



All About
Botnets

10100101011011010010101101010110110010101001
0100100110011001010100011100101010010
0100101110010010010101001001001
11101110010101001010101101010101
10100101011011010010101101010110110
01001001100110010101000111001010100100001010101

contents

All About Botnets



This content was adapted from Internet.com's Enterprise Networking Planet and Enterprise IT Planet Web sites and was written by Charlie Schluting.



- 2 Introduction
- 4 Do Botnets Need Windows?
- 6 Compromised Servers
- 9 What's the Point?



All About Botnets

by Charlie Schluting

Since the proliferation of viruses and other forms of malware, we've seen the beginnings of some frightening software behavior. Self-replication, self-preservation, and active attacks in response to attempts at detection—the malware ecosystem is starting to sound like a science fiction movie. Unfortunately, it's real, and today's malware is actively evolving at alarming rates.

In this eBook we're going to explore today's most intriguing manifestation of advanced malware: the botnet. After this introduction to botnets, we will examine the client side, the server side, and finally some of the more interesting uses of the power a botnet provides.

A botnet is a group of computers that have been compromised, and run a remote control bot application. The bot herder will send commands to the droves of compromised systems, which will gleefully obey.

What's a Botnet Good For?

Well-connected computers are generally the largest targets for botnet operators looking to expand their port-

folios. University systems and even high-speed, broadband-connected PCs are constantly under attack, but these aren't the old school attacks of a few years ago, where a human was attempting some exploit. These are automated scanning and exploitation tools that run from existing botnets. Nobody on the Internet is exempt from these probes, but if a computer is compromised on a high-speed connection, it will fetch a higher price.



Jupiterimages

Bots are extremely valuable on the open market. Remember the attack on six of the root DNS servers back in February 2007? The DDoS was actually an advertisement; they didn't want to take down the Internet. Without a functioning Internet infrastructure, botnets aren't very useful. Bot herders (or maybe just one) decided to show the world how powerful they had become. Mass media happily obliged and provided tons of free advertising in the form of "the Internet is in danger"

reports. If you're in the business of selling DDoS services, or extorting companies yourself, nothing could be sweeter than getting validated by, well, everyone.

Denial of service attacks aren't as useful as they once

A botnet is a group of computers that have been compromised, and run a remote control bot application. The bot herder will send commands to the droves of compromised systems, which will gleefully obey.

All About Botnets

were, but apparently the threat is still capable of producing some extortion dollars. The biggest usage of botnets is for spam. Spam is still big business, even though people say they're fed up with it. Similar to DDoS attacks, spam must exist because it's profitable. The use of blacklists and other dynamic spam fighting mechanisms have encouraged spammers to use botnets to send spam from millions of computers at a time. We'll get into the details of botnet spamming a little later.

Botnets are also used for hosting Web sites for phishing attacks, which are often initiated from a large spamming campaign on the same botnet. Bot herders quickly realized that Web sites hosted on compromised Web servers didn't last long because others on the Internet are quite good at reporting phishing sites. Herders took to finding a reliable bot client, and just hosting the site on the compromised machine. There haven't been any reports of dynamic DNS or proxy server involvement in hosting phishing or drug sales sites, but if these sites start getting identified too quickly (i.e., automatically by a smarter browser), botnets will easily adapt.

Last but not least in the laundry list of tricks, bot clients also act as a springboard for further attacks on neighboring computers. This is especially troublesome.

No Simple Answers

Many people wonder why Internet service providers can't just block "bot activity." The problem is that botnet command and control channels are no longer just IRC. Many corporate networks took to blocking IRC data to stop bot clients from calling home, effectively rendering the bot useless to the operator. The presence of IRC traffic was easily used to identify infected machines, as well. It took surprisingly long, but botnet developers have begun hiding their tracks. Imagine if botnets start using HTTP, and encrypting their own data. We won't be able to detect the presence of infection if antivirus software is unaware of a new virus, and we wouldn't even be able to cut off the command and control mechanism. Of course, botnet developers have started doing this.

Going one step beyond simply encrypting the data and making the old simple methods of detections useless, botnets have also begun using peer-to-peer technology. We may have thought that the whole command and control requirement for botnet existence was silly, but the fact is that it worked, and it worked extremely well. To continue expanding in the midst of botnets being spotlighted in mainstream media, botnets, of course, evolved. They're now using peer-to-peer HTTPS traffic, completely indistinguishable from other Internet traffic; they've raised the bar quite high this time.

Firewalls Fading in Effectiveness

The days of firewalls protecting both home and corporate users are long gone.

They cannot stop initial infections, nor can they prevent compromised hosts from participating in the botnet.

JavaScript browser exploits are all that's necessary to amass a huge botnet army, and just like the migration

away from IRC, this evolution is hardly surprising. Virus writers are always one step ahead of antivirus vendors, who are playing a reactionary game, by nature.

Once one user on a network ignorantly becomes exploited, the bot client is running and, as any security researcher will tell you, every host on that subnet should be considered hostile. If a bot herder does in fact have a zero-day exploit, neighboring hosts will certainly fall. Even without such a magic bullet, the fact remains that the local subnet is a very dangerous place to have an attacker. They can run man-in-the-middle attacks, masquerade as another host (including a router), and successfully execute every possible network-based attack you've ever heard about.

If a botnet cannot be detected, and we aren't foolish enough to think that antivirus companies are ever ahead of the real innovators, then there's only one thing left to conclude. We must get better at both operating system security and network security. That's not a dig at Microsoft; this is not just a Windows problem. ■

“Some SAN specialists quibble that NAS isn't really storage networking as it is just another box plugged in to the existing IT infrastructure.”

Do Botnets Need Windows?

Botnets would not exist without software vulnerabilities; this we can all agree on. The true source of the problem, however, is far from decided. The actual blame does not completely lie with a single company's products. This installment will cover botnet motivations, client infection and survival methods, and why this problem would exist without Windows.

Why?

Botnets exist for two primary reasons.

Executing DDoS attacks, a possibly dying fad, used to be the No. 1 reason. Nowadays spam is king. Spam, of the innocent we-want-to-sell-you-something type, is also dying off, even though it may not seem like it. Legitimate companies have realized that spam is not a marketing tool. Appalled customers finally got the word out on that one, thankfully.

Spam in the form of Nigerian Scams, phishing attempts, and promotion of illegal products is the main motivation now. Botnets run open proxy servers, not just mail relays, which provide an easy mechanism for spammers. At the same time, botnets are flexible

and ready to take on new tasks as well. The use of a massively distributed system of unwitting participants—that's "why."

Attackers infect PCs to install their botnet software, harvest e-mail addresses from your address books, and sometimes even log keystrokes or network traffic. There are secondary motivators, but without people willing to pay bot herders for allowing them to spam, the motivation simply wouldn't be great enough to maintain these systems.



Jupiterimages

The Client

While it is true that most bots run on Windows, and most spam comes from consumer broadband connections, this certainly doesn't mean botnets would perish if Windows suddenly became secure enough to stop them.

Botnet clients have been seen in the wild running on Unix-based systems, too. The extreme ease with which Windows can get infected, in addition to its market share, is responsible for the fact that most spam originates from compromised Windows machines. Unix systems running a LAMP stack are only as secure as the

While it is true that most bots run on Windows, and most spam comes from consumer broadband connections, this certainly doesn't mean botnets would perish if Windows suddenly became secure enough to stop them.

All About Botnets

applications that run on them, which are abysmal. Sloppily written PHP applications have been the bane of many a sysadmin's existence. Within the last few years, the problem has become "why is our Web server spamming?"

That's right, there are tons of Linux machines out there running botnet clients. Before the widespread adoption of botnets, the worst you'd see was a real-live person trying to execute exploits as the user your Web server runs as. Normally they would fail, you'd clean up their entry point, and everything was fine. Contrast that to the Windows world, where any inroad leads to total compromise, and you can easily see the difference in security models.

Regardless of the system compromise level, the damage we're talking about today is done as a normal unprivileged user. A bot client launches, begins running as your Web server user, and immediately starts sending spam. The Q8bot and kaiten bots are the most well known bots written explicitly for Unix systems, but countless little Perl scripts also pervade LAMP nightmares.

There is always vulnerable software to be taken advantage of, and the most widespread ones will be taken most often. They aren't necessarily more insecure than the others; they're just more accessible.

Infection and Survival

The initial infection of botnet client machines was done via worms, but soon the botnets began replicating themselves. Most botnets have the ability to self-update. The bot herder will issue an update command, and all his little troops will download and run new versions of themselves. This update mechanism is even more efficient than Windows update, and it's certainly frightening. Some viruses have also been known to disable antivirus software, and most users would never even notice. If a virus can successfully disable all defense mechanisms and then install undetectable bot

client software, it's sure to survive.

The botnet itself is also a worm, because many bots have the ability to spread. They will try a fairly large arsenal of exploits against computers on the same network, or possibly even across the Internet. Bot clients updating themselves were primarily used as a mechanism to distribute new exploit code at first, but then something marvelous happened, and the first self-preservation behavior documented occurred recently: bot clients began DDoS'ing any computer that attempted to detect them by scanning.

Some newfangled botnets still use IRC to communicate, but they do it over SSL. This essentially means that you cannot detect their presence. Furthermore, the old IRC model of "connect to a server" just isn't feasible. A distributed system that's dependent on a single server is useless, especially when that single server is a huge takedown target. Many a botnet was abandoned in the infancy stage of botnet evolution. We could see this with

“
Some newfangled botnets still use IRC to communicate, but they do it over SSL. This essentially means that you cannot detect their presence.
”

network anomaly detection tools quite easily: clients would appear as a TCP scanner when they unsuccessfully tried connecting to home-base over and over again.

At this point only one thing comes to mind: peer-to-peer applications. P2P networks have successfully thwarted the MPAA/RIAA, so it should work for botnets as well. Especially with their ability to replicate and attack back, they should be unstoppable. Indeed, there have been many reports of P2P botnet activity. Throw SSL in the mix, and they certainly are undetectable and unstoppable.

Let's think about this for a moment. If bots have the ability to self-update, self-preserve, and massively execute large parallel jobs at the command of a single person, what do we really have here? This is not just a tool for spamming and other ills; this is a living, breathing ecosystem. ■

Compromised Servers

Botnets are moving toward a more P2P-like communication strategy, but there remain 'nets that rely on a single server. Bots have been spotted running on compromised Web servers, too, so that they can easily exploit browser vulnerabilities on their victims. Code running on a Web server can be considered a "server side" of botnets, and so can an actual bot server. Let's explore what capabilities a bot server has, as well as talk about some Web exploitation kits.

Command and Control

Regardless of the fact that P2P technologies are starting to be used for communication between bots, it is still useful to understand how the less evolved bots function. The new P2P-enabled bots have the same functionality at their core, so the concept is the same.

A bot herder who controls a bot server (or multiple servers) has at his disposal a number of interesting tools. We briefly talked about what botnets are used for, but now let's take a more detailed look at the actual commands a server can send to bot clients.

Botnets have various capabilities, including denial of service attacks, spam relays, and theft of personal information. They even start Web servers on infected computers to aid in phishing attacks. Here's a brief list of a few of the more interesting things bots can be

instructed to do:

- Start flooding a specific IP or network using TCP, UDP, or ICMP
- Add/delete Windows services from the registry
- Test the Internet connection speed of the infected computer
- Start the following services: http proxy, TCP port redirector, and various socks proxies
- Run their own IRC server, becoming a master for other bots to connect to
- Capture (or "harvest") CD Keys from the Windows registry, AOL traffic including passwords, and the entire Windows registry itself
- Scan and infect other computers on the local network
- Send spam
- Download and execute a file from a given FTP site



Jupiterimages

Moreover, if that was not horrific enough for you, consider the following: all of the IRC bots have modular capabilities. Therefore, if someone programs a new module to extend the bots' capabilities, the owner of the botnet simply runs a single command to install and use the new module on every bot.

Web Exploitation Kits

These kits allow the attacker to gain control of a client machine when it visits a malicious Web page. The most common avenue of attack is via browser vulnerabilities. The attacking code will instruct the Web browser to download and execute malicious code without the user even knowing. It isn't always a matter of "stupid user that clicked yes," which is why it is so important to install patches as soon as they are released.

It is extremely rare for attack code to be part of the initial exploit. Instead, it generally instructs the victim browser to download the exploit from another server. A malicious Web page doesn't generally host the exploit, probably because it would be reported even more quickly. The server hosting the actual exploit is general-

“
Unix systems running a LAMP stack are only as secure as the applications that run on them, which are abysmal. Sloppily written PHP applications have been the bane of many a sysadmin's existence.
”

ly a Web server that was running some piece of PHP (or other) code that allowed someone to secretly upload whatever he or she wanted. This is caused by mistakes in server configuration, Web application programming errors, or sometimes just plain old security holes in the underlying technologies used.

Of course, attackers need to be able to keep track of which IPs they have compromised. MPack and IcePack are the two most popular kits available. They both provide the user with a Web interface and configuration options to set up a "downloader." The downloader is the program that gets run on exploited machines after an attack has succeeded. The downloader will fetch and execute malware from wherever it's configured to do so, and it can use encryption to avoid network-based detection.

These Web kits provide attackers with a neat Web page to view statistics about their attack progress. It provides information about how successful the attack is, as well as lists of already-compromised IP addresses.

Storm Rewrites the Game

By Pedro Hernandez

There is no escaping the suspicion that spammers have been charting a cagier course in recent months. Electronic messaging managed service provider MessageLabs has noticed too.

Previously pristine inboxes are finding that image files and PDFs containing pump-and-dump stock pitches and advertisements increasingly slip through. Excel and Rich Text Format (RTF) spam have also been detected in the wild.

The cause can be summed up by one word: botnets.

Although spam has decreased from its peak in July 2004 when it accounted for a staggering 94.5 percent of the e-mail monitored by MessageLabs – it now hovers around 71 percent – the monetary spoils have prompted spammers to pursue more exotic methods of keeping those coffers full.

Responsible for spewing spam and dropping the DDoS hammer on Web sites, botnets can hardly be considered an up-and-coming threat. However, a relatively new breed of botnet, spawned by the Storm worm, is proving to be tenacious adversary.

The malware has been contributing to a slight uptick in spam lately, according to MessageLabs' Chief Anti-Spam Technologist, Matt Sergeant.

Purportedly under the control of the notorious Russian spammer Zliden, the Storm-based botnet is a very different beast. First, its sheer size is immense. According to MessageLabs, Storm is believed to have infected 50 million machines, though only 10 to 20 percent of its capacity is being used.

Another key difference is that it masks its command and control structure in eDonkey-

All About Botnets

This is extremely trivial stuff. Anyone who gets a hold of IcePack, for example, can quickly begin compromising their Web site visitors' computers. No skill, and no knowledge of the actual exploits, is required.

Compromised Web servers, regardless of software, make, or model, pose a great threat to overall Internet safety. Vulnerable applications exist on every type of Web server, and the underlying OS does nothing to prevent simple exploits from taking place.

Simple exploits, like inserting a little text into a site, used to be pretty innocent. Script kiddies, as they were called, would run other peoples' exploits and deface sites with obscene text or their groups' markings. Every once in a while they would try running some code to open a backdoor into a Unix server, which allowed them access as the user the Web server ran as. But now, with botnets and automated attacks, a simple exploit like this is pretty serious.

Web servers play a huge role in the initial infection, re-infection, and maintenance of botnets. Very often the "downloader" provided by the Web exploitation kits will be used to install bot client software. This is likely an extremely effective method of expanding a botnet, since network-based attacks can be blocked and are more likely to be patched.

Fixing all Web server holes won't stop users from getting infected by any means, but understanding the role of exploited Web servers in the malware ecosystem helps us learn how to fight it. ■

derived P2P traffic, not IRC, rendering techniques to monitor for the latter useless. Plus, Storm-ridden machines are loaded with "intelligence" of the sort that turns victims' machines into multi-vector threats.

One trick, says Sergeant, is "fast flux Web hosting" aided by low DNS time to live (TTL) cycles. This enables a batch of machines to serve up phishing sites – or worse – for mere moments before switching to another set of dynamic hosts. By the time security researchers click an e-mail link and get close, the site has already moved on, offering very little insight into the parties responsible.

Other characteristics of this multifaceted threat include image and PDF generation engines that ensure no two e-mails remain exactly alike for long. This involves randomizing graphical elements and arranging letters in a seemingly haphazard manner (yet remaining strangely legible) to thwart detection or profiling.

And if this all fails, zombie machines can automatically shift to DDoS attack duty. Plus, Storm has shown a knack for self-preservation by knocking rival botnet malware offline and undergoing regular updates to circumvent anti-virus detection. ■

What's the Point?

There's no better way to round out our knowledge of the botnet ecosystem than to try and figure out what the point to all this is.

In a word: money.

Botnets, as we've said, are used for a few main purposes: DDoS blackmail, spam, and the spamming of Web applications. All of these activities themselves can be extremely lucrative, but botnets enable all of the above-at the same time.

DDoS Threats

Distributed Denial of Service (DDoS) attacks are the same as a DoS attack in that someone is simply sending you packets as fast as possible, but DDoS attacks can come from thousands of computers at once. Many people believe that botnets were engineered with this sole purpose in mind.

Back in 2005, we noted that most people do not realize how effective DDoS attacks can really be. Organizations that have fallen victim to an attack know firsthand how helpless they are. After a few companies learned that lesson, the word started spreading. Even recently, bot herders have been demonstrating their DDoS capabilities, and there's still some money to be made using botnets as a tool for extortion. One can only guess how many dollars companies pay each year to organized crime groups to sustain their Internet presence. The numbers, I think, would surprise us all. As lucrative as extortion may be, though, it's a risky endeavor, and the

majority of botnet usage seems to have shifted to other purposes.

Spam

According to a 2006 report by CommTouch, the global spam level increased by 30 percent. In early 2007, security company SoftScan issued a press release suggesting that a broken botnet decreased spam by one-third. In August 2007, security company Sophos claimed that a 30 percent increase in spam was due to pump-and-dump stock scams. OK, everybody likes to claim a 30 percent change, but the point is that spam is ever-increasing, and botnets are the main source. Spam certainly is profitable. Even though most people reading this cannot fathom the idea of someone clicking on links that come in spam, an extremely small percentage of spam recipients do, making unsolicited e-mail marketing an extremely profitable industry.



Jupiterimages

Web Site Spam

Botnets are being used as an illegitimate form of search engine optimization (SEO). SEO is used to attract more search engine traffic to a site by appearing to provide the most relevant content for a search engine's users. By enhancing SEO, Webmasters can boost their site's priority in search results.

As the No. 1 search engine, Google is the target of many SEO techniques, legitimate and illegitimate, all of

All About Botnets

which are designed to increase a site's relevance to the search engine. Google's name for the number it assigns to a site's likely overall relevance is "PageRank." Parts of Google's PageRank calculations include tallying the number of sites on the Web that link to a specific page or domain. The more inbound links a page has, the more likely Google's search algorithms are to decide it's relevant to searchers. The more relevant the words in a link to a site are to specific keywords, the more weight Google assigns to that site when presenting search results for those keywords. A number of links pointing to an online shoe store that include the word "shoes," for instance, will cause Google's search algorithms to consider that online shoe store a relevant result for its users when they search on the keyword "shoes."

Botnets use SEO to "spread the word" about certain sites and boost their PageRank. Generally creating many keyword-appropriate inbound links from other sites using the appropriate SEO techniques does this. If you've ever wondered why your favorite blog's comments section is peppered with links left behind by spam bots, that's one reason: The more sites that link to a page, the more likely that page is to turn up high in search engine results.

Botnets or their operators also create seemingly innocuous blogs and Web pages to boost the inbound links to their malicious sites. Sunbelt Security identified a number of blogs on Google's own Blogger service that included search engine-friendly phrases linking to sites with malicious content. The sites claimed to offer multimedia files that required users to download a CODEC to view the content. The "CODEC" was actually a Trojan horse that delivered a ZLOB virus variant. Yes, botnets use botnets to spread.

We have seen malware hosted on compromised Web sites before. It is generally trying to exploit some browser vulnerability, which means it must attract attention to itself, so using SEO to attract victims is a logical technique. But SEO is, of course, a big business in its own right. Companies pay top dollar to analysts who spend their time figuring out how and why a visitor

arrives at a site. Bot herders have figured out a few tricks, including the creation of bogus blogs, to quickly get their Web site of choice to the top of search engine results. Whether it's a phishing site trying to con people into entering personal information, or a "legitimate" business trying to sell drugs, botnets are very useful in gaining visibility for these operations. People who run questionable businesses will pay top dollar to bot herders who can increase their sales. That's what spam is all about, and affecting search engine ranking is just as powerful.

Vulnerable PHP applications, especially popular CMS and blogging software, are exploited en masse at regular intervals. As soon as a new vulnerability is discovered, nearly every instance of the application on the

Internet seems to spring up a new page chock full of links. Universities, all .edu sites in general, are a prime target. Google ranks content from them higher in search results, so a university Web page full of links to pharmaceutical dealers does wonders to help that page's search engine visibility.

You don't have to look hard to see the effect of botnet SEO on Google itself. Just now, a search for the mildly misspelled "Viagara" in Google yields as the first result a shady-looking Web site that offers to sell it to you without a prescription. One might think that the first search

result would be a Wikipedia article, or perhaps even some medical information site, but nearly the entire first page of search results is some Web site offering to sell the drug. Some may be legitimate (as much as a site can be when it's illegally selling drugs), and some may just be pharming credit card information.

In a few short years' time we've seen botnets evolve from spam-generating, DDoS spewing simpletons into highly evolved ecosystems. We keep coming up with new ways to block their communication channels, so they evolve. The botnet of today was built with high availability in mind, and it can evolve at the push of a button. Because of the variety of methods they employ to compromise servers and clients alike, they've proven they won't be easily stopped.

“If you've ever wondered why your favorite blog's comments section is peppered with links left behind by spam bots, that's one reason: The more sites that link to a page, the more likely that page is to turn up high in search engine results.”

All About Botnets

And while the sheer numbers of botnet zombies seem unwieldy, bot herders remain in control of their creations, perfecting their attacks. ■

This content was adapted from Internet.com's Enterprise Networking Planet and Enterprise IT Planet Web sites and was written by Charlie Schluting.

JupiterWeb eBooks bring together the best in technical information, ideas and coverage of important IT trends that help technology professionals build their knowledge and shape the future of their IT organizations. For more information and resources on IT security, visit any of our category-leading sites:

www.esecurityplanet.com
www.antonline.com
www.internet.com/security
www.internetnews.com/security
www.earthwebnews.com/security
www.enterpriseitplanet.com/security
www.insideid.com
www.smallbusinesscomputing.com
www.linuxtoday.com/security/

For the latest live and on-demand Webcasts on IT security, visit: www.jupiterwebcasts.com/security