10 answers to your questions about botnets

Version 1.0
November 21, 2008

By Michael Kassner

I recently asked TechRepublic members to submit questions about botnets, promising to forward them to the experts at Arbor Networks. Dr. Jose Nazario volunteered to provide the following informative answers.

1 Could you define what a bot or zombie is and how they become part of a botnet?

A botnet is a collection of machines that have been compromised by software installed by the attacker so that they now respond to commands sent by the attacker. This malcode can be installed by exploits on the base OS (e.g., as in the Sasser worm), through browser exploits, or through Trojan horse activities such as fake games or pornography codecs.

2 What are botnets used for—are they profitable?

Botnets are used by the attackers for a wide variety of tactics: spamming, hosting phishing sites, harvesting information from the infected PCs for use or resale (such as credit card or banking information), denial of service for pay or extortion, adware installations, etc. The botnet is a platform for the criminal underground, providing unfettered access to the compromised PC and its resources -- disk, bandwidth, IP reputation, personal information, etc. -- for the attacker. It's a way to load arbitrary software onto the machine, as well as to pull arbitrary information off of the machine.

We see botnets used all over the world: the United States, Europe, Russia and the Ukraine, China, Korea, Japan, South America -- all over. The main motivations in the past few years have become monetary, as opposed to curiosity or joy riding.

3 If I understand correctly, there are different command and control philosophies used by botnets. Could you explain how they work and their effectiveness?

The two main types of command and control structures used by botnets are a centralized mechanism and a decentralized, peer-to-peer mechanism. There is also a third, hybrid approach. Command and control refers to the server(s) that the infected hosts, the bots, contact to receive new commands from the attacker.

IRC botnets are the classic centralized structure, with one or more single IRC servers acting as the main hub. This is still the most popular way to run a botnet, using IRC, HTTP, or other protocols with a single hub. The storm worm used a hybrid approach, where it would pass messages to other bots using P2P, but it would use a central set of servers for files and updates. Finally, the Nugache botnet is the biggest and most well known true P2P botnet.

Obviously, if you can take one server out and disrupt a botnet, that is the most desirable way to approach it. If we take out the hubs of the botnet, the bots are still infected but not acting on commands. P2P botnets are far harder to disrupt and shut down.

4 Are all operating systems equally vulnerable to rootkits? Is there any advantage to using one operating system versus another?

Almost all commonly available operating systems -- Linux, BSD, Mac OS X, Windows -- are vulnerable to rootkits, either kernel-mode or user-land rootkits. These can be used to hide processes or files from the user. In the end, given that all systems have flaws and can be attacked, the only advantage one OS has over another is the research time devoted to it by an attacker.

5 My computer's CPU usage is more than 50%, and outgoing network activity is far from normal, so I suspect my computer may be part of a botnet. How can I confirm this?

AV scans can be of some help, through a number of means, assuming it's up to date. First, if you can scan with multiple scanners, this can make a significant difference in the detection rates. This can be easily done with free online AV scanners, as every major AV vendor has them.

Second, scan with something like a rootkit detector to see if a rootkit has been installed; this is usually not a major source of traffic and CPU usage, but would indicate malware infections that may be hidden from AV or manual inspection.

Third, look at your external IP using a *check my IP* service and then query a tool to see if the IP address is blacklisted for spamming. This is another sign than your system is infected and is a spam bot. The tools at Robtex can be very helpful at this.

Finally, a tool like Trend Micro's RUBotted can help spot some signs of botnet participation. All of these tools can be used freely. But always be wary of software that claims to be free until it charges you a sum to clean up your system; that's usually a scam product.

6 I've heard that rootkit scanners aren't effective. Is that true? If scanners are effective only for certain types of rootkits, how do I know which ones to use? Which scanners would you recommend?

They're somewhat effective, but they're being defeated by newer rootkits. GMer is one of the better rootkit scanners. It is kept up to date with new techniques and appears to address almost all common rootkits.

7 I thought my computer was protected by a firewall and antivirus program, yet the computer became infected with Rustock.B and ultimately a member of some botnet. I was told my only option was to completely rebuild the computer. I did, but what if anything can I do to prevent my computer from getting rooted again?

Keep up to date with AV software, keep updated on patches, don't run as Administrator (or with equivalent permissions), and run a personal firewall. If possible, if you're running Windows, run Vista, which does much of this for you. If not, use XP SP2. Make sure that your AV is enabled for e-mail and Web browsing.

8 I'm a systems administrator for a typical company network. I assume that there's more risk, just from the sheer number of computers. Is there any information I can pass on to the users (especially mobile workers) that will minimize the risk?

Mobile workers are probably the most susceptible, as they enter hostile networks (e.g., the broadband networks they may use at home). They should be told to not ignore software updates, keep their AV updated, and not to cancel such updates or to disable such software. The benefits of these simple hygienic approaches can't be understated.

9 Could you suggest any good sources of information related to rootkits and botnets (Web sites, forums, RSS feeds) that would allow me to stay current?

I maintain a website, InfosecDaily that covers some of the better blogs and news sites. It's freely available. I also recommend a handful of major sites:

- The F-Secure blog is very good and timely.
- Obviously, I'm pleased with Arbor Network's ASERT blog.
- The filtered news stream from Team Cymru is also very good, selecting the best and most important stories of the day.
- I use an RSS reader to fetch and maintain my news; RSS is vital to simplifying your daily news digestion in this business!

10 From all that I've read, it appears as though there's very little I can do to prevent my computer from becoming a member of some botnet. Is that really the case?

I don't think so; I feel this is a winnable battle. The best things you can do are to keep your software updated; the base OS, your browser (most important), and any add-ons. Most bots and malcode get in by using well known vulnerabilities.

The next best thing to do is to keep your AV software updated; most people don't update their AV software -- hourly or even daily, in some cases -- and have no real benefit from it as a result. Finally, a good anti-spam filter can do wonders to prevent threats via e-mail.

Final thoughts

I'd like to thank Dr. Nazario of Arbor Networks for answering these questions and Jessica Sutera, also of Arbor Networks, for helping to make the question and answer session possible. I found the links to be especially illuminating. Oh, almost forgot GMer, which already has a special spot in my rootkit scanner toolbox.

Michael Kassner has been involved with communications for 40-plus years, starting with amateur radio (K0PBX). He now works as a network field engineer for Orange Business Services and as a consultant with MKassner Net. Current certifications include Cisco ESTQ Field Engineer, CWNA, and CWSP.

Additional resources

- TechRepublic's Downloads RSS Feed XML
- Sign up for the Downloads at TechRepublic newsletter
- Sign up for our IT Leadership Newsletter
- Check out all of TechRepublic's free newsletters
- 10+ things you should know about rootkits
- Use honeypots to track and mitigate botnets

Version history

Version: 1.0
Published: November 21, 2008