COUNTER BOTNET ACTIVITIES IN THE NETHERLANDS

A STUDY ON ORGANISATION AND EFFECTIVENESS

Timo Schless & Harald Vranken (Open Universiteit, School of Computer Science)

Door de Commissie Toekenning René Olthuisprijs van de Vereniging Informatici Defensie is voorgedragen de majoor T.L.A. Schless voor zijn scriptie De organisatie van botnetbestrijding in Nederland afgerond op 10 september 2013 ter afsluiting van de opleiding Business Process Management & Information Technology aan de faculteit Informatica van de Open Universiteit. De winnende bijdrage is een scriptie waarin het cyberaspect botnets ter discussie is gebracht. Op een systematisch analytische wijze wordt de organisatie van de botnetbestrijding gefileerd. Intercom publiceert de scriptie integraal omdat dit onderwerp ook voor onze lezers van belang is. →

Abstract—Botnets are networks of compromised computers used to carry out malicious activities in a coordinated way under control of a botmaster. Botnets are a major threat on the internet and there is general agreement on the necessity of botnet countermeasures.
We studied how counter botnet activities are organised in the Netherlands. Through literature study and an empirical study we analysed organisations involved in counteracting botnets, and their capabilities and legal usage thereof. Our findings are that no single organisation is solely capable or has the authority to effectively oppose botnets, and therefore organisations cooperate in structural and ad hoc ways. Relatively simple botnets can be countered effectively, but capabilities and legal authority to disrupt more complex or foreign botnets are missing.

I. INTRODUCTION

Botnets are self-spreading and self-organising networks of compromised computers ('bots') that can be used to perform malicious activities in a coordinated way under control of a botmaster. Botnets can vary in size from hundreds to millions of bots. The bots are infected by malware ('botagents') and receive commands from the 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, compromising new hosts to extend the botnet, performing distributed denial-of-service attacks, and sending spam or phishing e-mails [8, 9, 12, 16, 18, 23].

The security threat caused by botnets is large and worldwide. In this paper, we focus on the situation in the Netherlands. The Netherlands are among the countries with the highest broadband penetration and quality, both wired and wireless, in the world[1]. Unfortunately, the Netherlands are also an important player in the world of cybercrime[2] and a prime target for botnets. It has been estimated that at least 5 to 10 percent (but probably significantly more) of all Dutch broadband subscribers suffered an infection that made their computer part of a botnet during 2009 [4]. The BredoLab-botnet, which distributed spam and denial-of-service attacks, was dismantled in 2010 in an internationally coordinated operation [7]. Although masterminded from Armenia, with millions of bots worldwide, its operations were concentrated in the Netherlands. The detection of the Pobelka-botnet in the Netherlands in 2012 showed that, although this botnet primarily targeted financial transactions, also sensitive data from vital sectors

[1] Organisation for Economic Co-operation and Development, www.oecd.org [2] IC3 2012 Internet Crime Report, www.ic3.gov.

Maj Schless ontvangt de René Olthuisprijs uit handen van Drs D.M. Koen Foto M.C.J. van der Ploeg

and civilians were obtained [14]. The press enlarged upon this, which led to questions raised in the Netherlands parliament in 2013. In the National Cyber Security Strategy, the Netherlands government stresses the importance of joint action, both civil-military, public-private, and national-international, against cyber threats caused by botnets [13].

Scientific literature focuses primarily on technical aspects of botnets, covering the structure of botnets, malicious activities performed by botnets, and countermeasures against botnets. However, little attention has been given to organisational aspects of counter botnet activities. In this paper we try to fill this gap and focus on organisational aspects of counter botnet activities.
Our contributions are threefold: First, we present a generic model that relates required capabilities, as well as intentions and structures of botnets, to botnet countermeasures. Second, we identify the organisations involved in counter botnet activities in the Netherlands and analyse their capabilities and legal authority, which may serve as an example for other countries. Third, by combining the generic model and the mapping of organisations, we answer the question whether counteracting botnets is effectively feasible in the Netherlands and we show which future directions are needed.

The rest of this paper is organised as follows (see Fig. 1): In section II we explain our research method. In section III we look at

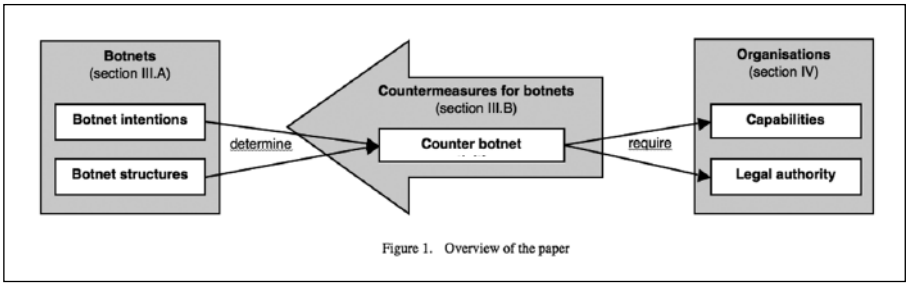

Figure 1. Overview of the paper

basic properties of botnets and countermeasures. In section IV we present the capabilities required for acting against botnets, we map the organisations involved in fighting botnets in the Netherlands, and analyse their capabilities and legal usage thereof. In section V we elaborate further on our empirical findings. Section VI concludes the paper.

II. RESEARCH METHOD

We started our research with an extensive literature study on botnets. We identified basic properties of botnets, countermeasures against botnets, capabilities and authority required for using these countermeasures, and organisations involved in combating botnets.

Next, we did an empirical study to validate the results from our literature study and to assess how counter botnet activities are organised in the Netherlands. We performed the empirical study by means of semi-structured interviews during April-June 2013 with 10 officials at 6 key organisations: Team High Tech Crime of the National Police, National Coordinator for Counterterrorism and Security, National Cyber Security Center, Public Prosecution Service, Fox-IT, and DefCERT. (See Section IV.A and Table II for more details.)

We identified a large number of both public and private organisations that are involved in fighting botnets. These include governmental organisations, computer security companies, internet service providers (ISPs) and hosting providers, and organisations in vital sectors (such as electricity, telecommunication, water, food, finances, and chemical industry). There are many structural and ad hoc relations and collaborations between these organisations.

In the public domain, we interviewed four key governmental organisations in cyber security. We excluded the intelligence services and armed forces from our empirical study because of their specific tasks and limited or unidirectional interaction with other organisations. We interviewed a single but prominent computer security firm (Fox-IT) that has numerous public and private organisations as customers, including organisations in vital sectors and ISPs. It therefore has a broad view on counter botnet activities in the private sector and on cooperation between the private and public sector. We also interviewed DefCERT, the CERT of the Ministry of Defence, which offers supporting services to the armed forces, but has no military tasks and therefore is considered as a representative of organisations in vital sectors.

The limited number of interviewed organisations may affect the reliability of our empirical study. We asked every interviewed organisation whether we had omitted organisations in our study with key capabilities and legal authority. This turned out not to be the case. Furthermore, in each interview we not only inquired after capabilities and legal authority of the organisation itself, but also of other organisations that cooperate with the interviewed organisation. The interviews gave a consistent view and hence we have confidence in the reliability of our results. Nevertheless, our results may be incomplete, particularly for ISPs and organisations in vital sectors.

The key results of our study are a generic model stating the capabilities required for acting against botnets as derived from our literature study and validated in our empirical study, the mapping of Dutch organisations involved in counter botnet activities and their capabilities and legal authority as derived from our empirical study, and a concluding statement on whether counter botnet activities are organised effectively in the Netherlands. More information on our research method (including interview reports) and results is available in [19].

III. BOTNETS: PROPERTIES AND COUNTERMEASURES

A. Properties of Botnets

We consider intentions and structures of botnets as two basic properties that can be used to classify botnets, of which botnet structure is most relevant as it says a lot about the strengths, weaknesses and behaviour of a botnet [22]. Other properties could also be used to classify botnets, such as types of attacks performed by botnets and methods to extend the botnet by infecting new hosts, but these are less relevant for our study on the organisation of counter botnet activities.

Literature offers numerous classifications for intentions of cyber attacks that are also applicable for classifying botnets. We use the classification in Table I, which is based on [14, 21]. Note that a botnet can have multiple botmasters that use the botnet simultaneously for different purposes [15] and a botmaster may offer the botnet to third parties that use the botnet for their own goals. Furthermore, the division between white hats and black hats is not always clear, e.g., intelligence services making use of criminals for cyber espionage. ➔

TABLE I. INTENTIONS OF CYBER ATTACKS USING BOTNETS

	Intention	Description
A	cyber vandalism	undesirable activities (not necessarily criminal), such as insulting tweets or bullying on social media, by individuals for pleasure or recalcitrance
B	crime over the internet	criminal activities supported by the internet, such as child pornography, racism, stalking or piracy, by individuals or criminals for profit or pleasure
C	cyber crime	criminal activities that primarily take place on/by the internet, such as phishing, denial-of-service attacks, sending spam, click fraud, digital burglary and stealing information, by criminal organisations for financial or other gain
D	hacktivism	activities such as (threatening with) denial-of-service attacks or digital burglary, usually for publicity by groups with a political or ideological purpose
E	cyber terrorism	activities such as (threatening with) sabotage of vital facilities by or on behalf of groups with a political or ideological purpose
F	cyber war	activities such as digital espionage, (threatening with) sabotage of vital or military facilities with cyber attacks on computer systems, supporting psychological warfare by spam or enforcing censorship, by or on behalf of national states

Generally, three command structures for botnets can be distinguished: centralised, decentralised and hybrid. In all command structures, command & control channels are used for communication between the botmaster(s) and the bots. Botnets with a centralised command structure make use of one or more central servers to send commands to individual bots, typically by means of the IRC-protocol or HTTP [9]. These channels are bidirectional, and hence the botmaster can also receive information from bots [25]. Botnets also can use chat servers, blogs or twitter accounts, instant messaging (IM) services or proprietary protocols [22]. In a centralised command structure, the botmaster can reach the bots quickly and easily, obtain information from bots, and control the entire botnet. The weakness is the dependence on a limited number of central servers. When these central servers are taken over or eliminated, the botmaster loses control over the botnet.

In a decentralised command structure, command & control channels are established between individual bots in a peer-to-peer fashion. The botmaster gives commands directly to a number of bots, which in turn spread the commands further. Such botnets are more robust than botnets with a centralised command structure. However, a decentralised command structure is more complex and difficult to implement [23, 24]. It also is difficult to reach all bots simultaneously due to uncertainty in propagation times. The channels are usually unidirectional, which makes it difficult for a botmaster to obtain information from individual bots [25]. Furthermore, measures should be taken, such as authentication and encryption, to ensure that bots only accept commands from genuine peers [22].

Recent research shows that botnets are becoming even more complex by applying hybrid command structures that mix centralised and decentralised command structures [24]. Examples are botnets that use a decentralised network of bot servants that act both as bot server and client [11], botnets that make use of social networks and cloud services [26], and botnets that use (reverse) proxies and fast-flux networks where domain names or IP addresses of bots, bot servers and DNS servers continuously change [6, 22, 27]. Also, channels for command & control and data can be separated such that each channel uses a hybrid structure that best fits its purpose [25].

B. Countermeasures

Botnets are visible through three activities: spreading and infecting new bots, traffic on command & control channels, and attacks [12]. Tracking and detecting botnets can take place by looking for traces of such activities, either actively by 'honeynets' or passively by searching for known botnet patterns or anomalies in software and network traffic [9, 17, 22].

The next step after tracking and detecting a botnet, is analysis of the command structure of the botnet. Analysis methods are available [3, 10, 18, 20], but analysis becomes more difficult with increasing complexity of the command structure and requires that at least some behaviour of the botnet is already known. When the internet address of a botmaster is revealed, the geographical location of the botmaster may be identified. In practice however, due to technical, political and legal reasons, this may be difficult to achieve [2, 26].

A botnet can be disabled by affecting either individual bots, the command structure or command & control channels, or the botmaster [5]. In practice, it is nearly impossible to track all bots in a botnet. Botnets with a centralised command structure can be disabled by taking over the command & control server, while botnets with a decentralised command structure can be disrupted by manipulating bots or traffic on the command & control channels [20]. Capturing the botmaster depends on its geographical location and jurisdiction. Command & control servers can be seized and, depending on available evidence, the botmaster can be arrested and prosecuted. In case of cyber terrorism or cyber war, the botmaster or the botnet infrastructure can be attacked physically. Counter botnet activities however may not always be effective. A disabled command & control server could have been backed up in another country, disrupting a botnet can have negative effects on other communications, and an arrested botmaster can be replaced. Botnets are designed to be operational soon after disruption [1]. The upper part of Table IV shows the relations between countermeasures, structures, and intentions of botnets.

IV. COUNTERACTING BOTNETS: ORGANISATIONS, CAPABILITIES AND LEGAL AUTHORITY

A. Organisations

Our literature research and empirical study identified key public and private organisations that are involved in fighting botnets,

shown in Table II. In addition, there are organisations in the background with supportive tasks: Nederlands Forensisch Instituut (NFI, Netherlands Forensic Institute) is a public organisation that provides support and expertise through independent analysis and interpretation of evidence; Stichting Internet Domeinnaamregistratie Nederland (SIDN, Foundation for Internet Domain Name Registration in the Netherlands) registers .nl domain names and stimulates initiatives for an open and secure internet; the Ministry of Economic Affairs promotes private initiatives in the field of cyber security; Autoriteit Consument en Markt (ACM, Authority for Consumers and Markets) monitors the telecommunications sector and can, for instance, impose fines for sending spam.

B. Capabilites and Legal Authority

From literature and empirical study, we identified 19 capabilities that are required to counter botnets effectively, shown in Table III. The lower part of Table IV shows the relations between countermeasures and capabilities. Table IV is a generic model indicating the relations between countermeasures on the one hand and command structures, intentions and capabilities required for acting against botnets on the other hand.

The lower part of Table V shows the capabilities and legal authority of organisations involved in counter botnet activities in the Netherlands. It can for instance be seen that the police and private computer security companies are capable of passive detection of botnets (C2), but this requires explicit authorisation. ISPs have the same capabilities, but are only allowed to perform passive detection on their own networks. Also computer security companies have several capabilities that they are not allowed to deploy on public networks, such as investigation of specific botnets (C4), decrypting information (C5), and taking over command servers (C7). On public networks such activities are considered as intentional and unlawful intrusion of computer systems, which is an offence under the Dutch criminal law (Wetboek van Strafrecht, Artikel 138ab). These capabilities may be applied on private networks, but even this may be prohibited by privacy regulations. The upper part of Table V shows which organizations in the Netherlands can counter botnets with specific intentions. Our empirical results indicate however that organisations do not use such specific classification. Instead, they consider the specific context of each individual botnet, in which relevant aspects are: location (whether the botnet infrastructure resides inside or outside the Netherlands), type of attack or offence, and exploited vulnerabilities. A classification of botnet intentions is however considered useful for policy making. A classification based on command structures is currently rarely used in practice, since most present botnets only apply relatively simple centralised command structures.

TABLE II. KEY ORGANISATIONS

Public organisations
Nationaal Coördinator Terrorismebestrijding en Veiligheid (NCTV) / National Coordinator for Counterterrorism and Security The NCTV resides under the Ministry of Security and Justice and is since 2011 the central organisation in the Netherlands responsible for counterterrorism, cyber security, national security and crisis control. The NCTV has several departments, including the National Cyber Security Center (NCSC). The NCSC is the center of knowledge and expertise on cyber security that also acts as central CERT and is responsible for crisis coordination in case of cyber incidents.
Politie / Police The police resides under the Ministry of Security and Justice. Cyber crime is dealt with by the Team High Tech Crime (THTC).
Algemene Inlichtingen- en Veiligheidsdienst (AIVD) / General Intelligence and Security Service The AIVD resides under the Ministry of the Interior and Kingdom Relations. The tasks of the AIVD, under the 2002 Intelligence and Security Services Act, are investigating individuals and organisations, conducting security screenings, promoting the security of vital sectors, gathering international intelligence, and compiling risk and threat analyses.
Krijgsmacht / Armed forces The armed forces reside under the Ministry of Defence. For cyber crime, the Militaire Inlichtingen- en Veiligheidsdienst (MIVD; Military Intelligence and Security Service) and the Koninklijke Marechaussee (KMAR; Royal Military Police) are relevant. DefCERT is the CERT of the Ministry of Defence, but has no military tasks.
Openbaar Ministerie (OM) / Public Prosecution Service The OM ensures that offences are investigated and prosecuted, and that judgments of the court are executed.
Private organisations
IT companies Relevant IT companies are ISPs and computer security companies.
Private organisations in vital sectors Examples are organisations in electricity, telecommunication, water, food, finances, and chemical industry.

TABLE III. CAPABILITIES FOR COUNTERACTING BOTNETS

Tracking, detection and analysis	
C1	Active detection of bots and botnets using a honeynet
C2	Passive detection of bots and botnets
C3	Examining behaviour and properties of malware (botagents)
C4	Investigating the behaviour and properties of specific botnets by means of honeynets, infiltration with botagents, capturing botnet traffic, manipulation of the command & control channels, acquiring a command & control server
C5	Revealing encryption keys and decrypting information
Disabling using technical measures	
C6	Removing botagents from bots
C7	Taking over a command & control server
C8	Disrupting a botnet using manipulated bots
C9	Disrupting a botnet by blocking or manipulating communication
C10	Taking over a botnet by manipulating communication
Disabling using legal measures	
C11	Tracing internet addresses and computers
C12	Tracing a botmaster by law enforcement agencies in a country or by cooperation with authorities abroad
C13	Confiscating a command server or computer equipment, and NTD
C14	Safeguarding evidence (both physical and digital)
C15	Arrest and prosecution of botmaster(s)
Disabling using physical measures	
C16	Special means of tracing botmaster(s) abroad
C17	Physically disabling botmaster(s) and/or botnet infrastructure
General measures	
C18	Cooperation and coordination of counter botnet activities
C19	Research on counter botnet activities

V. EMPIRICAL RESULTS

In this section we elaborate further on some of our empirical results. None of the interviewed organisations are actively engaged in removing bots from botnets (C6). NCSC and DefCERT have a general warning and advisory role. They can remove bots from their own networks and solve vulnerabilities in their own computer systems. In some cases, e.g. when a botnet has ➔

TABLE IV. COUNTERACTING AGAINST BOTNETS

Target		Bots	Botnet structure			Botmaster	
Countermeasure		remove bots from botnet	take over or disable command & control server(s)	disrupt botnet with manipulated bots	take over or disrupt botnet by manipulating communication	arrest and prosecute botmaster(s)	physically eliminate botmaster(s) or infrastructure
Command structure							
Centralised		4	2			4	4
Decentralised		4		2	2	4	4
Complex/ hybrid		4		2	2	4	4
Intention of botnet							
A	cyber vandalism	4	4	4	4	2	
B	crime over internet	4	4	4	4	2	
C	cyber crime	4	4	4	4	2	
D	hacktivism	4	4	4	4	2	
E	cyber terrorism	4	4	4	4	2	2
F	cyber war	4	4	4	4		2
Capability							
C1	active detection	2	2	2	2	2	2
C2	passive detection	2	2	2	2	2	2
C3	examine malware	2	2	2	2	2	
C4	investigate botnet		2	2	2	2	2
C5	encryption		3	3	3	3	3
C6	remove malware	1					
C7	take over server		1				
C8	manipulate bots			1			
C9	disrupt channels				1		
C10	take over channels				1		
C11	trace on internet		2		3	2	2
C12	trace botmaster					1	
C13	seize server or NTD		1			3	
C14	safeguard evidence					1	3
C15	arrest botmaster					1	
C16	detect abroad						1
C17	disable physically						1
C18	cooperate/coordinate		4	4	4	4	4
C19	research	4	4	4	4	4	4

1: primarily required capability
2: necessary capability
3: more or less necessary, depending on circumstances
4: general capability

TABLE V. ORGANISATIONS, CAPABILITIES AND LEGAL AUTHORITY

Organisation		NCTV	AIVD	OM	Police	MIVD	Armed Forces	ISPs	Security companies	Vital sectors	Non-vital sectors	Universities
Intention of botnet												
A	cyber vandalism			2	2		a	2	2	5	5	
B	crime over internet		3	2	2		a	5	2	5	5	
C	cyber crime	2	3	2	2		a	2	2	2	5	
D	hacktivism	2	2	2	2	2	a	5	2	2	5	
E	cyber terrorism	2	2	2	2	2	2	5	2	2		
F	cyber war	3	2			2	2	5	2	2		
Capability and legal authority												
C1	active detection	6	2	c	2	2	b	5	2	6		
C2	passive detection	2	2		3	2	2	2	3	2	5	
C3	examine malware	6	2	c	2	2	b		2	6		
C4	investigate botnet		2	c	2	2	b		4	5		
C5	encryption		1	c	2	1	b		4			
C6	remove malware		2			2	2	2	3	2	5	
C7	take over server				2		e	5	4	5		
C8	manipulate bots						e					
C9	disrupt channels	5			4		e	2	3	2		
C10	take over channels						e					
C11	trace on internet	2	2	c	4	2	e	2	6	2		
C12	trace botmaster		2	c	1	2	f		2			
C13	seize server or NTD	5		c	1		f	2	5	5	5	
C14	safeguard evidence	5		c	1		f	3	3	3		
C15	arrest botmaster			1	1		f					
C16	detect abroad		3			3	b					
C17	disable physically						1					
C18	cooperate/coordinate	2	5	2	2	5	2	5	3	5		
C19	research	5	5	d	d	5	d	5	2	5		2

1: primary or exclusive capability
2: independent capability
3: capable but requires explicit authorization
4: capable but no legal authority
5: uses capability of other parties
6: either 2 or 5

a: capability of KMAR
b: capability of MIVD
c: capability of OM but carried out by police
d: independent research
e: either a or 2
f: either a or 3

been taken over by the police, affected users are informed that their computer has been compromised.

A command & control server can be taken over (C7) or physically secured (C13) by means of confiscation, a 'notice-and-take-down' (NTD) procedure or 'hacking back'. Confiscation and NTD procedures are only applicable to botnets with a command & control server located within the Netherlands. Hacking back is strictly speaking illegal, although the OM has authorised the police to hack back in some cases when this was considered proportional in view of significant damage or infringement. Alteration of the law is currently being considered to regulate this. Hacking back can only be applied lawfully by public governmental organisations, because of proportionality assessment and accountability. This applies not only to taking over botnets (C7), but strictly speaking also to milder forms of data collection where still some degree of interference in a botnet is required (C4).

Also private computer security companies and other governmental organisations are capable of hacking back, but are not authorised to do so lawfully. Private parties however are eager to actively counter botnets to protect their own interests.

They consider that actively disrupting botnets is becoming more effective than increasing investments in computer security.

Disrupting a botnet by manipulating bots (C8) is to some extend effective for botnets with a decentralised command structure. However, the knowledge and resources required for applying this capability are still very limited, mainly since most botnets still apply a centralised command structure.Disrupting a botnet by manipulating communication on command & control channels (C9) is applied in private networks or in cooperation with ISPs by means of sink holing in which case bots are made unreachable in a network by blocking IP-ports or DNS manipulation. Taking over a botnet by manipulating communication on command & control channels (C10) is applied by none of the organisations.

Arresting and prosecuting a botmaster (C15) are major tasks of OM and police. The botmaster can either be someone who technically controls the botnet or who hires the botnet. The studied organisations cooperate in a limited number of structural partner-

ships, such as the relation between OM and police, international requests for legal assistance, the execution of court orders to take a command server offline, and contingency capabilities that DefCERT provides to NCSC. These are in fact legal forms of cooperation in the cyber domain that are no different than for other domains. Other forms of cooperation are largely bilateral, project-based or ad hoc, while all organisations are highly interdependent. This is evident since on the one hand authority to use some critical capabilities relies solely with the government, especially for far-reaching research into a botnet and taking over a server, while on the other hand the government needs the knowledge and direct cooperation of many ISPs, computer security companies and companies in vital sectors. The exchange of timely and accurate information is crucial for disrupting botnets, as well as alignment of interests (for instance, whether priority is with shutting down the botnet to minimise damage or with prosecuting the botmaster). All interviewees agree that, given the large number of organisations involved, the current multilateral partnerships are necessary, where every organisation is able to fulfil its own role. This multilateral cooperation is based on trust and recognition of mutual interests and arranged by (inter)national working groups and liaison officers. The NCSC plays an important role in coordination. Most organisations are evolving from the current situation in which they mainly react to botnets that are discovered by circumstances, to a more pro-active attitude in which they actively detect, track and counteract botnets.

VI. CONCLUSION

We conclude that relatively simple botnets can currently be countered effectively in the Netherlands. However, no single organisation is solely capable or has the required legal authority to effectively counteract botnets, and therefore organisations cooperate in structural and ad hoc ways. Capabilities and legal authority are missing to counter botnets with more complex command structures, or with botmasters or botnet infrastructure residing outside the Netherlands.

None of the studied organisations can take over or disrupt complex botnets by manipulating bots or communication in the botnet. Only the OM can authorise for hacking back, because of proportionality assessment and accountability. The government holds the monopoly on the use of some essential capabilities such as manipulation of communication and taking over a command & control server to take over a botnet. This situation may cause that the current cooperation between governmental and private organisations may be difficult to sustain in the long term, if the government is unable to raise enough resources to use its exclusive authority to counter all botnets.

For further research, we recommend to study under which circumstances private organisations might be allowed to apply 'digital self-defence', and to set up a government controlled operational framework for cyber defence in which public and private organisations structurally cooperate and contribute to counter botnets activities, each in line with their core business.

ACKNOWLEDGMENT

We kindly thank the interviewees from the National High Tech Crime Unit, the National Coordinator for Counterterrorism and Security, the National Cyber Security Center, the Public Prosecution Service, Fox-IT, and DefCERT for their cooperation. ➔

Over de auteurs:

Dr. ir. Harald Vranken is universitair hoofddocent aan de Faculteit Informatica van de Open Universiteit.
Hij doet onderzoek op het gebied van security in gedistribueerde systemen.

Majoor drs. Timo Schless is werkzaam als officier elektronica bij de Koninklijke Luchtmacht. Hij heeft bij genoemde faculteit afstudeeronderzoek gedaan naar de organisatie van de bestrijding van botnets. Dit artikel is gebaseerd op dat onderzoek.

REFERENCES

[1] D. Bleaken, “Botwars: the fight against criminal cyber networks,” Computer Fraud & Security, vol. 5, pp. 17-19, 2010.

[2] D.D. Clark and S. Landau, “The problem isn’t attribution: it’s multi-stage attacks,” Proceedings Re-Architecting the Internet Workshop, p. 11, 2010.

[3] D. Dagon, G. Gu, C.P. Lee, and W. Lee, “A taxonomy of botnet structures,” Proceedings Computer Security Applications Conference, pp. 325-339, 2007.

[4] M.J.G. van Eeten, H. Asghari, J.M. Bauer, and S. Tabatabaie, “ISPs and botnet mitigations: a fact-finding study on the dutch market,” TU Delft, 2011.

[5] V.C. Estrada and A. Nakao, “A survey on the use of traffic traces to battle internet threats,” Prcoceedings International Conference on Knowledge Discovery and Data Mining, pp. 601-604, 2010.

[6] G. Fedynyshyn, M.C. Chuah, and G. Tan, “Detection and classification of different botnet C&C channels,” Autonomic and Trusted Computing, vol. 6906, pp. 228-242, 2011.

[7] D. de Graaf, A.F. Shosha, and P. Gladyshev, “BREDOLAB: shopping in the cybercrime underworld,” International Conference on Digital Forensics & Cyber Crime, 2012.

[8] C. Li, W. Jiang, and X. Zou, “Botnet: survey and case study,” Proceedings International Conference on Innovative Computing, Information and Control, pp. 1184-1187, 2009.

[9] J. Liu, Y. Xiao, K. Ghaboosi, H. Deng, and J. Zhang, “Botnet: classification, attacks, detection, tracing, and preventive measures,” EURASIP Journal on Wireless Communications and Networking, article no. 9, 2009.

[10] S. Liu, J. Gong, W. Yang, and A. Jakalan, “A survey of botnet size measurement,” Proceedings International Conference on Networking and Distributed Computing, pp. 36-40, 2011.

[11] T.T. Lu, H.Y. Liao, and M.F. Chen, “An advanced hybrid p2p botnet 2.0,” World Academy of Science, Engineering and Technology, vol. 57, pp. 595-597, 2011.

[12] L. Mendonça and H. Santos, “Botnets: a heuristic-based detection framework,” Proceedings International Conference on Security of Information and Networks, 2012.

[13] Ministry of Security and Justice, “National Cyber Security Strategy 2: from awareness to capability,” 2013.

[14] NCSC, “Cybersecuritybeeld 2013, CSBN-3,” Nationaal Cyber Security Centrum, Ministerie van Veiligheid en Justitie, 2013.

[15] N.C. Paxton, G. Ahn, and M. Shehab, “MasterBlaster: identifying influential players in botnet transactions,” Proceedings Computer Software and Applications Conference, pp. 413-419, 2011.

[16] R. Puri, “Bots & botnet: An overview,” SANS Institute, 2003.

[17] N.S. Raghava, D. Sahgal, and S. Chandna, “Classification of botnet detection based on botnet architechture,” Proceedings International Conference on Communication Systems and Network Technologies, pp. 569-572, 2012.

[18] M.A. Rajab, J. Zarfoss, A. Terzis, and F. Monrose, “A multifaceted approach to understanding the botnet phenomenon,” Proceedings SIGCOMM Conference on Internet Measurement, pp. 41-52, 2006.

[19] T. Schless, “The organisation of counter botnet activities in the Netherlands”, MSc thesis, Open Universiteit, 2013.

[20] B. Stone-Gross et al., “Your botnet is my botnet: analysis of a botnet takeover,” Proceedings Conference on Computer and Communications Security, pp. 635-647, 2009.

[21] M.A.D Tettero and P. de Graaf, “Het vijfde domein voor de krijgsmacht: naar een integrale strategie voor digitale defensie” (in Dutch), Militaire Spectator, vol. 179, no. 5, pp. 240–248, 2010.

[22] A.K. Tyagi and G. Aghila, ”A wide scale survey on botnet,” International Journal of Computer Applications, vol. 34, no. 9, pp. 10-23, 2011.

[23] P. Wang, B. Aslam, and C.C. Zou, “Peer-to-peer botnets: the next generation of botnet attacks,” Electrical Engineering, pp. 1-25, 2010.

[24] P. Wang, S. Sparks, and C.C. Zou, “An advanced hybrid peer-to-peer botnet”, IEEE Transactions on Dependable and Secure Computing, vol. 7, no. 2, pp. 113-127, 2010.

[25] C. Xiang, F. Binxing, L. Peng, and L. Chaoge, “Advanced triple-channel botnets,” Proceedings Conference on Computer and Communications Security, pp., 2012.

[26] S. Yu, W. Zhou, W. Dou, and S.K. Makki, “Why it is hard to fight against cyber criminals?,” Proceedings International Conference on Distributed Computing Systems Workshops, pp. 537-541, 2012.

[27] L. Zhang, S. Yu, D. Wu, and P. Watters, “A survey on latest botnet attack and defense,” Proceedings International Conference on Trust, Security and Privacy in Computing and Communications, pp. 53–60, 2011.

[28] Z. Zhu, G. Lu, Y. Chen, Z.J. Fu, P. Roberts, and K. Han, “Botnet research survey”, Proceedings International Conference on Computer Software and Applications, pp. 967-972, 2008.