



NISCC

NATIONAL INFRASTRUCTURE SECURITY CO-ORDINATION CENTRE

NISCC Briefing 11a/2005 Issued 17 October 2005

Botnets - the threat to the Critical National Infrastructure

This paper has been written to inform the reader of the threat posed to the Critical National Infrastructure by botnets. It will discuss the current scope and scale of the botnet problem, and offer simple mitigation advice. A description of what botnets are and how they work can be found at Annex A.

Reference to any specific commercial product, process or service by trade name, trademark manufacturer or otherwise, does not constitute or imply its endorsement, recommendation or favouring by NISCC. The views and opinions of authors expressed within this notice shall not be used for advertising or product endorsement purposes.

NISCC shall accept no responsibility for any errors or omissions contained within this briefing notice. In particular, they shall not be liable for any loss or damage whatsoever, arising from or in connection with the usage of information contained within this notice.

**National Infrastructure
Security Co-ordination Centre**
PO Box 832
London, SW1P 1BG

Tel: 0870 487 0748
Fax: 0870 487 0749
Email: enquiries@nisc.gov.uk
Web: www.nisc.gov.uk

Key Points

- **Botnets are a distributed attack infrastructure consisting of a large number of compromised computers controlled by a malicious user via a command and control server.**
- **The controller of a botnet can both attack the compromised hosts, and use those compromised computers to launch further attacks on other Internet-connected systems.**
- **Although less than 5% of computers worldwide are likely to contain bots, many botnets are large enough to cause substantial disruption to almost any Internet-connected systems that exist. Potential victims, compromised hosts, command servers and malicious users can reside anywhere in the world.**
- **Current botnet usage trends focus on generating revenue, in particular through distributing spam and adware, stealing personal and financial information, and through extorting money from online businesses.**
- **Traditional threat groups currently lack the intent to utilise botnets to launch serious and damaging attacks against the Critical National Infrastructure. However botnets could be harnessed for this purpose at any time.**

Introduction

“Leveraging the power of several thousand bots, it is viable to take down almost any website or network instantly. Even in unskilled hands, it should be obvious that botnets are a loaded and powerful weapon.”¹

1. Coverage in articles such as the one quoted above have recently raised the profile of ‘bots’ and ‘botnets,’ malicious programmes which have infected thousands of computers across the world. Reports on bot activity have focused on the way in which they have been put to use for criminal purposes, particularly in support of fraud and extortion. However botnets are no more than a tool which any malicious user could bring to bear against any potential target. This paper therefore seeks to assess the threat that botnets pose to the organisations comprising the Critical National Infrastructure (CNI).²

2. The paper draws on open source research into botnets, as well as first hand experience of botnet activity. It will seek to:

- discuss how botnets are currently being used;
- speculate about possible ways in which botnets might threaten the CNI;
- provide an assessment of the threat groups likely to use botnets against the CNI; and
- suggest some ways in which this threat might be mitigated.

3. A description of what a botnet is and how it works can be found at Annex A.

What are the current trends in botnet usage?

4. Investigations into current trends in botnet usage have generally concluded that the majority of botnets are being used to generate revenue for the malicious user or his customers. Some sources suggest that organised crime elements have been instrumental in driving the use of botnets to make money, and press reporting has implicated criminal groups from the ex-Soviet bloc in the botnet-related extortion cases of recent times.

5. Credible reporting on this topic can be hard to obtain, as victims can be unaware that they have been attacked, or may be reluctant to report the attack for fear of the impact on corporate reputations. What is certain is that

¹ *Know Your Enemy: Tracking Botnets*, The Honeynet Project and Research Alliance (<http://www.honeynet.org>)

² Those assets, services and systems that support the economic, political and social life of the UK whose importance is such that any entire or partial loss or compromise could cause large scale loss of life, have a serious impact on the national economy, have other grave social consequences for the community, or be of immediate concern to the national government. See also www.niscc.gov.uk.

there has been a definite shift towards the utilisation of malware for profit across the spectrum of malicious computer use. What started out as a game, with bot controllers overwhelming each others' servers and stealing each others' bots, is now an industry, with controllers being paid to distribute spam, deny service to websites, and steal personal data to facilitate credit card and identity fraud. Some of the currently observed ways in which botnets are being used are outlined below.

Distributed Denial of Service (DDoS)

6. There are various techniques by which botnets are used to deny service to Internet-connected applications:

- Instructing bots to request pages from a website repeatedly, a malicious user can 'flood' a site with so much traffic that legitimate users are unable to connect, or the site crashes or is disconnected by its Internet Service Provider (ISP). DDoS attacks are not limited to websites; in theory a botnet attack could overload any Internet-connected application by sending it a large amount of traffic and entirely consuming the application's connection bandwidth, if its IP address were known.
- This 'blocked pipes' attack could have a knock-on effect, meaning that many related applications would be unable to operate as normal. In May 2004, a DDoS attack targeting several Australian online betting firms disabled the local ISP's platform for over five hours, effectively taking all the platform's subscribers offline for the duration of the attacks.³ In this incident, alleged Russian criminal groups attempted to extort money from the betting companies; however all of the ISP's customers ended up being the victims of the attack.

7. DDoS attacks are not just to extort money from online businesses. They have also been used to inconvenience and embarrass other bot controllers (by launching DDoS attacks against command and control servers), or as a protest tool used to deny access to websites whose ideology differs from that of the malicious user.

Spam (Unsolicited Email), Adware, Proxying

8. Botnets are also particularly useful networks for distributing unsolicited email (spam) and 'pop-up' advertisements (adware). Clearly, a network of many thousands of PCs can distribute more spam than a single computer. In September 2004, Spamhaus⁴ estimated that 70% of all spam email was distributed by botnets.⁵ Furthermore, with a botnet delivering spam, it is the

³ www.adelaideinstitute.org/Australia/022.htm

⁴ www.spamhaus.org

⁵ <http://news.zdnet.co.uk/internet/security/0,39020375,39167561,00.htm>

victim's, not the malicious user's, IP address that the ISP sees; hence the spam will probably get through.⁶

9. In the same way, a bot can hijack the victim's Internet connection, and send malicious emails that appear to come from a 'safe' user. The bot controller is effectively using the victim's computer as a proxy to obscure his involvement in any malicious activities.

Keylogging, 'Packet Sniffing'

10. Some bots contain the functionality to record the victim's keystrokes. The bot program might be coded to start recording only after the user has typed in key words – such as 'bank' or 'Paypal'⁷ – in order to filter the information retrieved. In this way the victim's usernames, passwords, credit card details, etc. can be harvested and used or resold. In a similar fashion, bots can use software to 'sniff' the 'packets' of data the victim's computer sends out over the Internet, often revealing information of the sort detailed above – including licence keys for games and music, and even the details of the other botnets present on the victim's computer.

'Clickthrough'

11. A simple task to which the botnet is often put is forcing the victim's computer to connect to a website and click on a link. This can be for innocuous reasons, for instance in order to increase the controller's score in an online game,⁸ or for profit, such as in the case of the Google Adwords marketing campaign. Under this campaign, companies can pay Google to add adverts to their search results page based on the search terms entered. Bots can be used to search repeatedly for specific keywords without then clicking on the related advert. If enough searches are conducted, the 'clickthrough' rate⁹ of the advert drops, and the Google software automatically disables the adverts, because it seems that they have not been popular or relevant. Security researchers have suggested that companies might pay botnet controllers to denigrate their competition in this fashion.¹⁰

Anonymising proxies

12. Botnets can be used to anonymize any online activity, including malicious activities such as hacking, by providing unattributable 'proxies' for a malicious user. The attacker can use his bots as a series of intermediate stages, sending attack traffic from victim computer to victim computer, each time stripping any information about the previous stage. Attempts to trace the

⁶ If an ISP can identify a user as being a persistent sender of spam or adware, it can list that user's IP address and blacklist him, ensuring that none of that user's email gets through to the ISP's customers. By using compromised computers, 'spammers' can get around this blacklisting.

⁷ A popular online payment service

⁸ Such as 'Outwar,' in which players are rewarded based on the numbers of clicks their character's link receives

⁹ i.e. the number of searchers entering a search term, but the not clicking on the adverts displayed

¹⁰ http://www.theregister.co.uk/2005/02/03/google_adwords_attack/

source of any resulting malicious activity are likely to identify the owners of the compromised computers, rather than the attacker themselves.

Storage of files

13. Malicious users operating botnets can use compromised computers as storage space, hosting pirated software, films and other illegal files. Not only is the illegal material stored on a computer seemingly unconnected to the bot controller, but the storage space is free. Compromised servers with large amounts of free disk space and fast connections will be at particular risk of becoming stores for illegal (and other) files.

Competition

14. Whilst the use of botnets is largely profit-driven, malicious users are still driven to compete with their peers, trying to be the individual with the biggest botnet, with the largest number of compromised victim computers, or able to command the greatest bandwidth for DDoS attacks. Some individuals may create botnets for no reason other than the fact that they can; however it is possible that this tool could be stolen or sold to an individual who will put it to malicious use.

What is the scale of the botnet problem?

15. It is difficult to find accurate and definitive figures on botnets, due to the distributed and anonymous nature of the problem. The HoneyNet Project and Research Alliance (HPRA)¹¹ released a paper¹² containing information captured by monitoring bot traffic situated on one of their bot 'honeypot' computers.¹³ HPRA stated that they were able, using a 'honeynet' of three computers over a period of a few months, to monitor the activities of a little over a hundred separate botnets of varying size and structure. Within this period, the project noted over 225,000 unique IP addresses joining at least one botnet command and control channel. Taking into account the fact that channels can be modified to obscure the number of logged-in users, the HPRA estimate that their figures, taken as a percentage of the entire number of botnets in existence, indicate that there could be in excess of 1,000,000 compromised hosts under the control of malicious users world-wide.

16. It is important to put this figure into context. Even if the figure of 1 million compromised hosts proves to be a gross underestimate, a figure as high as 10,000,000 represents less than five percent of the estimated

¹¹ An international not-for-profit research alliance dedicated to improving Internet security. This paper was produced by the German HoneyNet Project, in connection with researchers from Aachen University.

¹² *Know Your Enemy: Tracking Botnets*, The HoneyNet Project and Research Alliance (<http://www.honeynet.org>)

¹³ A 'honeypot' is a computer which is deliberately exposed to infection, and then monitored to gather information about the attacker.

300,000,000 Internet-connected computer-users worldwide.¹⁴ Moreover the total number of compromised PCs is in fact less relevant than the number of computers under the control of a single malicious attacker. The actual size of each botnet can be hard to establish, due to a number of factors. Not all bots will be logged on to a channel simultaneously, and command may be spread over several IRC servers. Malicious users can obscure the number of bots logged into control channels, making accurate figures difficult to obtain. A computer can also contain more than one bot; if the computer is vulnerable to a widely known exploit, it is likely that it will be compromised by a wide range of malware.

17. The size of botnets may also be changing. Whilst anecdotal evidence suggests the existence of botnets with up to 400,000 hosts, there is some information to suggest that controllers are increasingly opting for smaller, more manageable botnets, which are easier to take care of, and to protect from the designs of other malicious users. As connections to the Internet get faster and the bandwidth of domestic connections increases, the number of hosts malicious users will have to compromise to achieve the same level of throughput for their spam or denial of service traffic will continue to shrink.

18. There is limited information about the geographical distribution of bots and, more importantly, botnet controllers. According to Internet Security firm Symantec's 2005 Internet Security Threat Report, the UK topped the list of countries with the most observed compromised PCs during the latter half of 2004. The US, China and Canada also appeared high on the list of compromised computers. Large numbers of compromised computers in a country might indicate the presence of a high proportion of high-speed, connected but vulnerable computers. In the case of the UK, the high number of bots has been in part attributed to the recent rollout of high speed, always-on broadband services, without a complementary increase in security awareness.

19. It is harder to state the location of the malicious users actually controlling the botnets. Whilst analysis of attacks may reveal the location of compromised computers, and captured bot traffic may help identify the location of a control server, the malicious user can connect to his control server from anywhere in the world, and hence his location cannot always be readily identified. Some reports have linked botnet use to criminal gangs operating throughout the former Soviet Union, where organised criminality is known to flourish.

20. Whilst it is hard to quantify the botnet problem, what is not in doubt is the fact that many malicious users have control of botnets containing a great deal of compromised computers, and which are of a sufficient size to successfully attack almost any Internet-connected application. These bot controllers can exist in any community where there is access to the Internet, technical knowledge, and the will to undertake malicious activity.

¹⁴ <http://www.isc.org/ops/ds/host-country-history.php>

How might botnets be used to threaten the CNI?

21. A botnet is an attack infrastructure, in which the malicious attacker can attack both the compromised hosts, and use those computers to launch further attacks on others. As botnets can be updated and modified at will, the ways in which botnets can be used are limited only by the imagination and technical ability of the malicious user. It is a flexible, distributed and anonymous attack infrastructure which can be harnessed at any time for any number of malicious purposes.

Confidentiality attacks

22. Botnets are already being used to launch confidentiality attacks, using keyloggers to steal personal and financial information from compromised computers. It would also be possible for attackers to use access to compromised computers to obtain sensitive and proprietary data, the loss of which would have an adverse impact on the organisations making up the CNI. Having infiltrated a number of victims' computers, the bot controller could command his bot to scan the victim's hard drive for files. Bots already have the capability to transfer files without the knowledge of the victim, for instance to download executables from websites for malicious purposes. There would be nothing to stop a bot from copying any files it finds and sending them to a controller's server for later retrieval.

Availability (Denial of Service) attacks

23. Whilst none of the sectors of the CNI rely exclusively on an online presence to survive, several sectors could be affected if their or their customers' access to Internet-based connectivity was denied.

- Any system relying on Internet connectivity could theoretically be 'knocked offline' by a concentrated, prolonged DDoS attack. Even systems that are not being specifically targeted by the attacks could be affected, as a sufficiently large botnet could generate enough malicious traffic to overwhelm all but the largest Service Providers' Internet platforms.
- A protracted DDoS attack against a major high street bank's Internet banking services could cause considerable damage to consumer confidence, and to that bank's reputation and profits. A dedicated attack from even a medium-sized botnet has the potential bandwidth to knock a major company's website offline for some time.
- An industrial process control system (used, perhaps, to control the opening and closing of valves on a gas pipeline) issuing commands over an Internet connection could lose the ability to contact, monitor or control a remote control process because botnet traffic is occupying the remote system's bandwidth. The attacker would have to know the IP address of the computer, or of the network on which it is running, but could conceivably overwhelm the system by consuming all the system's available bandwidth. Damage to the CNI would in this situation depend on

the remote system's failsafe processes, and on whether it could be operated manually or via a non-Internet-based fallback system unaffected by the DDoS attack.

- Communications systems relying on Voice over IP (VoIP) would be likely to suffer from a prolonged DDoS attack. Targeted attacks against servers distributing VoIP traffic could cause widespread disruption, depending on the makeup of the infrastructure (distributed or dedicated networks being arguable more robust) and any redundancies in place. A targeted attack on a critical system - for instance a local police communications system in the wake of a physical terrorist attack - would have serious and damaging consequences.
- Any government initiative relying on a reliable and accessible Internet presence, such as an e-voting scheme, NHS online, etc., could be affected by a sustained denial of service attack.
- Electronic systems for the distribution of critical supplies such as food and fuel may rely on automated online processes that could be disrupted by sustained DDoS. Although it is likely that deliveries could be maintained via manual fallback systems, the resulting interruption to, for example, petrol stations and supermarkets, could have serious economic and social consequences.
- If secondary and support services that support the Internet, such as domain name servers and routers were knocked offline, all Internet traffic - including that of CNI sector entities - would be disrupted. It should however be stated that as current trends indicate that the majority of bot controllers rely on the availability of Internet connections to make money, they would be unlikely to want to compromise its operability in any way.

24. It should be stated that it is unlikely that a denial of service attack would permanently compromise a system, and mitigation such as dedicated networks, fallback servers, increased bandwidth, traffic filtering and manual redundancy could reduce the impact of such an attack. However a determined, targeted attack restricting access to critical systems for even a relatively short period could have a serious effect on the state of the CNI.

Traditional electronic attack via botnets

25. Botnets also offer benefits to traditional, computer to computer ('hacking') attacks. The use of individual bots as anonymous proxies has already been mentioned. Malicious users can use a chain of compromised computers to hide their trail, jumping across a series of innocent computers before reaching the victim of their attack. Botnets provide not only anonymity but also persistence; if one bot is recognised as being in the hands of a malicious user and blacklisted by downstream defence systems, the attacker can quickly switch to another computer. Having expendable proxies in this manner might also assist a brute force password attack, as some systems will

refuse connections from an attacking computer after a number of failed attempts to guess its password.

Botnets for sale

26. Traditional threat groups will not necessarily have to develop their own technical expertise to deploy and direct botnets. Botnets are freely traded throughout the 'underground economy,' an informal network of chatrooms, newsgroups and Internet Relay Chat (IRC) servers known to those with an interest in malicious code and online misdemeanours. Some individuals, for a fee, will give you access to their botnet command and control server, in essence 'selling' you the botnet. Others will offer to commit acts of DDoS or spamming on your behalf – just supply the target. In an anonymous environment such as an Internet chatroom, bot controllers are unlikely to have any scruples about the types of people into whose hands these technologies are passing.

Mitigation

27. There are many ways in which a botnet – in essence just another tool in the malicious user's arsenal – could be directed against the CNI with potentially damaging consequences. Malicious users can obtain pre-existing bot code, tailor it to their needs, spread the bot, and then remotely execute almost any series of pre-defined functions on thousands of globally distributed computers. Botnets offer anonymity, can be updated remotely to add extra functionality, and can be used to carry out simple tasks repeatedly on a large scale, or to support more targeted hacking activities. Most importantly, botnets can be bought or hired, meaning that threat actors without advanced technical ability can use them. Given the widespread nature of this threat, what steps can be taken to mitigate the risk posed by botnets and their users?

Mitigation Advice

28. Botnets can only spread if they can locate and compromise vulnerable computer users. It appears that the majority of botnets rely on relatively widespread and well-known vulnerabilities to propagate. Users should be made aware of the threat posed by botnets, and should take actions that will decrease the chances of further computers becoming compromised. These actions should include:

- using anti-virus, anti-spam and anti-spyware products;
- using a correctly configured firewall to allow only the inbound and outbound traffic of services required for home or corporate needs¹⁵;
- keeping all software and hardware products patched and updated;
- avoiding the download of files and programmes from 'untrusted' sources; and
- blocking unusual outbound connections, especially those operating on ports associated with IRC¹⁶.

¹⁵ NISCC Technical Note 10/04 contains advice on choosing and implementing firewalls.

29. Whilst hardening only UK systems against compromise will help to protect British computer users from 'local' threats, such as bots armed with keyloggers and packet-sniffers, this is not a complete solution to the international problem, as compromised computers capable of launching DDoS attacks can reside anywhere in the world. However, by reducing the number of UK computers vulnerable to compromise, malicious users will be forced to work harder to secure resources with which to continue their malicious and criminal activities.

30. As well as hardening their systems against botnets, we would encourage users to report botnet attacks. Successful mitigation relies upon users having an accurate picture of the threat, and the sharing of information about botnet attacks is key to maintaining this picture. Some companies will be reluctant to report attacks, as they fear that they will suffer damage to their reputation if it emerges that their systems are vulnerable to attack; others may choose to handle the incident themselves, or in concert with their ISP. However incidents of attacks which can be recognised as utilising a botnet need to be reported so that the overall assessment of the threat posed by botnets can be kept current. Clearly attacks with a criminal motivation, such as extortion threats backed by DDoS attacks, will be a matter for the police; however all incidents will provide NISCC and collaborative partners with information which can be fed back into the ongoing assessment process.

Ongoing work

31. There is more work to be done on the issue of botnets. ISPs have their part to play in mitigating the impact of botnet attacks. They too bear responsibility for reporting botnet attacks; ISPs will also be in a position to observe and report the malicious traffic passing through their systems, and identify the victims (and hopefully the perpetrators) of DDoS attacks. During denial of service attacks, ISPs may also be able to 'null-route' malicious traffic (ensuring that malicious traffic destined for the target gets sent to a non-routable address, and consequently dropped from the network) to protect their customers from attack.

32. The authorities' investigation of details such as the registration and financing of the command and control server may help to identify the malicious users behind the botnet attack. However, it is possible (and indeed likely) that the target of the attacks, the control server, and the malicious user could be in three different countries (not to mention the compromised computers themselves). Co-ordinated international efforts will therefore be needed to bring the perpetrators of botnet attacks to justice. If a command and control server is identified, prompt action by the high level registrar to freeze¹⁷ DNS records can prevent bots from 'calling home,' thus disrupting the botnet attack. These methods of technically 'dismantling' a botnet can be

¹⁶ NISCC Quarterly 01/05 contains further details on steps users can take to mitigate against the threat of botnets.

¹⁷ i.e. change the DNS entry so that the command and control domain is non-routable.

difficult to co-ordinate and implement. NISCC is working with local and international law enforcement partners to tackle these issues.

Annex A

What is a 'botnet'?

33. A 'bot' (short for 'robot') is any piece of software (or hardware) designed to perform the functions of a human. In computer terms, a bot is a program that performs a set of pre-defined functions normally carried out by a person; on the Internet, bots act as characters in online computer games, regulate chat channels and perform tasks such as the indexing of websites. A 'botnet,' therefore, is any network of bots controlled by a single user, in which computers work together for a common purpose. However the recent rise in the criminal usage of certain 'bot' programs has given the term 'botnet' a pejorative meaning, referring exclusively to those unwanted programs covertly placed on victims' computers and used for malicious purposes. It is this kind of 'botnet' to which this paper refers.

Programming

34. A 'botnet' starts life as a program, a piece of malicious software code. Botnet code can be complicated, and requires a high level of technical ability to write. However, pre-existing botnet source code is readily available on the Internet, which can then be modified by less technically able programmers. Because original code is often modified and reused, these malicious programs tend to fall in to categories or families, defined by their functions, method of spreading and programming language. For instance, the original Agobot program was written by a 21-year-old German virus writer, but has since spawned a family of different versions, building on and improving the program's functions and capability. It is likely that any reasonably competent programmer would be able to create a botnet program if they had sufficient time, motivation and access to information on current software exploits.

Distribution

35. Once the malicious user has created or adapted the bot program, he (or she) needs a method of distributing it to victims' computers. Although methods vary, bot code can often be carried in Trojan email attachments, or in links to websites which, once visited, covertly download the code onto the victim's computers. However bot code does not need to rely on 'social engineering' to spread; malicious users will scan the Internet for computers with a particular known software vulnerability that the bot has been programmed to exploit, and use that weakness to infiltrate their code directly onto the victim's system. Bots can be coded with a number of different exploits, trying each in turn until the remote computer is compromised. Once a bot is in place, it may contain the functionality to spread itself by sending out more emails or scanning more computers; the botnet has been created.

Command and control

36. Once the malicious user has created his botnet, he needs a way of relaying orders to his bots. The majority of existing bots take advantage of Internet Relay Chat (IRC), a web-based system designed to let users chat in real time with other users from all over the globe. In a typical IRC set-up, the user will install IRC client software on his computer, which enables him to communicate with an IRC server. The server will host multiple chat groups ('channels') in which, by posting strings of text in real time, the user can chat with other users, connecting to the server in the same fashion. In a botnet, the malicious user usually controls access to the channel (and possibly the entire server, which may itself have been set up on a compromised computer), and the bots have instructions to connect to it to receive commands. Because a channel can support multiple users, the bot controller can issue instructions to multiple bots simultaneously. Channels can be password protected, in order to ensure that no one else can command (and effectively steal) a user's bots.

37. Although the majority of botnets, for historical reasons, tend to operate over IRC, there is no reason why botnet command and control communication should be limited to this protocol. Practically any method of communicating over the Internet – instant messaging, peer to peer – could be utilised to control a botnet, although current usage favours distributed, real-time communication methods.