BOTs: Cyber-zombies



Tom Kellermann, CISM World Bank Treasury Security Team July 2004



BOTs

Bot is short for robot, a program that provides services such as IRC channel management, IRC channel spying, network and host scanning and DoS attacks. Short for robot, a bot is a script that autonomously imitates a legitimate user or client computer.

The Cyber-underground has evolved over the past 2 years. The average denizen/hacker has become much more cosmopolitan. The act of hacking has become somewhat compartmentalized as organized crime begins to gravitate towards the digital cocaine. Most criminal who hack join crews; within these crews Pay the guy to write the code "coder"; Pay a guy to launch the code "launcher"; Pay a guy for data extraction "miner" and finally Pay a guy to launder it on E-gold "washer". The real "crews" create botnets with key stroking and data extraction capabilities. Remote hackers launch bots through Trojan horse programs so as to manipulate tunnels in a compromised system. Bots, however, are "intelligent" applications that are programmed to find and analyze information on the Internet. Originally created for data mining functions, bots are capable of crawling across the Internet in search of specific information, utilizing a form of adaptive intelligence to 'make decisions' along the way for more efficient processing. Recently, however, many Trojans have combined powers with bot technology for malicious purposes. Bots can establish connections with an infected host's Internet Relay Chat (IRC) channel. They then act as proxies, standing by the open IRC channel, awaiting commands by a remote cracker. The GTBot Trojan is an example of a weapon that will unleash an IRC bot.

Malicious IRC bots can be programmed to do anything from flooding users' machines in massive Distributed Denial of Service (DDoS) attacks, to launching synchronized fanning attacks, or spreading worms that infect other user machines with backdoors. There are even armies of IRC bots standing by to launch what sources fear is a large-scale, coordinated attack. In fact, CERT states that GTBot Trojan has infected over 140,000 systems,³ thus converting them from harmless user computers, to soldiers standing by awaiting instructions from a remote commander to launch a potentially harmful attack. These compromised systems, also known as zombie bots, can relegate processing power from the legitimate user over to the remote attacker.

Remote Control Capabilities

While remote access to user information is a compelling threat, equally harmful is the fact that Trojans can provide hackers and crackers with uninhibited control over compromised systems, including the power to execute programs, manipulate data files, pilfer sensitive information, alter

¹ IRC began as a talk feature for Unix based operating systems. IRC is based on a client-server model. Clients are programs that connect to a server, a server is a program that transports data, (messages), from a user client to another. IRC allows for multiple users on multiple servers to talk in real time.

² GTBot is a shortened name for Global Threat Robot. This program was originally called Aristotle's Trojan.

³ This statistic is from CERT Coordination Center (CERT/CC), "CERT Advisory CA-2003-08 Increased Activity Targeting Windows Shares," 11 Mar 2003, accessed on 3 Dec 2003 at: http://www.cert.org/advisories/CA-2003-08.html>.

computer settings, and cause denial of service attacks. In addition to the Backdoor.IRC.Bot.B mentioned above, the Subseven Trojan provides illegitimate users with the ability to obtain control over infected systems. The Subseven Trojan is initially sent as an e-mail attachment, but attempts to deceive the victim by feigning to be a customized message. Subseven can launch a function similar to a continuous screen camera, enabling the hacker to receive screen shots of the victim's computer. The attackers know this, and by launching new attacks from 3rd party machines, they insulate themselves from a lot of risk.

IRC Bots and their cousins

An IRC ("Internet Relay Chat") Bot makes automated responses based on what is happening on an IRC. No person need be typing behind an IRC Bot; the Bot will respond based on public or private messages, pings, or any other IRC event. It can also talk to a database, the web, a filesystem. Generally these Bots are used for valid and useful purposes, but since a person can create his own TCL scripts, Bots can be used for malicious reasons as well. ⁴

IRC Bots vary according to one's operating system. For Windows, there are three specific types of Bots:

- (1.) Bots that consist of a single binary (i.e. AttackBot, SubSeven, EvilBot, SlackBot).
- (2.) Bots that use one or more binaries and open source script files normally based around mIRC 32 and commonly referred to as GT Bot (Global Threat).
- (3.) Bots that are a backdoor in another program such as Socket Clone Bots in mIRC. When you open mIRC, it will make two connections to the server instead of the normal one connection (i.e. Scripted Worms such as Judgement Day).

Join any popular IRC server and you will receive a plethora of DCC filesends or ads for web sites with infectious downloads or even infectious HTML. A great many Bots (i.e. Leave Trojan/Worm) scan for victims of other Trojans, such as SubSeven, thinking that it might be easier to get their Bot onto already-infected machines. Another common trick has been to scan for Exploitable Windows 2000 IIS (Internet Information Server) machines and use Unicode exploits to spawn an FTP server that can be uploaded with a Trojan of choice. Bots are also configured to generate clones that join other IRC Servers and spam message users with URLs for infectious downloads (i.e. GT Bot and Litmus Bot). The Bot-herders have adopted some ingenious strategies--- rather than scan the hard drive, the bot will seek out Anti-Virus in memory and destroy it. Many bots relay the keystrokes of the user of the computer, to their bot-herder, thus compromising the authentication and giving the hacker user privilege on that device and its parent network. Once the Trojan is run it secretly installs itself and creates a method to restart itself. When installed and running, the Bot will attempt to connect to an IRC Server on a pre designated port. The most common connection port to attempt connection to is the default Port 6667. Often as these Bots join the IRC channel the Master will log into them with a special and sometimes encrypted access password. This ensures that the Bots cannot be controlled by other people and makes it harder for someone to hijack the BotNet. That aside, there are a lot of exploits against IRC clients (see BUGTRAQ) and a number of these exploits are implemented in bots that listen for properly formatted messages in particular IRC channels on particular IRC servers. If a hacker

⁴ Bots are often also commonly referred to as Zombies or Drones. In actuality a Zombie is a Unix process which is dead and has not yet relinquished its process table slot. A drone is similar to a zombie and is also not an accurate description of an IRC Bot.

⁵ It should also be considered that IRC Servers usually listen on several other ports by default including: 6660, 6661, 6662, 6663, 6664, 6665, 6666, 6668, 6669 and 7000.

desires to "safely" attack someone's IRC client he or she merely has to send the right message into the correct IRC channel in order to trigger an effectively anonymous attack.

The Spread of Bots

ur

Note: The prefixes scanned by each bot weren't shared. Bot08 is in a target rich network.

At this rate, and presuming that all eight bots are scanning and are able to maintain their present rate of return, this miscreant is adding approximately 28.67 bots per hour, or 688.08 bots per day. That would be 4816.56 bots per week. That's not a bad return on an investment of eight bots.

In a similar case study Out of the 3925 possible IRC servers, scientists found 88 DDoS botnets, or 2% of the total. One could surmise that 2% all (sampled) IRC traffic is utilized solely for the purpose of running DdoS botnets.

Managing Bots: Understanding the Bot Facts a Checklist

- ☐ Most Bots require no technical expertise to spread and control.
- □ Knowing WHAT is on your network is the first step to understanding WHY it is on your network. nalyzing flow data, even in batch mode, produces network awareness like no other tool. *Nothing compares*, not IDS, not IPS, not filter and firewall logs of all sorts. Flows from production networks are the real deal, the actual picture of activity ⁶. To be sure flows can't answer all questions. Flows don't include payload information, and thus the nature of the traffic is often inferred rather than empirically derived. Understanding the limitations of any technology or methodology is critical. Flows aren't a panacea. The greatest problem with flows, however, isn't in what they are unable to

⁶ Spot bot, along with flows and assorted tools. http://www.cymru.com/Darknet/index.html>

convey or contain. It is that they can not be gathered in all situations. I have spoken with a few large providers about their flow collection efforts. Their answer? "We don't." Why not? "Because we can't." Limitations in vendor equipment make it impossible for these providers to reliably and consistently collect flows in some instances. The providers are unable to achieve network and situational awareness, unable to perform network forensics, due to limitations in the gear. That is a problem we must fix.

- □ People to be reasonably paranoid about accepting any files over the Internet from chatrooms or visiting unknown websites without checking that their web browser is updated with the latest critical updates. Tools like Swatit exist for removing some bots. ⁷ But scanning activity doesn't always produce stellar results. This is one of the reasons why the bot-herders share lists of productive, undproductive, and dangerous (e.g. vigilant) prefixes.
- □ Some IRC servers use Ziplink (a compression method using Zlib) to communicate with the hubs. This is employed to bypass IDS. The IRC daemon is configured to obfuscate the bot Ips and hostnames.
- ☐ The loss of even several channels does not nullify the entire botnet.
- ☐ It's no longer sufficient to route packets, regardless if you are an enterprise or transit network.
- □ The bots have SSL capability, though this hasn't been regularly used.
- □ It is essential to attack the command and control of the botnets. By attacking the C&C, one does not disinfect the bots rather one removes the head of these botnets, generally leaving the bots unavailable even to the bot-herder who harvested them.

Conclusion

Bots are the cash registers of the underground economy. They provide the hosts, DDoS, spam, bnc, and financial data such as Ebay accounts, PayPal accounts, and bank accounts. They provide credit and debit cards. They provide sundry merchant and utility accounts. To a large degree bots fuel the underground economy, and are themselves fueled by the underground economy. Bots beget bots, after all. (Rob, 2004)

⁷ http://swatit.org/bots/ The site also offers a free download of its Trojan, Bot, Zombie and Worm Scanner: Swat It.

The bots are being used to extract financial data from the infected hosts. Bots are flexible entities. They can be used as collateral or they can generate profit. Bots are themselves a commodity, though hardly a scarce one. The loss of support for Agobot and Phatbot has left many miscreants without the means to build botnets, thus increasing the profit for those who code bots, and those who have bots.

What can be done in a macro sense?

- 1. Networkers asking for better network awareness tools,
- 2. Vendors responding to that challenge with equipment that can process a 1 to 1 flow ratio in real time.
- 3. Research dollars allocated to the challenges of large (flow) data analysis problems. Here is where the government can assist.

I don't see a market need for more bandwidth; I see a market need for more intelligent bandwidth. The answer shouldn't be "run more fiber! increase the bandwidth!" The answer should be to provide the foundation of tools that make efficient bandwidth utilization and situational awareness possible. We need more awareness, particularly as we continue to run at breakneck (and breaknetwork) speeds toward total convergence. If your providers don't know what is on their networks, how will you? (Rob,2004)