enisa
European Network and Information Security Agency

ENISA Position Paper No. 3

Botnets – The Silent Threat

Author: David Barroso (S21sec, Spain)

November 2007

Botnets – The Silent Threat

ENISA Position Papers represent expert opinion on topics ENISA considers important emerging risks or key security components. This paper has been written and reviewed by the group of experts listed below who work in the area of malware analysis.

The paper aims to provide a useful introduction to the rising problem of botnets. It describes the reasons for concern, the infection vectors of bots, the motivation of their creators and expected trends. It concludes with recommendations to policy-makers, providers and end-users on how to counter this serious threat.

Audience

The management summary is aimed at high-level decision-makers seeking a basic understanding of the problem. The remainder of the paper explains the situation in more detail for those who are responsible for IT in public or private organisations.

Table of Contents

Executive Summary	1
Introduction – Botnets are a Big Problem	2
Infection and Distribution Methods	3
The Usage of Botnets	4
Different Roles in Organised Crime	5
Botnet Trends	5
Mitigation is Challenging, but not Impossible	6
Resources to Fight Botnets	8
References	9

Author

David Barroso (S21sec, Spain)

Reviewers

Carsten Casper (ENISA)
Ralph Thomas (Verisign, USA)
Jose Nazario (Arbor Networks, USA)
Ed Skoudis (IntelGuardians, USA)
Alberto Garcia (Guardia Civil, Spain)

Executive Summary

An increasing number of articles in the media discuss the growing criminal activity involving botnets. Bots are little programmes that are installed silently without any user intervention. A botnet is a network of computers on which a bot has been installed, and is usually managed remotely from a Command & Control (C&C) server. The main purpose of botnets is to use hijacked computers for fraudulent online activity; they are managed by a criminal, a group of criminals or an organised crime syndicate.

Once a set of computers has been compromised, they can be involved in many kinds of online criminal activity, including identity theft, unsolicited commercial e-mails, scams and massive attacks. It is estimated that more than 6 million infected computers worldwide are connected to a botnet, with China, the USA, Germany, Spain and France the top five countries for the number of infected computers. Most owners of infected computers do not know that their machines have been compromised.

The criminal organisations behind the implementation of this new online threat are well organised. They employ software developers, they buy and sell infrastructure for their criminal activities and they recruit people (mules) for money laundering to hide their identity. They have the technical resources to continually improve their attacks – conditions that make online frauds more successful than offline ones. (According to an IBM survey [1], three times more Americans think they will be hit by computer crime than real-world crime.) Lack of user security awareness combined with the common habit of using old (sometimes pirated) and unpatched operating systems increase the success of criminal exploitation.

Despite initiatives by Internet Service Providers (ISPs) to control botnet traffic flowing in their networks, better solutions are needed to tackle and resolve this growing issue. Botnets usually involve computers from several countries, making tracking more difficult. Close co-operation between multi-national law enforcement agencies, and between ISPs and private companies is essential.

Internet users, often the least informed in the computer security chain, are the weakest link in solving the botnet problem. While the warning not to open e-mail attachments from unknown sources slowly sinks in, most users are completely unaware that clicking on a malicious web link is often sufficient for an infection. Browser exploits already account for two thirds of all infections. Education of everyday users in the detection of malicious activity in their computers and the prevention of any anomalous action that leads to computer infection is crucial.

The study of botnet attacks has shown an evolution of criminal technologies, and the trends are not encouraging. The objective of criminals is twofold:

- to infect as many users as possible (by using new propagation techniques such as instant messaging or Bluetooth, and by extending infection to mobile devices and media centres) and
- to increase stealth (by using rootkit technologies and covert channels, and by resisting blockage attempts or eradication through the use of peer-to-peer communication or polymorphic malware).

A significant effort from private and public stakeholders in the information society is necessary to counter this threat. The legal basis for prosecution of cyber crime must be improved, especially in relation to cross-border scenarios. Co-operation between law enforcement agencies and communication service providers has started, but there is a need for more structure and more resources. User awareness programmes must continue and should be adjusted to this changing threat. Technical co-operation among providers exists, but must be extended to more (especially smaller) providers, and to more countries. Continuous investment to improve the security of operating systems and application software is also required.

Botnets represent a steadily increasing problem threatening governments, industries, companies and individual users with devastating consequences that must be avoided. Urgent preventive measures must be given the highest priority if this criminal activity is to be defeated. Otherwise the effect on the basic worldwide network infrastructures could be disastrous.

Introduction – Botnets are a Big Problem

An accurate calculation of the amount of bot activity is made difficult by its worldwide nature; however, between 1.000 [2] and 2.000 [3] different botnet Command & Control (C&C) servers are known to be up and running every day; each botnet C&C has an average of 20.000 compromised computers (bots): some C&C servers manage just a few infected computers (~10), large ones manage thousands of bots (~300.000).

In the first semester of 2007, the security company Symantec reported [4] an average of 52.771 new active bot-infected computers per day, with a total of 5.029.309 distinct bot-infected computers at the time of the report. China, the USA, Germany, Spain and France are the top five countries with the most infected computers. Focussing on a specific country, Spain, for example, INTECO [5] (a Spanish government institution related to security) detected over 5 million Peacomm infection attempts targeting Spanish companies during the first half of 2007. (Peacomm is the malicious code responsible for the infamous Storm botnet). The number of bots in the Storm botnet is unknown but it is suspected to be more than 1 million [6].

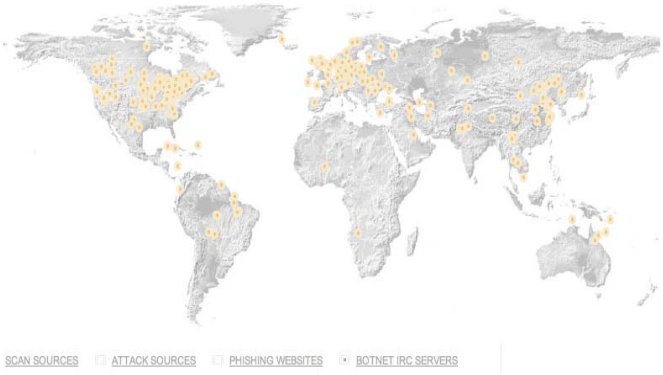

Figure 1: Botnet Internet Relay Chat (IRC) Servers Map
(Source: Arbor Networks, http://atlas.arbor.net)

Belonging to a botnet affects not only the infected computer (with spam, identity theft etc.), but also the resilience of the network infrastructure itself.

Firstly, identity theft figures are alarming; in a recent botnet incident, S21sec recovered more than 20.000 unique users and passwords from a popular webmail provider.

Secondly, a Distributed Denial of Service (DDoS) attack can have a sustained upload bandwidth of 40Kb/s as an average from each bot (a relatively small botnet of 10.000 machines can overwhelm most companies, and a large botnet might be able to take out a fair-sized ISP; the Arbor Networks' VB 2006 paper [7] shows that half of the tracked botnets launched at least one DDoS attack).

Finally, a spam bot can send up to three spam e-mails per second (259.200 e-mails per day). Other side effects include, for instance, the malfunction of Internet infrastructures (routing devices, Domain Name Server (DNS) etc.) due to the high traffic generated by the above.

Malware classification

Virus: a programme that can copy itself and infect a computer without permission.
Worm: a self-propagating piece of malicious software that spreads on a network.
Trojan: a destructive programme that masquerades as a benign application.
Bot: a programme used for the co-ordination and operation of an automated attack on networked computers.
Rootkit: a set of programmes that work to subvert control of an operating system from its legitimate operators by making changes to the underlying operating system itself.
Spyware: a programme installed surreptitiously to intercept or take partial control over the user's interaction with the computer.
Backdoor: a method of bypassing normal authentication obtaining covert access to a computer, while attempting to remain undetected.
Downloader: a programme that downloads and installs malicious software.
Adware: a package that automatically displays or downloads advertising material to a computer.
Ransomware: a type of malicious code that encrypts the data belonging to an individual on a computer, demanding a ransom for its restoration.

One of the key issues is the people behind this new threat. Malicious code authors used to be smart people eager to learn new techniques and show off their skills in what they regarded as a romantic scenario. However, some years ago, criminal organisations realised how powerful the Internet is for committing online fraud, and they invested huge resources. They learned to take advantage of the Internet's weaknesses and to exploit these for their own profit. Some anti-virus vendors like Kaspersky [8] even admit that they struggle with the vast number of new malicious code samples that arise each day. A huge percentage of all e-mail is now

spam (according to Postini's Annual Communications Intelligence report [9], 94% of all e-mail in December 2006). More than 30.000 malicious websites appear every day, trying to infect their visitors (Sophos [10]). A recent analysis [11], carried out by Google, revealed that about 10% of the analysed URLs were malicious (in a sample of 4.5 million URLs). This indicates a major problem that is not going away.

Some studies claim that the extent of online fraud is around three times greater than offline fraud. This 'new' fraud includes credit card fraud, theft in online banking, illegal pharmacies, scams, cyber squatting, fraud in online auctions and malicious code.

Infection and Distribution Methods

The probability of being infected depends on several factors: most of the infection vectors work by exploiting a vulnerability in the victim's computer. Unfortunately, a large number of people still run old operating systems or software applications, or unpatched versions of these. Such computers are more likely to become infected. Another factor is the lack of layered security, i.e. the number of layers implemented in both a network and a computer (anti-virus, IDS, firewalls etc.). The final factor is a lack of user awareness – the uninformed user is the weakest link.

The most common infection methods detected by S21sec include browser exploits (65%), e-mail attachments (13%,) operating system exploits (11%), downloaded Internet files (9%) and other methods (2%), as illustrated in the figure below.

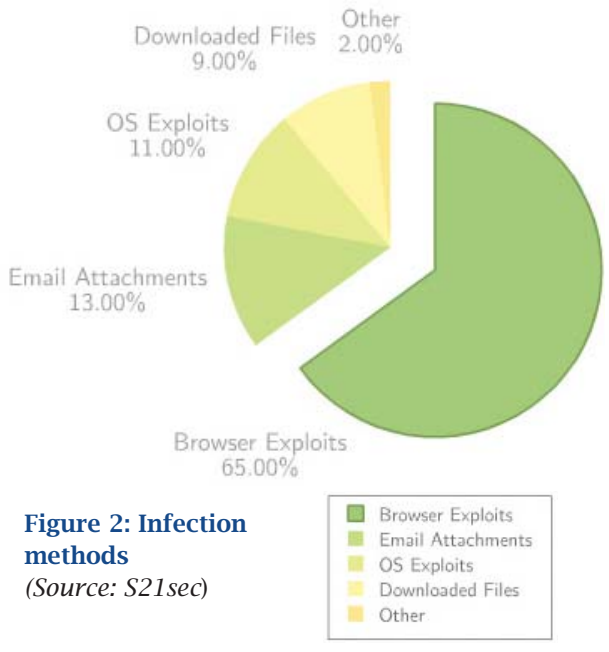

Figure 2: Infection methods
(Source: S21sec)

What is the relationship between vulnerabilities and botnets? Exploiting a vulnerability is just the first step in the malicious code lifecycle. Once a vulnerability has been exploited in a computer, it usually downloads a malicious binary from the Internet and executes it locally (second step). Then, this new process connects to its C&C server to notify its master that the computer is compromised and ready to take orders (last step).

The type of vulnerability that is exploited depends on the malicious code family. Some well known malicious codes such as Blaster, Slammer, Sdbot, Agobot etc. rely heavily on exploiting operating system vulnerabilities, typically services exposed to the Internet (e.g., Microsoft LSASS (CVE-2003-0533), DCOM (CVE-2003-0352) etc.). Another type of vulnerability that is commonly exploited is the targeting of browsers and their plugins (Flash, Java etc.).

Currently the largest botnet is the Storm botnet, which uses a mixed method of social engineering via an enticement, 'lure' e-mail, browser exploit and malicious file download. It is estimated that more than 60% of the exploits related to botnets are browser exploits.

An important issue is that, even with a fully patched operating system, exploits appear in the wild that do not yet have a proper patch from the vendor (i.e., a zero day exploit). In this situation, we need to rely on other security layers because we are vulnerable to that new exploit. Back in April 2007 a popular exploit kit (known as MPack), which is responsible for malicious code delivery, included an ANI (animated cursor) exploit that targeted Microsoft Windows computers three days before Microsoft released the patch.

In addition, it is fairly easy to set up the necessary infrastructure to support a botnet:

1. **Malicious code:** one can freely download from the Internet bots with advanced features. For instance, the Agobot source code was released under GPL (General Public License) and includes: DDoS attacks, remote update, port scanner, information harvesting, rootkit, keylogger and a polymorphic engine to evade anti-virus detection.

2. **Exploits:** the Agobot contains some exploits to infect other computers or different tools to guess passwords for some services like telnet or network shares in an automated brute-force manner. Furthermore, in some forums, attackers can buy exploit kits (like MPack or WebAttacker) for less than US $1000.

3. **C&C site:** usually the available botnet kits include C&C software, which typically is a modified Internet Relay Chat (IRC) server, or a multipurpose web console that needs a LAMP (Linux, Apache, MySQL, PHP) environment.

There are different infection methods depending on the type of malicious code described above. As we have seen, one of the main aims of a botnet is to massively infect as many computers as possible, meaning that they will use any infection vector that will infect the greatest number of computers.

The following are the most common methods of bot infection:

- **Client applications vulnerabilities:** exploiting security bugs to download and install a malicious programme (by using a downloader). Most targeted client applications include browsers (Internet Explorer, Firefox, Opera etc.) but also popular applications such as Microsoft Word, Excel, PowerPoint, Outlook, Acrobat Reader, WinZip, …
- **Exploiting network services:** undertaking massive scans of local or same subnet IP addresses to exploit network services (RPC, MSSQL etc.)
- **Network shares:** looking for unsecured computers (default passwords, public shares) in nearby networks (classic behaviour for some worms and viruses)
- **Spam or unsolicited e-mail:** sending e-mail with malicious code attachments, or sometimes with just URL links that hide a browser exploit. This can also be observed in Instant Messaging (IM) networks (MSN, Skype, Yahoo, AOL, Google Talk etc.)
- **P2P (Peer-to-peer):** tricking users into downloading and executing fake programmes from P2P networks (both commercial and open source)
- **Other common methods:** asking for a codec installation needed to watch a video, fake anti-spyware programmes that are malicious, network acceleration programmes, …

Currently, the most dangerous infection method is when users surf to an infected webpage. Attackers compromise a public web server (e.g., bank, travel agency, famous person's homepage etc.) and inject a tiny html code (iframe) in its main page, to try to exploit a vulnerability in their visitors' browsers.

The Usage of Botnets

The motivation behind setting up a botnet has changed in the last few years; the people behind this threat are no longer teenagers playing games, but experienced criminals involved in online fraud and illegal activities. Why are such people interested in controlling so many computers?

- **Distributed Denial of Service attacks (DDoS):** the average number of bots inside a botnet is 20.000. It is also very common to control several botnets from the same attacker, so the consequences of launching a DDoS against a company or government can be devastating. There may be different reasons behind these attacks: attacks against competitors, attacks from a political motivation (as in the recent case against Estonian government sites) or just to attack a security organisation that is looking into the attacker's interests (recent cases include the CastleCops website, a site which focuses on fighting malicious code, or 419eater.com that fights scams – both of which were targeted by the Storm botnet).
- **Online fraud:** each infected computer in the botnet (also called a zombie) sends significant personal details to a C&C central server: online login credentials (for banks, intranet applications, webmail, online services, social web pages – see also ENISA's Position Paper [12] on threats in Social Networking), stored personal information [13] [14] [15] (e.g. mail credentials, browser auto completed forms, certificates etc.) and all kinds of exploitable information (such as installed programmes' serial numbers, online gaming credentials etc.), which is then used to transfer money, buy or sell goods or for money laundering.
- **Further stealth attacks:** often, the zombie computer has a backdoor installed, allowing the attacker to use the computer as a proxy to hide his actions. In fact, sometimes they share two different ports; one for web proxy access (proxying HTTP connections) and the other one for SOCKS access (proxying IRC, SSH and other connections).
- **Spam:** by using the thousands of controlled zombies to send spam, it is almost impossible to track down the source. Frauds related to spam can be: scam, illegal pharmacy sites or the fraud known as 'pump-and-dump' (or 'stock spam'), involving the use of false or misleading statements to hype stocks, which are 'dumped' on the public at inflated prices (see also ENISA's survey of anti-spam measures [16]).

- **Malicious code distribution:** the zombie computer is used for distributing malicious code and attempts to infect new bots.

- **Click Fraud:** malicious software is installed in the infected computer to automatically click on specific Internet banners or advertisements.

- **New business models:** the entire infrastructure can be rented or sold. Attackers rent these proxies or SOCKS to other people, or just sell the collected personal information to other criminal groups.

Different Roles in Organised Crime

In the last few years, the efficiency of the criminal organisations behind most botnets has been apparent, translating their real life hierarchical and organisational structure to the online world. The structure of these organisations is distributed over several countries, and they have militants in every country where they have interests. However, at the moment there are very few connections between distant organisations (e.g., botnet activity in South America seems to be unconnected with botnet activity in Europe). Based on our observations, we can locate organisations behind botnet activities in a number of specific areas of the world (e.g., Brazil, the US, Russia and some Eastern European countries, Hong Kong and China), although sometimes it is the same criminal organisation which is behind the malicious activity in different countries.

The structure of each organisation appears to be quite similar, including a number of common roles:

- **Pen-testers:** look for vulnerabilities that could be exploited to infect computers. It is also very common to buy a new vulnerability (zero-day). Pen-testers are also responsible for searching vulnerable web servers (typically, open source content management systems, PHP scripts, CGI scripts, …) where they can inject their malicious payload (iframe).
- **Network and system administrators:** botnet architectures are gaining in complexity. Load balancing or reverse proxies are commonly used in the C&C servers, as well as other security technologies like Virtual Private Networks (VPNs), firewalls or ciphered communications. The set-up may also often include Linux operating systems, Apache web servers and PHP scripts that need to be properly installed and configured.
- **C&C developers:** all the different features in the C&C are usually coded using existing IRC daemons or PHP, but sometimes they require other languages to implement, for instance, log search using Perl or obfuscation to their web exploits using JavaScript.
- **Malicious code developers:** have an in-depth knowledge of operating system internals (both Windows and Linux, although Windows is the most commonly targeted operating system). Sometimes they need developers with experience in kernel development if they are implementing or modifying a rootkit.
- **Herders:** look for people (usually by e-mail) who will help in the final tasks of the fraud (mules).
- **Mules:** transfer money and ship on high value goods that have been fraudulently obtained in one country, usually via the Internet, to another country.
- **Spammers:** send a large volume of spam related to different steps in the fraud, and help herders to attract more victims, phishing e-mails etc.

Of course, many of the roles described here are not permanent in the organisation, such as hiring an independent coder to develop a new malicious code or perhaps buying an exploit kit (e.g. MPack, Icepack, WebAttacker, Nuclear Kit etc.) instead of developing it. The entire scenario is currently sold as an underground service [17] [18] [19].

Botnet Trends

As we have seen over the last few years, botnet features have been changing with new infection methods and new usages, and they will keep adapting to new emerging technologies. For instance, there are currently worms that use Instant Messaging (IM) networks like MSN or Skype to distribute themselves, but there are also worms that distribute themselves by using MMS (e.g. Commwarrior) or SMS (although this needs user interaction) and Bluetooth communications. With full-day Internet connections of multiple mobile devices (e.g., BlackBerry, Windows Mobile, Symbian), we might soon see malicious code targeting those devices (a 'mobile devices botnet') as well.

The same occurs with the home devices that are now being connected to the Internet. For instance, some media centre devices now belong to botnets.

Although most ISPs are implementing security measures to protect their customers from infections, the reality is that today many computers do not use static locations (i.e., static addresses or addresses within a specific dynamic range) because they connect to unknown wireless networks (e.g., in

hotels, airports, universities) and use different connection technologies (e.g., 3G, Wireless, Bluetooth, DSL etc.), making the providers' efforts useless.

Another change is the bot's C&C communication. Internet Relay Chat (IRC, see figure 1) was one of the preferred protocols since it was very easy to implement and was able to support the management of thousands of infected computers. IRC is still being used by some botnets, but HTTP is now more widespread, since it is even easier to implement and can be hidden in normal user navigation. (It is easier to detect IRC traffic than to detect malicious HTTP connections within normal HTTP traffic.) The key factor determining the survival of botnets is the use of a protocol that cannot be blocked because it is needed by the infected computer for some legitimate reason. There are other methods of communication that use covert channels (e.g., in DNS, ICMP etc.). Again, such protocols cannot be blocked, but some effort is required by botnet operators to adjust them for their purpose. Moreover, the real menace will be the use of P2P communications – in fact, there is already some malicious code that uses a protocol similar to P2P (such as the Storm botnet, which uses UDP-port 4000 for communication between peers). Such protocol makes closing down C&Cs – which would normally be an effective countermeasure against botnets – useless.

Two examples of botnet complexity are fast-flux networks and Rock Phish. Fast-flux services are a network of compromised computer systems with public DNS records that are constantly changing, in some cases every few minutes. They can also use reverse proxies to redirect the user to another compromised computer, making it harder to track down the attacks. On the other hand, Rock Phish uses compromised computers and thousands of DNS subdomains in order to set up phishing scenarios that hide the real phishing site (Rock Phish is responsible for between one-third and half of all phishing messages being sent out on any given day).

Another trend is the improvement in attackers' security measures. Frequently both the malicious code and the infrastructure that builds the entire scenario are quite simple (e.g., open directories in web servers, the use of weak cryptography, normal packers etc.), suggesting that nobody is analysing them, but this is changing. Now attackers are becoming more cautious in every step they take. When they notice something strange they use public key cryptography, distributed VPN, fast-flux, Rock Phish, PHP encoding, JavaScript obfuscation, kernel packers, covert channels and auto-removal.

Mitigation is Challenging, but not Impossible

The number of botnets recorded in 2007 has increased since 2006 for two main reasons: there are more computers connected to the Internet and, according to Arbor Networks' research, just as the good guys hear more about botnets, so more bad guys become interested. It is a growth industry. At the same time, there is no clear sign of a rise in user awareness. People still do not know that their computers are infected and, if they do, they often do not know what to do about it.

All the indicators show that the number of bots and botnets will keep growing if we do not face up to the problem and mitigate both the non-technical and the technical factors that are the pillars of these threats.

Non-technical and Technical Factors Supporting Botnets:

- Non-technical:
  - Distributed environment: each botnet may involve several countries
  - Covert channels: the use of compromised hosts
  - Legal issues: laws are different in each country
  - Low user awareness: users are unconcerned about it
- Technical:
  - Insecure software and bad patching habits
  - Passive ISP: they are not responsible for the security of their customers' operating systems (antivirus software, patches etc.)
  - Improper ingress and egress filtering: blocking inbound and outbound malicious users' connections (spam, malicious code, attacks etc.) is often in conflict with blocking normal, benign user traffic

The solution to the non-technical problems can be divided into three different initiatives, depending on the actors: Government, law enforcement agencies and private companies, and the end-user.

Recommendations – Non-technical

- **Rec. Bot. 1 – Involving the Government –** whether botnet activity is punishable depends on the precise activity and on the law that can be applied. Agreement is needed within the EU and beyond to prosecute cyber crime in a consistent and co-ordinated way (for example in line with the European Convention on Cybercrime, which has still not been ratified by all signing countries). Too few decision-makers are sufficiently aware of the extent of the botnet problem and the consequences of inaction.

Steps should be taken to raise awareness among political decision-makers about the severity of the botnet problem.

- **Rec. Bot. 2 – Better co-operation between law enforcement agencies and private companies** (ISP, financial entities, security companies etc.), working for a better dialogue and helping each other to detect, prevent and react to botnet incidents. Government Computer Emergency Response Teams (CERTs) are a valuable first point of contact, perhaps with ENISA acting as an additional focal point for long-term co-ordination and the sharing of best practice. A dialogue has been initiated among individual bodies (especially law enforcement agencies and providers), but it could be improved, for example with the establishment of working groups and workshops at the European level. The option of a permanent body to fight cyber crime in Europe should be discussed.

Co-operation between law enforcement agencies and private companies should be improved.

- **Rec. Bot. 3 – User awareness** – everyone who uses a computer connected to the Internet should know and understand the threats that could affect him/her. Proper education about security measures should be included in school curricula, in public service announcements on television and the Internet and other awareness raising initiatives.

The education of users about botnet threats should be extended.

Recommendations – Technical

- **Rec. Bot. 4 – Secure operating systems and software applications** – vendors should make strenuous efforts to increase their products' security and, for example, improve the update and patch management process. Investment should be encouraged, with public and private funding for secure software development.

Vendors should continuously improve the security of their products.

- **Rec. Bot. 5 – ISP co-operation** – ISPs are key to the solution, since they can detect and block botnet communication. Of course they would need to inspect the user's traffic, which could lead to privacy issues. Guidance on this from a privacy authority would be welcome, similar to the Article 29 Working Parties' opinion 118 on e-mail filtering [20].

Guidance should be provided on the extent to which ISPs can inspect users' e-mail traffic to detect and block botnet communication.

- **Rec. Bot. 6** – Law enforcement agencies could be given the capability to clean botnets, but this would be an extreme measure. Almost any botnet can upload and force all its zombie computers to execute a specific programme. This programme could be a malicious code removal tool that uses the same technology for good purposes. However, given the privacy implications and potential side-effects, this should not be considered an option at this time.

Policy-makers should monitor the threat of botnets closely. If the problem worsens, they should consider whether forced removal of bots might be an option, assuming that privacy issues and potential side-effects are resolved.

The Detection of Botnets

Botnets can be detected; there are a variety of different approaches:

1. **At ISP level:** Some products analyse DNS queries to detect whether a computer has been infected by malicious code. Although this approach seems to be a valid one, the truth is that it might be useful but it is not the final solution. Analysing DNS traffic to detect zombie computers that are attempting to connect to their C&C is only useful if the C&C is already known (in the same way that signature-based intrusion detection or anti-virus software also needs to have a record of which traffic is known to be bad), but:
   - DNS traffic analysis does not detect unknown C&C panels
   - Some C&C panels connect directly to an IP address instead of a domain name
   - Some C&C panels are hosted in compromised computers with an authentic domain name.

Then, in order to detect botnet traffic, in a similar way to anti-virus software or intrusion detection systems, ISP administrators need to combine a signature-based method (e.g. based on DNS or HTTP) with a heuristic one, for instance with a flow-based method (analysing where the user is connecting), which looks for anomalous connections.

2. **At LAN level:** as many worms try to infect nearby computers in a local area network (LAN), a local honeypot (a computer system set up as a trap for attackers) could help with the early detection of any malicious software that is trying to infect all the computers in an organisation. Local administrators play a key role since they can detect an infection and take appropriate action. Cooke [21] and Riordan [22] shed some light on detecting and disrupting botnets.

3. **At computer level:** there are some hints as to whether malicious code is running on a computer:
   - Strange process names
   - Slow connection to the Internet (the computer could be sending spam or participating in a DDoS attack)
   - Strange browser behaviour (home page change, new windows appearing on the screen)
   - Anti-virus software seems not to be running
   - Strange programme filenames added to the list of programmes that are allowed to access the Internet
   - Changes to the computer's *hosts* file
   - Strange files in the startup programmes
   - New Browser Helper Objects (plug-ins) added to the Internet Explorer browser, or malicious extensions added to Firefox browsers
   - Strange Windows services
   - Unknown network connections established in the computer

All these give-away signs are only valid if the computer has not installed a rootkit, because a rootkit will hide all the above indicators to enable it to survive in the system without being detected. There are, however, special software tools (rootkit detectors) that help to uncover the existence of rootkits on infected machines.

Resources to Fight Botnets

There are some websites that provide further reading about botnets basics:
- Wikipedia: Botnet [23]
- The Honeynet Project: *Know your Enemy: Tracking Botnets* [24]
- Microsoft: *Zombies and botnets: Help keep your computer under your control* [25]
- CastleCops [26]
- ShadowServer Foundation [27]
- SANS Internet Storm Center (ISC) [28]

There are several websites that can analyse binaries files (Windows PE, the Windows executable binary format) in order to ascertain whether a specific binary sample is malicious or not. It is important to check that the analysis systems are real computers and that they are not using virtual software (VMware, VirtualPC, Parallels etc.) since many malicious code samples can detect that they are running in virtual environments and do nothing.

The analysis may be incomplete if the malicious code is using a rootkit to hide its actions so, as a general rule, users or administrators should invest in malicious code analysis only if they can justify the resources. Otherwise, they should leave it to the experts.

Additional online resources that analyse a malicious code sample:
- www.cwsandbox.org/
- http://research.sunbelt-software.com/Submit.aspx
- www.norman.com/microsites/nsic/
- www.threatexpert.com/
- http://analysis.seclab.tuwien.ac.at/index.php

There are also other sites that analyse a binary sample against a set of anti-virus tools to discover whether the sample is already known and can be detected:
- http://virusscan.jotti.org/
- www.virustotal.com/

Some of the tools that experts and analysts use to dissect programmes and their actions:
- OllyDbg: a userland free debugger. www.ollydbg.de/
- IDA Pro: an advanced commercial disassembler and debugger. www.datarescue.com/idabase/index.htm
- BinNavi: a debugger based on IDA Pro that uses visualisation. www.sabre-security.com/products/binnavi.html
- PEiD: a packer detection tool. http://peid.has.it/

Other websites related to reverse engineering and botnets:
- OpenRCE: www.openrce.org
- Nepenthes: http://nepenthes.mwcollect.org/
- Offensive Computing: www.offensivecomputing.net/

Commercial products related to botnets:
- Norton Antibot www.symantec.com/norton/products/overview.jsp?pcid=is&pvid=nab1
- Simplicita ZBX (now Sandvine) www2.simplicita.com/product_zbx.html
- Arbor Networks www.arbornetworks.com/index.php?option=com_docman&task=doc_download&gid=10
- FireEye www.fireeye.com/products/index.html

References

[1] IBM Survey: *Consumers Think Cybercrime Now Three Times More Likely Than Physical Crime.* IBM. www-03.ibm.com/press/us/en/pressrelease/19154.wss

[2] *Arbor Networks Atlas.* http://atlas.arbor.net/summary/botnets

[3] ShadowServer Botnet Charts. www.shadowserver.org/wiki/pmwiki.php?n=Stats.BotnetCharts

[4] *Symantec Threat Report Volume XII* (September 2007). Symantec. www.symantec.com/business/theme.jsp?themeid=threatreport

[5] Instituto Nacional de Tecnologías de la Comunicación (INTECO). www.inteco.es

[6] *Just How Bad Is the Storm Worm. Washington Post.* Brian Krebs. http://blog.washingtonpost.com/securityfix/2007/10/the_storm_worm_maelstrom_or_te.html

[7] *Botnet Tracking techniques and tools.* Jose Nazario, Jeremy Linden. www.virusbtn.com/pdf/conference_slides/2006/JoseNazarioVB2006.pdf

[8] *The contemporary antivirus industry and its problems.* Eugene Kaspersky. www.viruslist.com/en/analysis?pubid=174405517

[9] *2007 Postini Communications Intelligence Report.* Postini. www.postini.com/2007report

[10] *Attacks via web and email strip business of cash.* Sophos. www.sophos.com/pressoffice/news/articles/2007/07/toptenjun07.html

[11] *The Ghost in the Browser Analysis of Web-based Malware.* Niels Provos, Dean McNamee, Panayiotis Mavrommatis, Ke Wang, Nagendra Modadugu. www.usenix.org/events/hotbots07/tech/full_papers/provos/provos.pdf

[12] *Security Issues and Recommendations for Online Social Networks,* ENISA Position Paper, 2007 www.enisa.europa.eu/doc/pdf/deliverables/enisa_pp_social_networks.pdf

[13] *The Underground economy: priceless.* Rob Thomas, Jerry Martin. www.usenix.org/publications/login/2006-12/openpdfs/cymru.pdf

[14] *The Economy of Phishing.* A survey of the operations of the phishing market. Christopher Abad. www.firstmonday.org/issues/issue10_9/abad/

[15] *An Inquiry into the Nature and Causes of the Wealth of Internet Miscreants.* Jason Franklin, Adrian Perrig, Vern Paxson, Stefan Savage. www.cs.cmu.edu/~jfrankli/acmccs07/ccs07_franklin_eCrime.pdf

[16] *ENISA Surveys on Anti-spam and security measures of ISPs.* www.enisa.europa.eu/pages/spam/index.htm

[17] *Who's Stealing Your Passwords?* Global Hackers Create a New Online Crime Economy. CIO Magazine. Scott Berinato. www.cio.com/article/135500/Hacker_Economics_Malware_as_a_Service

[18] *Hacker Economics 2: The Conspiracy of Apathy.* CIO Magazine. Scott Berinato. www.cio.com/article/135550/Hacker_Economics_The_Conspiracy_of_Apathy

[19] *Hacker Economics 3: MPACK and the Next Wave of Malware.* CIO Magazine. Scott Berinato. www.cio.com/article/135551/Hacker_Economics_MPACK_and_the_Next_Wave_of_Malware

[20] *Working Party 29 Opinion 2/2006 on privacy issues related to the provision of email screening services.* http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2006/wp118_en.pdf

[21] *The Zombie Roundup: Understanding, Detecting and Disrupting Botnets.* Evan Cooke, Farnam Jahanian, Danny McPherson. www.eecs.umich.edu/~emcooke/pubs/botnets-sruti05.pdf

[22] *Billy Goat, an Accurate Worm-Detection System.* James Riordan, Diego Zamboni, Yann Duponchel. http://domino.watson.ibm.com/library/CyberDig.nsf/398c93678b87a12d8525656200797aca/d7c39a9a2e73d870852570060051dfed?OpenDocument

[23] *Wikipedia.* Botnet. http://en.wikipedia.org/wiki/Botnet

[24] *Know your enemy: Tracking Botnets.* Paul Bächer, Thorsten Holz, Markus Kötter, Georg Wicherski. www.honeynet.org/papers/bots/

[25] *Help keep your computer under your control.* Microsoft. www.microsoft.com/protect/computer/viruses/zombies.mspx

[26] CastleCops. www.castlecops.com

[27] ShadowServer. www.shadowserver.org/

[28] SANS Internet Storm Center (ISC). http://isc.sans.org/

For further information about this Position Paper, contact David Barroso (S21sec) or Alain Esterle (ENISA) at: info@enisa.europa.eu

ENISA – European Network and Information Security Agency
PO Box 1309, 710 01, Heraklion, Crete, Greece
Tel: +30 2810 39 12 80, Fax: +30 2801 39 14 10
www.enisa.europa.eu

01/11_07