Net of the Living Dead: Bots, Botnets and Zombies

Is your PC a zombie?
Here's how to avoid the attentions
of blacklisters and vampire slayers.

David Harley BA CISSP FBCS CITP
Andrew Lee CISSP
Cristian Borghello CISSP

Table of Contents

Introduction

Organized crime long ago discovered the Internet's profit potential, and has succeeded not only in recruiting the necessary expertise to exploit that potential, but in capturing and subverting a significant quantity of innocent Internet-attached systems and, in the process, acquiring the owners of those systems as unwitting accomplices. They have done this, almost exclusively, through the building of botnets.

Most people will have heard references to bots and botnets, but few people actually understand them, what they do or what the scale of the problem is. It was, for instance, reported on June 13th 2007 by the Department of Justice and FBI with reference to "Operation Bot Roast" that over 1 million victim computer IP addresses were identified.[1] Craig Schiller and Jim Binkley[2] refer to Botnets as "arguably the biggest threat that the web community has faced."

Exactly how big that problem is, it's difficult to say. Vint Cerf has claimed that between 100 and 150 million PCs are compromised (or infected) by bot software, out of the 600 million systems estimated to be connected to the Internet.[3] Many observers consider this figure a little high, and by the very nature of the problem, it isn't possible to estimate with significant accuracy.[4] There is no doubt, however, that there are large numbers of compromised systems active on the Internet at any one time. Evron and Solomon suggest that "there are 3.5 million bots on unique IP addresses used every day for spam purposes alone."[5] A 2007 survey by Computer Economics[6] suggests that while costs from direct malware damage (i.e. direct impact on compromised systems) is declining, indirect secondary damage arising from the theft of data and credentials is on the rise. Peter Gutmann pointed out[7] that the Storm botnet, viewed as a multi-processor supercomputer, "easily outperforms the currently top-ranked system, BlueGene/L, with a mere 128K CPU cores…[and]…has better hardware resources than what's listed at http://www.top500.org for the entire world's top 10 supercomputers".

The Shadowserver Foundation (http://www.shadowserver.org/) constantly monitors bot and botnet volumes, among many other things: here's a representative graph as posted on the 27th January 2008.

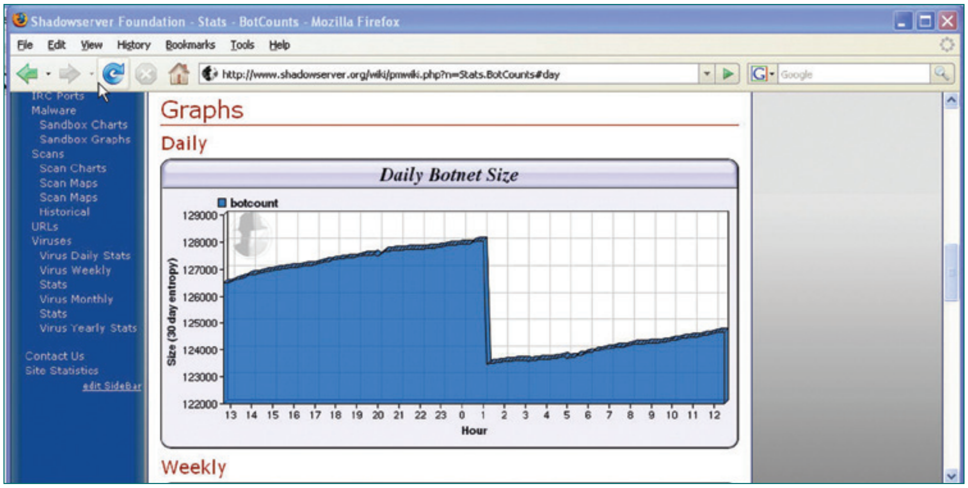


Figure 1: Shadowserver Foundation Bot-Count Statistics, January 2008

Bots

The term “bot” (derived from “robot”) has been applied to many types of automated software. Originally, it was most typically used in the IRC (Internet Relay Chat) community for performing mundane administration tasks, and later in gaming to ‘autoplay’ a character, for instance to gain more experience or in-game currency – hence, perhaps its suitability for use when talking about crimeware. There are many examples of ‘bot’ use:[4]

- Web spiders/crawlers such as those used by search engines to gather data related to web-hosted directories and files, or for more specific ‘scrapeable’ content.
- Gaming bots used in multi-user game-playing.
- Auction bots
- Administrative/support bots used to automate tasks on IM (Instant Messaging) services and IRC (Internet Relay Chat.)
- Spambots traversing web sites, newsgroups and other forums for purposes such as:
  - harvesting target email addresses
  - spamming links into blog comments, guestbooks, wikis and so on, with the intention of increasing search-engine ranking for spammed sites.

When we talk about the botnet threat, we're not talking about harmless IRC administrative bots, gaming bots or P2P bots, but unequivocally malicious software intended to use compromised machines for largely criminal purposes. So, for our purposes, a botnet is a network of linked systems, under the express control of a remote entity, each compromised by one or more bots and used to accomplish tasks and attacks that can be carried out more effectively by many linked machines than by isolated machines.

Although they are grouped under the name ”bot”, these do not constitute a single class of malware like viruses or worms, though they are usually considered to belong to the general class of Trojans. Some bots have replicative mechanisms, so also meet the definition of a worm or mass mailer, whereas others rely for propagation on external mechanisms such as spamming. So the definition of a bot, even a malicious bot, is not as straightforward as the popular (if simplistic) definitions of a virus (“replicates by attaching itself to other code”) or worm (“replicates non-parasitically”.) We can, however, define individual bots and bot families according to these narrower definitions.[4] While most resources are understandably non-committal on an exact definition of the term “bot”, the following points summarize what we generally consider a bot to be, and the behavior that may characterize it:

- A bot is described by Bradley as “malware which allows an attacker to gain complete control over the affected computer.”[8] This definition is quite generic, in that it could just as easily be applied to some kinds of rootkit.[9] However, in combination with the behaviors described below, it gives a pretty good idea of what the security community usually means by the term.
- The nearest thing to a defining characteristic is that a bot compromises a victim system without the knowledge of its owner, rendering it open to remote manipulation, not just individually, but in concert with thousands or tens of thousands of other compromised machines.[10]
- Once a system has been compromised, the bot listens for instructions from a “remote attacker” or allows “backdoor access”.[11] The exact mechanisms by which this is achieved are often referred to as “Command and Control” (C&C). In the past, many botnets have used one or more C&C servers to control compromised systems over IRC (Internet Relay Chat). We are now seeing a widening range of mechanisms and protocols used to the same end, though, and some botnets don't use C&C servers at all.[4]

Bots can, therefore, be of several types:

- Single binary executables such as SubSeven
- Multiple scripts and/or binaries (including a precursor application whose task is to download the main functional components)
- Backdoors in other applications or malicious programs
- Some bots, such as MyTob variants, combine mass mailer propagation techniques with IRC C&C techniques.

However, bots don't only (or even primarily) use IRC as an infection vector. Most of the best-known bot groups have used poorly-secured network shares as an entry point. They look for such commonly used shares as PRINT$, C$, D$, E$, ADMIN$, or IPC$, and are likely to:

- Try to access network resources, SQLServer installations and so on, using a hard-coded list of common weak user-names and password combinations
- Harvest usernames and passwords used by the compromised system
- Use peer-to-peer networks (P2P) like Kazaa and Limewire to propagate malware
- Use spam runs of messages including malicious attachments or URLs, in order to trick end users into running code that will compromise (infect) their systems.

SDBot and its derivatives often include a backdoor component,[4] typically a Remote Access Trojan (RAT). This not only opens a Command and Control channel by which the bot can wait for instructions from the botmaster, but also harvests and forwards information about the compromised system and the individual who uses it.

The "owner" of the botnet can also run IRC commands directing the compromised computer to join an IRC channel, to download and execute files, or to connect to a specific server or Web site to initiate or take part in a distributed denial-of-service (DDoS) attack, among other tasks.

Drones and Zombies

A drone or zombie is a system controlled (or controllable) by an active bot. In other words, the bot is the agent software that resides on the compromised host or drone, allowing the bot master to maintain control. Systems can be compromised ("zombified") by any number of routes, or combinations of routes:

- Self-launching 0-day exploits such as buffer and stack overflows and drive-by downloads (for example, when just visiting a web site is enough to launch malicious code)
- User-launched email attachments
- Probes over local shares by previously compromised machines.

Day of the (Un)dead

The use of the term "zombie" is dramatic and captures the attention of the media,[12] with its connotation of reanimated corpses totally controlled by a sinister magician, but is slightly misleading. A system over which its legitimate owner has little or no control is likely to be reformatted, reconfigured, swept for malware, even scrapped. The owner of a malicious botnet often gets better value out of the hijacked systems, therefore, if their legitimate owner is unaware of their extracurricular activities and takes no remedial action. Using compromised machines intermittently and with fairly light loading not only keeps the compromise under the system user's radar, but makes it harder for third parties (system administrators, ISPs, botnet tracking specialists) to identify compromised machines and initiate or urge remediation. The longevity (or "persistence") of a compromise can also be prolonged by modifying or replacing the agent software on the compromised system with updates and alternative binaries, for example, so that it's harder for security software that relies on signature detection to spot it.

When an IRC-controlled bot has been installed, it "calls home" by joining an IRC channel and listening for instructions from the server. The C&C server is used by the bot master to relay instructions to its zombie population, in order to execute commissions from his customers for tasks such as spam runs and DDoS attacks. These instructions allocate jobs to particular sets of zombies, specifying the targets, time and duration of the attack.

The power of distributed computing for legitimate projects has long been known and exploited in various areas of research and collaboration, such as medical research projects. Characteristically, heavy and resource-intensive computational tasks are shared between high volumes of networked machines volunteered for the task, rather than carried out on a single dedicated machine,

A more exotic example of distributed computing is the SETI@home project (Search for Extra Terrestrial Intelligence – http://setiathome.berkeley.edu/).[12] This is a high-profile research project that uses a virtual network of internet-connected machines running BOINC (http://boinc.berkeley.edu) software to access and analyze radio telescope data. The use of (see [URL]) distributed processing on such projects, shared between large numbers of machines and interested parties, offers (for certain kinds of task) processing power comparable to that of a dedicated supercomputer by "borrowing" spare capacity from many smaller machines. Characteristically, the agent software only borrows capacity at times when the system isn't doing anything much ("idle time"), so that the borrowed system doesn't suffer from degraded performance while it carries out its primary tasks.

Unfortunately, it's not only legitimate researchers who have become aware of this potential. Botmasters may use such techniques to implement jobs like circumventing Captcha screens using OCR technology. Such tasks and technologies can be resource-intensive, and may benefit from the sort of distributed processing that botnets can do rather well. Many of the brute force intrusions and disruptions for which malicious botnets are most commonly used (Distributed Denial of Service attacks, for example) require high volumes of participating machines rather than algorithmic complexity. In such attacks, quantity and effectiveness is more important than either quality and processing sophistication, so that a large network of not-necessarily-state-of-the-art desktop machines may be as effective as a group of top-of-the-range, brand new servers.

Blue Bots

There have also been attempts to turn the botmasters' own tools and techniques against them using distributed processing. A high-profile example was Blue Security's controversial Blue Frog, which attempted to recruit Blue Security clients to populate web forms on spamvertised sites with opt-out requests: this initiative, however, ended in disarray.[13] It seems that a botmaster with less scruples and more machines used those machines to implement a more effective DoS (Denial of Service) counter-attack against Blue Security and associated sites.

Botnet

A number of bot-compromised machines controlled by a common controller constitute a botnet. There are rumors and dire warnings of huge botnets linking over a million or even tens of millions of machines.[14] Certainly it's not unusual for botnets of thousands or tens of thousands to be reported.

In principle, a botnet doesn't have to be malicious or even covert, but in terms of malware, a botnet is a population of zombie machines controlled by the same gang or individual, making use of a bot present on each compromised machine, usually (but not always[4]) with the use of a command and control (C&C) infrastructure.

At the time of writing, IRC remains a very common channel for communication between the bot controller and the compromised machines, though there other mechanisms, for example using HTTP exploits (not necessarily over port 80). The so-called Storm Worm (it isn't technically a worm!) uses the eDonkey peer-to-peer (P2P) protocol,[15] and other contenders for Bot Enemy Number 1 such as Nugache have attempted to emulate its success by using similar techniques.

Still, IRC remains a convenient C&C mechanism for the bot master (zombie master), the "owner" or "administrator" of the botnet. A bot master is also sometimes referred to as a bot herder,[4] so the botnet may, therefore, be referred to as a bot herd, and the practice of exploiting and administering the botnet is sometimes referred to as bot herding. However, bot herding is, strictly speaking, migrating zombies from one C&C location to another when a C&C box becomes unavailable. This can happen when the server is traced and shut down by law enforcement, or a compromised ("owned," "pwned" or "owned" in hackerspeak) machine is disinfected.

Infection & Disinfection

Conventionally, we talk in the anti-malware business of a viral infection, and of disinfection as being the removal of a virus (and, hopefully, the reversal of its effects). However, over recent years, as worms, mass mailers and Trojans have gained ground and equalled or surpassed viruses in numbers and arguably in impact, the terms have become accepted almost universally as applicable to infestation[16] by non-replicative malware, and we won't try to reverse the tide here.

Internet Relay Chat (IRC) is a teleconferencing system which can make use of a client-server model to run over multiple machines in "a distributed fashion"[17]: this model is well-suited to synchronous dialog and data exchange, offering a convenient C&C channel. Public IRC networks have, in general, become much less open to misuse by bot masters as providers have become aware of the problem.[18] Consequently, botmasters have had to make more use of their own servers, or of compromised PCs used as C&C servers rather than as run-of-the-mill zombies. C&C servers (or "rallying boxes") tend to run modified IRC servers. While the default IRC port is TCP/6667, C&C servers tend to avoid this and other ports commonly used by IRC, to avoid drawing attention to IRC/bot traffic in environments monitored by tools such as netstat. Other approaches such as HTTP, Instant Messaging, various forms of P2P networking, and DNS tunneling are also used, and offer the same advantages of easy communication to the bot master. They are also less susceptible to filtering and blocking at the enterprise perimeter.

If we look at current bot structures,[12] we find malware with rich command sets that include, for instance those included in Table 1 (parameters are omitted, as are many other similar commands that offer enhanced functionality).

mac.login	user log-in
ftp.execute	actualization of the bot through an ftp address
http.execute	actualization of the bot through an http address
rsl.logoff	user log-out
rsl.shutdown	computer shutdown
rsl.reboot	computer reboot
pctrl.kill	process ending
ddos.httpflood	Initiate http flooding DDoS
ddos.synflood	Synflood DDoS
ddos.udpflood	UDP flooding DDoS
harvest.emailshttp	obtains mailing lists through http
harvest.emails	obtains mailing lists
harvest.cdkeys	obtains a list of CD keys
harvest windowskeys	obtains Windows registry settings

Table 1: Typical Bot Commands

Such a command set offers a range of services from login access for the botmaster to the shutdown of the computer, DDoS attacks, bot actualization, spam dissemination, and so on.

Chains of Command

It's interesting to compare these to the command sets offered by older threats.[4] Other works referenced here include some detailed information on bot command sets old and new,[2, 4] and you may find the following papers useful, too, if you find the topic interesting:

"Know your Enemy: Tracking Botnets - Bot-Commands. Which commands the bots understand" by Honeynet Project:
http://www.honeynet.org/papers/bots/botnet-commands.html

"An Inside Look at Botnets" by Paul Barford, Vinod Yegneswaran:
http://pages.cs.wisc.edu/~pb/botnets_final.pdf

Command and Control (C&C)

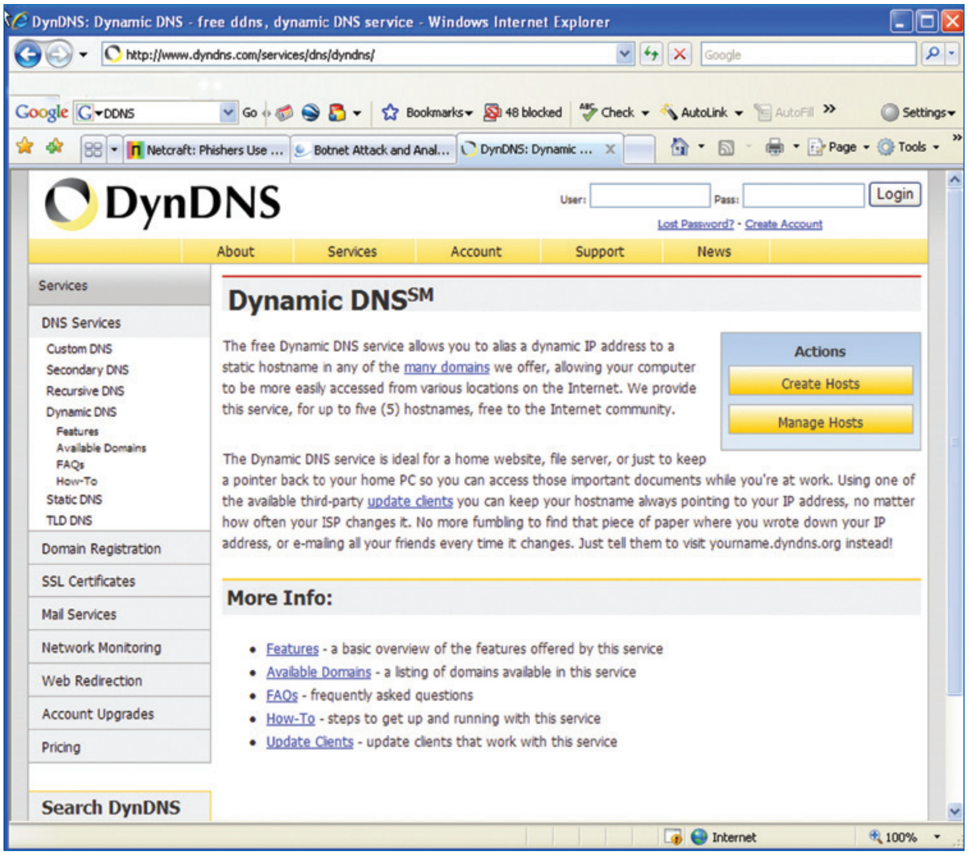
Once a PC is zombified, a number of measures are taken to prolong the "persistence" of the compromise to the system, and therefore its usefulness to the bot master. Defensive counter-measures such as antivirus updates are neutralized, updates and further modules are downloaded, and other systems are scanned for vulnerabilities that will allow the compromised system to infect them. Propagation is a significant aspect of bot functionality: in the words of David Dagon,[19] "the network is the infection."

In recent years, the main way of dealing with a botnet has been to take down the C&C server. However, this has become more difficult.[2] C&C services may be distributed between zombified, high performance servers, possibly augmented by other compromised machines, rather than concentrated within a single system, leading to a single point of failure (SPoF). Botnets can be adaptive and modularized in other respects. The lifetime of the agent software on a compromised system can be extended by updates and the acquisition of other program modules. The lifetime of the whole botnet is extended by switching ranges of active zombies in and out according to what type of attack and target is currently "commissioned." The fact that bot functionality is shared between multiple, upgradeable components can create difficulties in automatically eradicating bot traces from a compromised system without re-imaging or re-installing.

Bots and other forms of spyware bury themselves deep into the file structure of a compromised PC in a number of ways.[4] They generally add entries to Registry keys so that the software is started automatically at the beginning of each Windows session, using sophisticated techniques to make detection and removal harder. They often try to disable security processes such as antivirus programs, the Windows firewall and Windows Security Center, service pack and patch updates, and so on. They frequently modify the "hosts" file to stop signature-based detection software from updating its definitions.

Dynamic DNS (DDNS)

The use of IRC in combination with free DDNS services with a short "Time to Live" (TTL) or disposable domain names and hosts means that domain names and DNS records can be discarded and replaced at will, further extending the life of the botnet. Botnets have become more resilient by moving away from centralized single C&C services towards Peer-to-Peer networks incorporating redundant, resilient node interconnections, and by using "fast flux" DNS services. When the service provider knows that a subdomain is being pointed towards a compromised system hosting a malicious IRC server, it will normally be incapacitated by "nullrouting" – that is, by directing it to an inaccessible IP address. However, the use of nested botnet structures[5] in which one "cell" is hidden from others means that a botnet is often not seriously disrupted by disabling a single server, since other servers and zombies are not disclosed to the botnet hunter.



Dynamic DNS^{SM}

The free Dynamic DNS service allows you to alias a dynamic IP address to a static hostname in any of the many domains we offer, allowing your computer to be more easily accessed from various locations on the Internet. We provide this service, for up to five (5) hostnames, free to the Internet community.

The Dynamic DNS service is ideal for a home website, file server, or just to keep a pointer back to your home PC so you can access those important documents while you're at work. Using one of the available third-party update clients you can keep your hostname always pointing to your IP address, no matter how often your ISP changes it. No more fumbling to find that piece of paper where you wrote down your IP address, or e-mailing all your friends every time it changes. Just tell them to visit yourname.dyndns.org instead!

More Info:

- Features - a basic overview of the features offered by this service
- Available Domains - a listing of domains available in this service
- FAQs - frequently asked questions
- How-To - steps to get up and running with this service
- Update Clients - update clients that work with this service

Figure 2: A Dynamic DNS Service

Botnet Attacks

Botnets are used for many purposes, and many attacks are amplified and made much more effective when processing is distributed between multiple systems. Some of the most common tasks carried out by botnets are:

- Self-propagation through the distribution of malware.
- Spam dissemination through the establishment of SMTP relays and open proxies. In this case we don't just use the term spam to include the Viagra and slimming drug spam with which we've all become far too familiar, but also for out-and-out fraudulent mail such as phishing,[2] mule recruitment and pump and dump scams.[4]
- Denial of Service (DoS) attacks, especially Distributed DoS attacks, usually for purposes of criminal extortion – "pay-up or we'll DDoS you off the 'net'," as Martin Overton describes it.[20]
- Click Fraud[4]

We should emphasize that the bot master is only one of many participants in a complex "black economy." Often, he simply leases and administers access to the botnet by clients who may be phishing gangs, extortionists, spammers, and so on.

Self-Propagation

Self-propagation is an essential component of botnet functionality.[19, 21] However, it takes a number of forms, and it doesn't mean that bots are viruses, though some "true" viruses or worms may also be accurately defined as bots. It means that bots and other malware are exported directly (as email attachments, over weakly protected network shares, and so on) or indirectly (as URLs to malicious sites and resources, for example), but their spread is not necessarily self-replicative.

Spam Dissemination

Botnets are used for spam forwarding by virtue of the fact that compromised machines can be used as open relays (mail relays configured to forward mail without requiring authentication) and open proxies. Open relays have long been known to be liable to serious abuse by spammers, and it's rare for a legitimate server to be set up that way these days. However, a zombie system to be set up in any way that suits the bot master. Given the sort of games that can be played with DNS and bot-herding, it's also much less likely that such relays will be significantly disrupted by conventional DNS blacklists that include IP addresses for known open relays.

Open proxies, which take connections from one IP and pass them on to another, have many uses[22] in botnet-related crime: in fact, some sources use the term zombie and open proxy interchangeably.[23] Typical uses include concealing the true source IP of an attack, proxying port 25 to send spam, inflating web site rankings, click fraud, and so on.

We won't go into detail on spam types here, but we have addressed email-borne fraud and spam issues in general in other papers in this series.[24, 25]

Email Fraud

Clearly, fraudulent email constitutes a major element of the spam problem: in fact, it's sometimes argued that all spam is essentially fraudulent.[25, 26] Leaving aside older scams such as 419s[24] and pyramid schemes, spamming through botnets is specifically associated with phishing[27] and Pump & Dump fraud.[4] In this instance, the spammer usually buys access to the botnet from the bot master and sends mailout instructions to the zombie population via the C&C server.

However, botnets have uses other than email dissemination, including other aspects of phishing (spoofed web page storage and display, for example) and identity theft, including the theft, storage and distribution of login IDs and passwords, financial data, and so on.[21]

DoS and DDoS

Denial of Service (DoS) attacks are attempts to impair or nullify the functionality of services or systems, normally by directing so much traffic towards the victim site that it doesn't have the free resources to process normal, legitimate traffic, to supply normal services, or to maintain communications with users and clients. In the context of botnets, these are usually associated with extortion attempts. Historically, though, there have been many other motives for DoS attacks, such as:

- As part of an ongoing feud
- To prove the "inferiority" of the victim
- To put a competitor or rival out of business
- For propaganda purposes
- Out of sheer malice.[4]

When a DoS attack is amplified by being distributed across many machines, this is referred to as a DDoS (Distributed Denial of Service) attack. An important stage in the development of the botnet threat was the series of very public attacks that hit the Internet around the turn of the century,[28] launched from chains of systems (to all intents and purposes botnets) compromised by iby TFN (Tribe Flood Network), Trinoo (or Trinoo) or Stacheldraht. These and related tools were largely developed to launch DDoS attacks. They didn't attempt the range of attacks that characterize modern botnets. Victims included Amazon and eBay, and combinations of DoS attack types used included ICMP flooding, SYN flooding, UDP flooding, and Smurf attacks.[29] None of these tools used IRC for C&C (TFN used ICMP, Trinoo used UDP, and Stacheldraht used both), but Stacheldraht did include the capability for IRC flooding attacks.

DoS attacks normally fall into one of two categories.[4] Resource starvation attacks are intended to disrupt services by depleting resources (bandwidth, processor cycles, storage and so on) so that the system doesn't have the capacity to handle service requests. Misconfiguration attacks involve disrupting services like DNS (Domain Naming System) so that services are impaired because of inaccurate system data. Network DoS attacks may also include direct or indirect attacks on physical devices. A "Degradation of Service" attack is one which reduces the effectiveness of a service rather than disabling it entirely. A pulsing zombie attack is an example of an intermittent denial or degradation of service where attack traffic comes in unpredictable bursts rather than a steady stream, making it harder to trace the source of the attack.

We won't go into the details of various types of DoS and DDoS or specific countermeasures (firewall filtering, Access Control Lists, rate limiting) here, but have done so elsewhere,[4] and a few of the better known attacks are summarized briefly in the glossary below.

Click Fraud

Click fraud is used to exploit Pay per Click (PPC) advertising. Data collection is corrupted by the generation of illegitimate clicks, so that the advertiser pays for clicks that offer no sales prospects. The distributed processing offered by a botnet allows the bot master to allocate the task of running automated scripts and binaries to machines. These programs generate clicks and therefore (illicit) income.[4]

The Tuzhilin report[30] is focused on Google's attempts to detect invalid clicks. While highlighting definitional problems (how do you define an "invalid click"?) and disclosure problems (defining the problem so that advertisers can verify clicks, without encouraging the public at large to join in the click fraud game), it is very informative on the general issues.[4]

Miscellaneous Attacks

In principle, you can use a botnet for just about any attack you can launch from a single machine, but amplified. Here are few less obvious uses for a botnet.[21]

- Distributed processor-intensive computation (key cracking, for instance)
- Sniffing for username/password combinations and other sensitive traffic[17]
- Keylogging
- Theft, storage and propagation of warez (illegally obtained or pirated software) and copyright violation

Meet the Bots

Modern botnets could be said to have started to evolve around the end of the 20th century: 1999's PrettyPark worm already had most of the characteristics of today's bots,[31] in that it harvested system information, ICQ login names and email addresses, and dialup username/ password combinations, and updated itself over IRC. Other transitional malware includes:

- GT (Global Threat) mIRC Bots (GTBot)
- The SubSeven Trojan
- TFN, Trinoo and Stacheldraht – as previously described, these pioneered the concept of the DDoS attack, though they weren't generally associated with overt extortion.

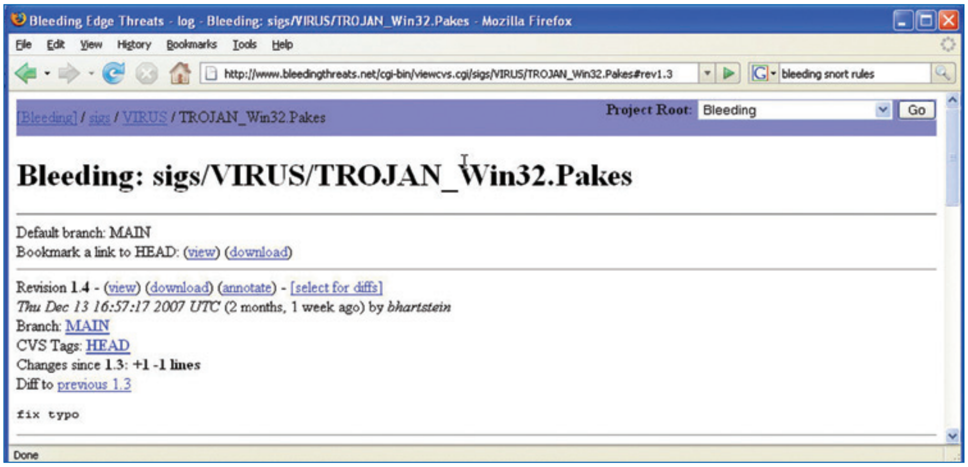
SDBot, arguably the first modern bot, seems to owe its popularity and long life – it still features strongly in current WildLists[32] – to the fact that its source code is freely available. Rbot was one of the first bots to use packing and encryption, and uses a variation on retroviral functionality: it tries to disable processes started by security programs. It also goes after "competitive" malicious processes, though it isn't too proud to use backdoors opened into a system by other malware. Agobot/Gaobot uses P2P (Peer to Peer) networks: Phatbot is an encrypted variation, while Polybot makes significantly more use of polymorphism. The source code for Spybot is also freely available, and this family is notable for its use of spyware technology such as keylogging.[4]

Bot/Botnet Detection

Many formal and informal groups trace bot and botnet activity and cooperate on the takedown of compromised systems, especially C&C servers. Some of these groups include Shadowserver (http://www.shadowserver.org/), North American Network Operators Group (NANOG) at http://www.nanog.org, many CERTs and WARPs, law-enforcement agencies, security vendors, and so on.

DDoS attacks are sometimes mitigated by firewall and switch and router configuration, but these measures are really out-of-scope for this paper. Dissemination of spam, fraudulent mail, and email-borne malware by open relays and open proxies can be mitigated by local monitoring and blocking of SMTP traffic from systems other than authorized mail servers. In fact, ISPs often block outgoing traffic on port 25 for DHCP-allocated addresses for the same reason.

Unfortunately, it isn't usually practical to halt local botnet activity simply by disabling IRC. Apart from the fact that there are alternatives for C&C channels (indeed, not all botnets even use a C&C structure), a botnet doesn't have to use the ports normally associated with IRC. In fact, these ports are usually deliberately avoided. However, locked down desktops with minimum user privilege do make it harder for malware, including bots, to execute and self-install.


Bleeding Edge Threats - log - Bleeding: sigs/VIRUS/TROJAN_Win32.Pakes - Mozilla Firefox
File Edit View History Bookmarks Tools Help

http://www.bleedingthreats.net/cgi-bin/viewcvs.cgi/sigs/VIRUS/TROJAN_Win32.Pakes#rev1.3

bleeding snort rules

[Bleeding] / sigs / VIRUS / TROJAN_Win32.Pakes

Project Root: Bleeding Go

Bleeding: sigs/VIRUS/TROJAN_Win32.Pakes

Default branch: MAIN
Bookmark a link to HEAD: (view) (download)

Revision 1.4 - (view) (download) (annotate) - [select for diffs]
Thu Dec 13 16:57:17 2007 UTC (2 months, 1 week ago) by *bhartstein*
Branch: MAIN
CVS Tags: HEAD
Changes since 1.3: **+1 -1 lines**
Diff to previous 1.3

```
fix typo
```

Figure 3: Snort Signatures at Bleeding Edge

Signature-based solutions such as "conventional" anti-virus (AV) and Snort signatures are largely reactive, but remain effective in many cases[18] for detecting bots and bot components. However, the sheer weight of numbers means that purely reactive detection is not in itself sufficient to stem the flow of malicious programs. Sophisticated heuristic analysis and other behavioral analysis techniques, like those used by the best AV scanners and spam filters, significantly increase detection capability. However, the move away from self-replicative malware and the increased use of runtime packers and other obfuscation to evade AV has lessened the effectiveness of even the most advanced heuristics.[33] Bots and related malware types present particular detection difficulties:

- Where they have no direct replicative function, they present the same difficulties in terms of generic detection as other Trojans: in other words, because they're not viruses, you can't detect them by trapping replicative code.
- The use of techniques such as multiple packers to obfuscate the code lessens the effectiveness of many detection techniques, though detecting the known signature of a runtime packer in code is, increasingly, used as a heuristic indicator in its own right.
- Antimalware scanning over HTTP, a very common bot attack vector, has not yet reached the same peaks of technical development as other scanning technologies[34]

Perhaps the most obvious problem, though, is that a barrage of packed and repacked sub-variants, propagated in short spam runs, is less likely to be analyzed in detail and in a timely manner.

A multi-layered antivirus strategy remains essential to most businesses. It needs to be supplemented by generic filtering and other preventative controls, as well as backup and recovery strategies. Intrusion Detection (anomaly detection, signature detection and hybrid detection, at host level and at network level) and Intrusion Prevention Systems (IPS) also have a part to play.

Harley et al have enumerated a wide range of approaches to monitoring and detecting botnet activity,[2, 4, 18] locally and globally. Many of these are quite generic in nature, and can flag other kinds of attack too, but generally require significant knowledge and operational expertise to reap their full benefit.

Traffic on ports associated with particular malware, vulnerabilities and exploits can be very suggestive. Many botnet attacks involve the covert transmission of illicit email traffic, so monitoring SMTP traffic on port 25 from IP addresses that aren't authorized email servers can be very helpful. Traffic on Microsoft file share ports (135-9, 445) may suggest attempts to exploit common exploits. Table 2, modified from Harley and Bradley[4] shows some common backdoors and the ports associated with them all.

Backdoor Type	TCP Port
Bagle backdoor	2745
Kuang backdoor	17300
MyDoom backdoor	3127
OptixPro backdoor	3410
SubSeven backdoor	27347

Table 2: Commonly-Used Backdoors and Ports

Forensic investigation of suspected botnet activity is way beyond the scope of this paper, but is considered in some depth in the AVIEN Malware Defense Guide[35, 4] as well as by Schiller & Binkley et al.[2] Whether you can make use of such tools as Wireshark, Snort, Ngrep and so forth very much depends on the expertise and resources available to you. However, any enterprise needs to make the best of the patching, logging, monitoring and updating tools available to it.

A darknet (sometimes referred to as a network telescope or black hole) is IP address space which contains no active hosts: it can thus be assumed that traffic detected there is due to misconfiguration or malicious activity (worm and bot probes, for example.) A "packet vacuum" server[36] can thus acquire potentially useful attack data. Internet Motion Sensor (IMS) uses a global network of distributed sensors to track attempted attacks.[37] A honeypot is a decoy system, one set up to attract attackers in order to learn more about them. A honeynet is usually a network of high-interaction honeypots monitored by a honeywall (usually a Layer 2 bridging device.)[38]

Conclusion

Malware has moved a long way from the old model of replicative malware (viruses and worms) motivated by a desire for notoriety, towards a black economy where the malware author is part of a sophisticated gang working according to a business model.

Bot and anti-bot technology has become a complex, dynamic area, in which corporate and home users have become not only victims but part of the problem, at least when their protective measures fail. Consequently, action is required from businesses and from individual users if the risks are to be mitigated. Any vulnerable home system needs the basic defenses – anti-virus/anti-malware software, desktop firewall – and corporate systems need defense in depth: multilayered antimalware defenses, content filtering, corporate firewall, Intrusion Detection and Prevention Systems, and so on, as well as an understanding on the part of management and end-users of their own responsibilities.

References

1. http://www.fbi.gov/page2/june07/botnet061307.htm
2. Craig Schiller, Jim Binkley et al: "Botnets: the Killer Web App" (Syngress, 2007)
3. http://news.bbc.co.uk/go/pr/fr/-/1/hi/business/6298641.stm (2007)
4. David Harley & Tony Bradley: "Big Bad Botnets": in "The AVIEN Guide to Managing Malware in the Enterprise." (Syngress, 2007)
5. Alan Solomon & Gadi Evron: "The World of Botnets" (Virus Bulletin, September 2006)
6. http://www.computereconomics.com/article.cfm?id=1225 (2008)
7. Peter Gutmann: http://seclists.org/fulldisclosure/2007/Aug/0520.html
8. Tony Bradley, "Essential Computer Security", Syngress 2006
9. David Harley & Andrew Lee: "The root of all evil? – Rootkits Revealed" (http://www.eset.com/download/whitepapers.php)
10. Brian Baskin, Tony Bradley, Jeremy Faircloth, Craig A. Schiller, Ken Caruso, Paul Piccard, Lance James, Tony Piltzecker: "Combating Spyware in the Enterprise" (Syngress, 2006)
11. Thomas M. Chen, Jimi Thompson, Matthew C. Elder: "Electronic Attacks", in "Handbook of Information Security" (Ed. Bidgoli, Wiley 2006)
12. Cristian Borghello: "Botnets, redes organizadas para el crimen"; http://www.eset-la.com/threat-center/1573-botnets-redes-organizadas
13. http://www.theinternetpatrol.com/blue-frog-croaks-as-blue-security-closes-its-anti-spam-program-in-wake-of-relentless-attacks-from-spammers (2008)
14. http://blogs.zdnet.com/security/?p=533; http://www.pcworld.com/article/id,138721-c,virusesworms/article.html
15. Pierre-Marc Bureau: "Nuwar Traffic Analysis"; http://www.eset.com/threat-center/blog/?p=87
16. Simon Widlake, quoted in "Viruses Revealed" by David Harley, Robert Slade and Urs Gattiker (Osborne, 2001)
17. RFC 1459: http://tools.ietf.org/html/rfc1459
18. David Harley, Jim Binkley: in "Botnets: the Killer Web App" (Syngress, 2007)
19. David Dagon: "The Network is the Infection: Botnet Detection and Response" at www.caida.org/workshops/dns-oarc/200507/slides/oarc0507-Dagon.pdf
20. Martin Overton, "Bots and Botnets: Risks, Issues and Prevention" (http://momusings.com/papers/VB2005-Bots_and_Botnets-1.0.2.pdf)
21. "A Taxonomy of Botnets": David Dagon, Guofei Gu, Cliff Zou, Julian Grizzard, Sanjeev Dwivedi, Wenke Lee, Richard Lipton; http://www.math.tulane.edu/~tcsem/botnets/ndss_botax.pdf
22. http://www.lurhq.com/proxies.html
23. http://www.rickconner.net/spamweb/glossary.htm
24. David Harley & Andrew Lee: "A Pretty Kettle of Phish" (http://www.eset.com/download/whitepapers.php)

25. David Harley & Andrew Lee: "Spamalot Revisited" (http://www.eset.com/download/whitepapers.php)

26. Phillip Hallam-Baker: "The dotCrime Manifesto: Bringing Accountability to the World Wide Web" (Addison-Wesley 2008)

27. Lance James: "Phishing Exposed" (Syngress 2005)

28. David Harley, Robert Slade and Urs Gattiker: "Viruses Revealed" (Osborne, 2001)

29. David Dittrich: http://staff.washington.edu/dittrich/misc/tfn.analysis; http://www.cert.org/incident_notes/IN-99-04.html; http://staff.washington.edu/dittrich/misc/trinoo.analysis; http://staff.washington.edu/dittrich/misc/stacheldraht.analysis.txt

30. Alexander Tuzhilin: "The Lane's Gifts v. Google Report" (http://googleblog.blogspot.com/pdf/Tuzhilin_Report.pdf)

31. John Canavan: "The Evolution of Malicious IRC Bots" (www.symantec.com/avcenter/rference/the.evolution.of.malicious.irc.bots.pdf)

32. http://www.wildlist.org

33. David Harley & Andrew Lee: "ESET Heuristic Analysis Report- March 2007" (http://www.eset.com/download/whitepapers.php)

34. Igor Muttik, "A Tangled Web" in "The AVIEN Guide to Malware Management in the Enterprise" (Syngress, 2007)

35. Michael Blanchard, Bojan Zdrnja: "DIY Malware Analysis" in "The AVIEN Malware Defense Guide for the Enterprise" (Syngress, 2007)

36. Cymru Darknet project (http://www.cymru.com/Darknet/)

37. http://ims.eecs.umich.edu/

38. http://project.honeynet.org/papers/kye.html; Honeynet Project and Research Alliance: "Know your Enemy: Tracking Botnets" at www.honeynet.org/papers/bots

39. Randal Vaughn and Gadi Evron "DNS Amplification Attacks" (http://isotf.org/news/DNS-Amplification-Attacks.pdf)

Glossary

419	See Advance Fee Fraud
Advance Fee Fraud	419 or "Nigerian" scam, in which the victim is promised large sums of money but is required to make initial payments before the non-existent money can be transferred.
Blacklist, Blocklist	In spam management, a list of IP addresses that are blocked for various reasons including identification as open relays, open proxies, RFC non-compliant, and so on.
Bot Herder	Popularly, alternative term for bot controller or bot master.
Botnet	A virtual network of zombie (drone) machines compromised by the installation of a bot and under the control of a bot master.
Broadcast address	Address that allows all hosts within a network to be addressed rather than one specific address. (See RFC 919.) RFC 2644 recommends disabling directed broadcast forwarding by default, so that broadcast addresses can't be abused by DoS attacks.
C&C (Command and Control)	Channel for communication between the bot controller and the drone (zombie) PCs that constitute his botnet. Used to control compromised machines and direct attacks.
CERT	Computer Emergency Response Team
Click Fraud	Illicit simulation of mouse clicks on advertisements, intended to defraud businesses that offer payment per click to sites that display them.
DDNS	Dynamic DNS
DDoS	Distributed Denial of Service
Decentralized Naming Resolution botnets	Botnets where zombies use existing botnets for DNS resolution, rather than the centralized DNS resources used by legitimate systems.
DHCP churn	Re-use and re-allocation of IP addresses using DHCP (Dynamic Host Configuration Protocol), as opposed to the use of static IP addresses. The very widespread use of dynamic addressing is one of the factors that makes it very difficult to produce accurate statistics relating to bot compromise, among other things.
Distributed Reflected DoS Attack (DRDoS)	A Denial of Service attack using forged source IPs to lure traffic towards the forged address.
DNS	Domain Name System (or Service): handles mapping of IP addresses to domain names.

DNS Amplification Attack A type of DDoS attack exploiting open recursive DNS name servers using spoofed UDP packets [39]

DoS Denial of Service: an attack that damages a site or system's ability to provide a service or execute a function.

Drive-by Download Download of a program to a system without the system user's knowledge or action, especially from a web page.

Drone Another term for a zombie: a computer system compromised by the installation of a bot.

Extortion Illegally obtaining money by threats, e.g. of implementing or continuing a Denial of Service attack..

Fraggle attack A DoS attack where UDP echo packets with forged source addresses are sent to IP broadcast addresses.

ICMP flooding Bombarding a system with ICMP packets (error messages, Echo Requests, or Echo Responses.).

Keylogging Capture of sensitive information such as login information by monitoring and logging keystrokes, especially when subsequently forwarded to a remote attacker.

LAND Attack SYN attack using packets where the destination address is the same as the spoofed source address.

Mule, Muledriver As used here, an individual used with or without their knowledge to facilitate money-laundering.

Packer See"Runtime Packer"

Phishing A generic name for various forms of fraud in which the scammer tries to trick victims into giving away sensitive data, usually financial, using spoofed email and web sites.

Ping Flood DoS attack effective where the victim system responds by default with Echo Reply packets.

Polymorphic In malware, a malicious program such as a virus, bot and so on, which changes from one instance to another, in the hope of making it more difficult to detect and remove. Is also used more loosely to describe email messages, especially spam and scams, that vary from instance to instance.

Port In this context, a number that identifies the channel used by an Internet service (for example, TCP/25 is SMTP – Simple Mail Transfer Protocol.)

Pump and Dump

An email scam where the recipient is encouraged to buy stock at a low price on the promise that it will appreciate dramatically in value in the very near future. However, the scammer already holds a significant quantity of the stock and sells the hyped stock at a profit. When the hype stops and the market notices the trend to selling, the price plummets again.

Rallying Box

An alternative name for a C&C server: a bot master is described as "rallying" victim systems in order to coordinate them in an attack.

Recidivism

In this context, the re-infection or re-infestation of systems by a bot, either the same bot or another.

Remote Access Trojan (RAT)

Sometimes referred to as a Remote Access Tool. A program that enables an attacker to access and/or control a compromised system, usually covertly.

Retrovirus

In computer virology, a virus that attempts to evade, hamper, or disable the functioning of an antivirus or other security program. The term is used by analogy with biological viruses that generate reverse transcriptase to produce DNA using their own RNA as a template. This DNA is incorporated into the genome of infected cells. Yes, it's an imperfect analogy, but real viruses are a lot more operationally complex than malicious software.

Runtime Packer

A type of program originally intended to compress an executable so that it takes less space on disk, decompressing itself into memory when needed. Malware authors noticed long ago that passing a known malicious program through one or more packers results in obfuscation of the code, making it harder for malware-specific scanners to recognize an already-known program. However, the use of a packer can be used as a heuristic to identify probably malicious code.

Smurf Attack

A DDoS attack in which the victim system is flooded with broadcast ping traffic: attack packets have a spoofed source address that appears to correspond to that of the victim system.

SubSeven

A Remote Access Tool (RAT) which could be controlled remotely over IRC, and is therefore considered an important stepping stone in the evolution of botnets.

Syn Flooding

DoS attack where the target site is bombarded with non-existent or unreachable IP source addresses, depleting its resources by leaving half-open, unresolved connections until they time out.

Tor Botnets Botnets that make use of the Tor proxy network to anonymize traffic, making it harder to trace and deal with the network.

Tunneling botnets Botnets that tunnel through other protocols such as NNTP and blogs.

Warez Pirated software, found on a "warez server", often kept there without the knowledge of the system owner.

WARP Warning, Advice, and Reporting Point (http://www.warp.gov.uk)

Zombie Synonym for drone: a PC compromised by a bot, and therefore under the control of a bot master.

Corporate Headquarters

ESET, spol. s r.o.
Aupark Tower
16th Floor
Einsteinova 24
851 01 Bratislava
Slovak Republic
Tel. +421 (2) 59305311
www.eset.sk

Americas & Global Distribution

ESET, LLC.
610 West Ash Street
Suite 1900
San Diego, CA 92101
U.S.A.
Toll Free: +1 (866) 343-3738
Tel. +1 (619) 876-5400
Fax. +1 (619) 876-5845
www.eset.com