notify the infected customer (N-1), for example by email, phone or an in-browser message. This message should also contain information on remediation tools that can be applied to solve the problem of the infection (N-2). ISPs can also notify other stakeholders such as peer ISPs about infections (N-3).

E. Remediation

ISPs can take remediation measures to deal with compromised customer systems that are part of a botnet. An ISP can isolate a compromised system by disconnecting it partially or completely from the internet (V-1). ISPs can also share information with customers about how to mitigate a botnet infection (V-2), or provide links on where to get professional help (V-3). An ISP should share information on how it deals with compromised systems that are isolated (V-5), both to its customers and other stakeholders. For instance, the procedures should be clear to customers for disconnecting a system and reconnecting it again after the infection has been solved. ISPs can also share best practices on how to remove infections with bot-malware with other stakeholders (V-5), such as peer ISPs.

F. Recovery

The final step after notification and remediation is recovery. An ISP reconnects the customer system after the infection is removed (H-1). An ISP can also support their customers in recovery after an infection (H-2), for example by offering appropriate information. An ISP can inform its customers about the possible effects of the recovery operation on personal data and user accounts (H-3), and offer support in the recovery process (H-4).

VI. Empirical Results

In this section we present the results of our empirical study in which we validated the reference model in interviews with five Dutch ISPs and the NCSC (see [17] for detailed results).

A. Completeness and Correctness of Reference Model

We presented our reference model to the interviewees and we examined all aspects of the reference model during the interviews. All interviewees concluded that the reference model is complete and correct. Although this cannot be considered as a thorough scientific or statistical proof, it provides basic confidence in the validity and reliability of the reference model.

Our reference model does not include advanced follow-up actions in botnet mitigation such as taking down C&C-servers, hacking back by taking over C&C-servers or infiltrating in a botnet to dismantle the botnet from within, disinfecting compromised customer systems remotely, unsolicitedly terminating the contract with a customer after multiple infections, and blocking websites that infect visitors with bot-malware. All ISPs indicated that they do not apply such actions, and this was also confirmed by the NCSC.

B. Detailling the Reference Model

We used the results of our empirical study to add further details to the aspects in our reference model. This is reflected by the shading in Table I: of the 31 aspects in our reference model, 6 (marked in dark grey in Table I) are barely applied by the interviewed ISPs, 11 (marked in light grey in Table I) are applied only by a limited set of the interviewed ISPs, while 14 (in white in Table I) are applied by almost all of the interviewed ISPs.

The aspects P-5, D-1, D-2, D-6, D-7 and H-4 are barely applied by the interviewed ISPs. None of the interviewed ISPs is currently applying an IPS (P-5), only one ISP is applying an IDS on a limited scale (D-7), and only two ISPs are applying a honeynet in their networks on a limited scale (D-6). All ISPs pointed out that they do not actively monitor and analyse the content of traffic as generated by their customers, and hence they do not perform Deep Packet Inspection (DPI). Some ISPs however are considering to offer this as a commercial service in the near future. The aspects D-1 (offering a portal where customers can self-identify a potential bot-malware infection), D-2 (receiving information on botnet infections directly from customers by other means), and H-4 (providing information about the recovery process to customers) are applied only by two ISPs, and even by those two only on a limited scale.

The aspects P-6, P-9, P-10, D-3, N-3, V-1, V-3, V-4, V-5, H-2 and H-3 are fully applied by some (i.e., two or three) of the five interviewed ISPs. Some ISPs apply technical measures to prevent botnet infections such as secured DNS servers (P-6), some offer SLAs (P-9), and some conform to security standards (P-10). It is notable that information sharing with stakeholders (such as peer ISPs) is rather limited: only some ISPs communicate with (D-3) or notify (N-3) other stakeholders about botnet infections, or share information about walled garden procedures (V-4) or best practices about removal of infections (V-5). Also, most of the other measures for remediation and recovery are only applied by some ISPs: isolating infected customers (V-1), directing infected customers to professional help (V-3), supporting customers in the recovery process (H-2), and informing customers on the effects of recovery on personal data and accounts (H-3).

C. Discussion

It is evident from Table I that ISPs are currently spending most of their effort on prevention and notification towards their customers (P-1, P-2, N-1, N-2). Our literature study already pointed out that prevention is most effective and efficient (see section V). ISPs in the Netherlands are also required to protect and inform their customers against botnet infections according to the Telecommunications Act. All ISPs provide end-point security solutions to their customers (P-1), they actively educate their customers on botnet threats and mitigation (P-2), they notify infected customers (N-1), and provide remediation tools (N-2). The way customers are notified, is however not standardized (yet): ISPs either use a walled garden environment or communicate with infected customers by email, sms or phone.

A second observation from Table I is that ISPs are reluctant to take further actions in botnet detection. It is remarkable that ISPs offer limited support for botnet detection initiated by customers (D-1, D-2). All ISPs emphasize that they do not monitor and analyse the content of customer traffic by applying IPS or DPI (P-5, D-6, D-7). Customers should feel safe that their privacy is respected and that ISPs do not eavesdrop on their messages. On the other hand, we already identified in our previous work [19] that ISPs are well capable of performing advanced detection and follow-up actions by means of active and passive detection, removing malware from customer systems, combatting botnets by taking over or seizing C&C-servers and disrupting C&C-channels, tracing botnet traffic, and safeguarding evidence. Largely driven by the fear for terrorism, a public debate is currently ongoing whether and to what extent privacy of citizens could be sacrificed to gain stronger security. In this context, customers may be more willing to accept that their internet traffic is monitored and analysed if this helps in the fight against cybercrime.

A third observation from Table I is that ISPs have customer support processes in place for prevention (P-8) and detection (D-8, D-9), but they offer little customer support for remediation and recovery. There is room for improvement, particularly considering the sharing of information (V-3, V-4, V-5, H-3, H-4). ISPs are however not obliged by law to take such actions. On the positive side, ISPs do provide information to customers on solutions for mitigating a botnet infection (V-2). Two ISPs isolate infected customers in a walled garden (V-1). After a customer has been isolated, the customer however has to take action in order to be reconnected to the internet (H-1).

A final observation is that, although information sharing both with customers and other stakeholders can be improved, ISPs are currently well informed on botnet threats (P-7, D-4). The AbuseHub system (D-5) is a prominent example of a central system in which abuse information from reliable notifiers is gathered and distributed to the member ISPs.

VII. Conclusion

Quantitative studies [11] showed on the one hand that Dutch ISPs on average perform among the best in the world with respect to botnet mitigation and have low infection levels. However, on the other hand quantitative studies [12][23] also showed that botnets still are a significant threat and a considerable amount of end-user systems is infected by bot-malware. Hence, there still is a need to take further actions towards botnet mitigation, which also involves ISPs.

We created a reference model that states measures that ISPs (can) take in botnet mitigation. The model is structured according to the five stages in the anti-botnet lifecycle: prevention, detection, notification, remediation, and recovery. We validated the reference model with a representative sample of Dutch ISPs. It has become clear that these ISPs spend most effort on prevention, not only since this has been proven to be the most effective and efficient approach, but also since ISPs in the Netherlands are required to do so according to the Telecommunications Act. The act however does not explicitly state what actions ISPs should take towards their customers. It furthermore has become clear that ISPs currently have little incentive to implement further measures for detection, remediation, and recovery. ISPs do not apply advanced detection and follow-up actions, although they are well capable of doing so. The main reason for not applying IPS, IDS or honeynets is privacy concerns of customer data. ISPs cooperate to some extent. A prominent example is the AbuseHub system, a central system in which abuse information from reliable notifiers is gathered and distributed to the member ISPs. Nevertheless, there still is room for improvement, particularly in the sharing of information on botnet infections and mitigation practices with stakeholders and peer ISPs.

VIII. Recommendations

Various recommendations can be derived from our results.

Timely action is crucial in botnet mitigation given the dynamic nature of botnets. Hence, also prompt action by ISPs is required: infected customer systems should be detected and subsequently isolated as soon as possible. ISPs currently focus on supporting their customers in prevention and notification, although the way ISPs communicate with their customers is non-uniform. Detection and remediation are addressed less and furthermore these focus on individual bots (i.e., infected customer systems) rather than botnets as a whole. There is considerable room for ISPs to improve on these aspects.

A second recommendation is that ISPs improve their information sharing with stakeholders such as peer ISPs. ISPs rely on systems such as AbuseHub to receive information on infected systems (IP addresses), but in return ISPs do not share information on infected systems in their own networks. Also, ISPs do not follow up on customers that report possible infections. Hence, there also is room for improvement in the registration of infections and reporting to stakeholders.

Cybercrime is evolving fast. The latest trend in cybercrime is ransomware. Ransomware can be distributed by botnets, and hence fighting ransomware to some extent implies fighting botnets. However, addressing new trends in cybercrime should not lead to flagged attention for botnet mitigation.

Acknowledgment

We kindfully thank the interviewees (who wished to stay anonymous) at the ISPs and NCSC for their cooperation.

References

[1] R. Abdullah, N. Abu, M. Faizal and Z. Noh, “Understanding the threats of botnets detection: a wide scale survey,” Research Journal of Information Technology, 2014, 6(3), 135-153.

[2] R. Anderson, R. Böhme, R. Clayton and T. Moore, Security economics and the internal market. European Network and Information Security Agency (ENISA), 2008.

[3] H. Asghari, Botnet mitigation and the role of ISPs: a quantitative study into the role and incentives of Internet Service Providers in combating botnet propagation and activity. Master thesis, Delft University of Technology, The Netherlands, 2010.

[4] H. Asghari, M. van Eeten and J. Bauer, “Economics for fighting botnets: lessons learned from a decade of mitigation,” IEEE Security & Privacy, September/October 2015, 13(5), pp. 16-23.

[5] J. Bauer and M. van Eeten, “Cybersecurity: stakeholder incentives, externalities, and policy options,” Telecommunications Policy, 2009, 33(10-11), 706-719.

[6] ECP, Raamwerk afspraken botnetbestijding, 2009.

[7] Federal Communications Commission (FCC), US Anti-bot code of conduct (ABCs) for Internet Service Providers (ISPs), 2012.

[8] S. Khattak, N. Rasheed Ramay, K. Riaz Khan, A. Syed and S. Ali Khayam, “A taxonomy of botnet behavior, detection, and defense,” IEEE Communications Surveys & Tutorials, 2014, 16(2), 898-924.

[9] J. Livingood, N. Mody and M. O’Reirdan, Recommendations for the remediation of bots in ISP networks (RFC 6561). Internet Engineering Task Force (IETF), 2012.

[10] T. Moore, R. Clayton and R. Anderson, “The economics of online crime,” The Journal of Economic Perspectives, 2009, 23(3), 3-20.

[11] G. Moura, Q. Lone, H. Asghari and M. van Eeten, Evaluating the impact of AbuseHUB on botnet mitigation, interim deliverable 1.0. Delft University of Technology, The Netherlands, 2015.

[12] National Cyber Security Centre (NCSC), Cyber Security Assessment Netherlands (CSAN 2015), 2015.

[13] Online Trust Alliance (OTA), Combatting botnets through user notification across the ecosystem: a view of emerging practices, 2012.

[14] Online Trust Alliance (OTA), Botnet remediation overview & practices, 2013.

[15] Organisation for Economic Cooperation and Development (OECD), The role of internet intermediaries in advancing public policy objectives: forging partnerships for advancing policy objectives for the internet economy, Part II, 2011.

[16] Organisation for Economic Cooperation and Development (OECD), Proactive policy measures by Internet Service Providers against botnets, 2012.

[17] J. Pijpker, The role of Internet Service Providers in botnet mitigation. Master thesis, Open Universiteit, The Netherlands, 2015.

[18] I. Png and C. Wang, “The deterrent effect of enforcement against computer hackers: cross-country evidence,” Workshop on the Economics of Information Security (WEIS), 2007.

[19] T. Schless and H. Vranken, “Counter botnet activities in the Netherlands: a study on organisation and effectiveness,” Proceedings 8th International Conference for Internet Technology and Secured Transactions (ICITST), 2013, pp. 442-447.

[20] S. Silva, R. Silva, R. Pinto and R. Salles, “ Botnets: a survey,” Computer Networks, 2013, 57(2), 378-403.

[21] H. Tiirmaa-Klaar, J. Gassen, E. Gerhards-Padilla and P. Martini, Botnets. Springer, 2013.

[22] M. van Eeten and J. Bauer, “The economics of malware: security decisions, incentives and externalities,” OECD Science, Technology and Industry, 2008, Working Paper No. 2008/1.

[23] M. van Eeten, H. Asghari, J. Bauer and S. Tabatabaie, “ISPs and botnet mitigations: a fact-finding study on the Dutch market,” Delft University of Technology, The Netherlands, 2011.

[24] M. van Eeten, J. Bauer, H. Asghari, S. Tabatabaie and D. Rand, “The role of Internet Service Providers in botnet mitigation: an empirical analysis based on spam data,” Workshop on the Economics of Information Security (WEIS), 2010.

[25] Q.-H. Wang and S.-H. Kim, “Cyber attacks: cross-country interdependence and enforcement,” Workshop on the Economics of Information Security (WEIS), 2009.