The movie *Terminator* features a classic plot: man against machine. The concept of a powerful robot machine that can become more powerful than man is a frightening one that has lit up the screens of Hollywood for several decades. Today that fear has become a real threat in the eyes of some system administrators who have had to deal with something known as a bot.

Bots are powerful malicious codes that are like a hybrid threat — a mixture of both worm and Trojan components. Bots became a major threat in 2004, with thousands of variants and dozens of bot families. New computers, unprotected and vulnerable, are more likely to be infected by a bot prior to updating on the Internet today than perhaps any other threat. For that small percentage of computers in an organization that are not patched properly, bots will likely infect them in a short period of time. In fact, bots are so successful that they have become an auditing tool of sorts for some frustrated administrators — investigating questionable activity on the network only to find that it is related to yet another bot-infected computer that was not properly patched.

According to iDEFENSE Inc., there are about 20 common bot families to date and thousands of variants. In 2004 there was explosive growth of bots (see Figure 1). This year looks even worse, with many new bot variants and a few more families likely to emerge. Over a 300 percent growth of bots was seen in 2004. This growth curve is somewhat exponential compared to former years, with bots knocking on the perimeter of networks globally 24/7/365. If this growth trend continues bots may exceed 400 percent, with the potential for as many as 6000 to 12,000 new bot variants, in 2005.

The most popular bot families include rBot, AgoBot (GaoBot/PhatBot), SdBot, SpyBot, Randex, Wootbot, and KorGo. Agobot has perhaps the most variants for a given family to date, with over 900 variants by late fall 2004. The rBot family has also been a major factor, with over 250 variants in 2004. More recently, a new family of bot variants, Wootbot, emerged in the fall of 2004.

Looking at these popular bot families, it is easy to see why they are considered a hybrid type threat, composed of both Trojan and worm attributes. For example, the typical rBot worm does the following:

- **Worm functions:**
  - Creates a *copy of itself* in the Windows or Windows System directory
  - *Attempts to spread* to other computers through automated means, including brute-force attacks against weakly protected shares and through multiple vulnerability exploits

- **Trojan functions:**
  - *Masquerades* as a legitimate file or process on an infected computer to avoid detection and deletion

---

KEN DUNHAM is Director of Malicious Code for iDEFENSE Inc.
Installs a backdoor Trojan horse with Internet relay chat (IRC) functionality, which allows the attacker to fully access and control the infected computer through IRC.

As shown above, rBot is a classic, with both worm and Trojan horse components. More importantly, it is a malicious code that can be remotely controlled by an attacker via the IRC backdoor Trojan horse. Thus, it acts as a robot for the attacker. The attacker is then able to steal sensitive data, modify local settings on an infected computer, perform file management, install additional malicious codes, use the computer in a DDoS attack, or perform other actions. The story is the same with all the other bots aforementioned — powerful codes with a hybrid quality, controlled by an attacker for malicious means.

PhatBot SOURCE CODE
In the spring of 2004, hackers released the full source code to the most robust and powerful bot to date, PhatBot. PhatBot is a major update to the original Agobot/Gaobot worms that developed about two years prior. A German hacker by the name of Ago commercially developed this bot, selling undetected variants for as much as $300 or more. Ago regularly updated the bot with new exploits as he could figure them out and add them to his arsenal of options for compromising computers. After 18 months of work, he had a well-developed community of followers helping him develop the code. Then someone took the source code to Agobot/Gaobot and upgraded it significantly in early 2004. This led to what is now known as PhatBot, and the subsequent leak of the full source code to the underground.

PhatBot source code makes it easy for hackers to make new bots and variants of bots. By simply copying and pasting or doing a little editing of the code, a new variant can be created. This makes it trivial for a programmer to compile a new variant to avoid detection by anti-virus software. Worse, the collections of source code are now robust, enabling hackers to quickly copy and paste code from multiple source codes. Source codes for multiple bots, MyDoom, Bagle, and others are now available to hackers. PhatBot source code has been analyzed by LURHQ Corporation at http://lurhq.com/phatbot.html. This report accurately reflects the robustness of this powerful code, including the following vectors for spreading the code:

- MyDoom backdoor
- Bagle backdoor
- DameWare
- DCOM Exploit
- DCOM2 Exploit
- Locator Service Exploit
- WebDav Exploit
- WKS — Windows Workstation Service Exploit
- CPanel resetpass Exploit
- UPnP (MS01-059) Exploit
- MSSQL weak administrator passwords
- Brute-force attack against weakly protected shares
- Private WASTE P2P network

That is a dozen direct vectors for spreading the worm. Administrators found in 2003 and 2004 that bots will often infect a new computer before it can be patched on a live network. This has forced administrators to fully patch computers prior to a live network deployment. The days of hooking up a new computer and remotely updating it over the network are gone due to the threat of bots, scanners, and malicious code attacks in 2004.
Once PhatBot is installed the attacker “owns” the system. He can steal passwords, install keyloggers, run IDENT and ftp servers on demand, run proxy Trojans, sniff network traffic, steal software keys, harvest e-mails, or perform other malicious attacks. The private WASTE P2P network also allows an attacker to easily update a network of bots through any infected computer, rather than a single IRC chat room. This protects the attacker and makes it possible for the WASTE network to maintain functionality and not be shut down easily because there is no single point of control that can be managed or monitored by authorities.

WHAT AND WHEN BOTS ATTACK

Bots are opportunistic by design. They neither discriminate nor are they normally used for a targeted attack. Rather, they scan the Internet, largely in an opportunistic fashion, looking for any computer to infect. A common means for a bot to attack a vulnerable computer today is through unpatched computers on a network. Take, for example, new computers purchased during the holiday season by consumers. Such a computer is not patched against the more recent vulnerabilities. When the consumer connects the computer to the Internet, he or she will likely perform an update of the software as directed by the manufacturer. However, this update will likely take some time. During this time period, the computer may be vulnerable to bots that are actively scanning the Internet at large for any computer they can infect.

Another common means of attack is through corporate computers. Just two years ago, administrators would regularly put newly imaged, but not fully updated, computers on the network to then immediately initiate updates over the network. The problem with this approach is that bots find the computer before it is updated, and infect it immediately. When bots are faster than updates against the bots and other codes, administrators must change the way they do business. As a result, few administrators employ this technique anymore. Instead, they are forced to fully protect a computer in a lab environment before ever placing it on a public network vulnerable to bot attacks.

Corporations also have another problem: pesky computers that do not patch correctly. There is a smaller number of computers that just do not patch like they should. Even if that number is in the one percentile range, it only takes one computer to be vulnerable to a bot attack to compromise an entire network. Administrators sometimes tracked questionable traffic and other activities back to a computer, only to find out that the computer was infected with a bot.

Once a hacker has gained access to a computer, he or she can then use that information to gain leverage to more valuable illicit goods. For example, if an important network has been compromised, an attacker may then attempt to sniff network traffic, install additional undetected codes, and monitor the computer to gain additional information about the network, logons, passwords, and other information useful for exploitation.

Bots tend to be most actively deployed during the months of March through June. This correlates to Spring Break for college students and activity that traditionally occurs prior to summer months for the Northern hemisphere.

Exploit codes included in bots tend to be older exploits for which there is a patch. In some cases, such as DCOM/RPC2 in September 2003, there was new exploit code for this vulnerability within seven days, then put into a bot. This was an unusual situation where the exploitation on the bot level took place in a very rapid fashion. Hackers are able to more rapidly develop multiple exploits, as shown with exploitation seen throughout 2004.

The Witty worm is a good example of this, where a worm emerged in the wild within 24 hours following a detailed vulnerability announcement by eEye. The eEye announcement had details that were advantageous to any individual wanting to verify the
vulnerability or to author an exploit. From a hacker viewpoint, this is where it is at — great details on a new vulnerability. The work has mostly been done for the hacker, leaving just a little bit of work to polish off a fully functional exploit such as a worm. That is exactly what happened with the Witty worm, which spread like wildfire among the small BlackIce community within two days following the eEye announcement.

Organizations that practice security-in-depth are at a lower risk for traditional bot attacks. By simply removing the low-hanging fruit, such opportunistic code does not stand a chance against a hardened network. The low-hanging fruit includes all of the exploits aforementioned and newer ones that became widely available in the underground in late 2004 and 2005. If these vulnerabilities are patched and network shares are strongly protected, how can a bot infect? The answer is that it cannot, because the spreading venues of the bot have been terminated!

Bots are not expected to be a major zero-day vector in 2005, but bot authors will definitely use such exploits if they are able to acquire such code. However, their traditional market of exploitation is that of unpatched corporate, home, and SOHO computers. As the threat scene changes in 2005, bots may prove themselves a more significant force early on as new exploits are developed.

PROTECTING AGAINST BOTS

Updating anti-virus software against known bot threats may also help protect against emerging threats. However, many new variants are likely to emerge in a short period of time, of which many are not detected by leading anti-virus software. Ultimately, due diligence is required to battle against bots because they are opportunistic in nature. They are not user interaction type threats. Rather, they look for weakly protected shares, older vulnerabilities, and other vectors through which the bot can automatically spread. As such, an aggressive patching policy and auditing program are required. Additionally, IDS/IPS solutions are recommended to detect questionable traffic related to bots and Trojans and WASTE communications coordinated by bots. Further, an intelligence provider with comprehensive data and bot analysis support may be invaluable for companies investigating questionable code.

By removing the low-hanging fruit and implementing a multi-layered solid security plan, many — if not all — bots on a corporate network can be successfully mitigated. This requires support from the CEO downward in an organization. It requires multiple technologies on every layer. It requires due diligence in driving home security on every front. Make sure you are not the easy target for a bot or a hacker. By doing so, you will dramatically lower your risk of an attack.

Bots are a growing problem — a significant issue in 2004 and likely in 2005. Malicious code incidents are still high, although anti-virus software is in place on many computers today. Technology alone is not enough to fight the battle. People, process, and technology must work together in harmony to help lower the overall risk of an attack. This is especially true when one considers the ever-present malicious code danger at large. Many of the top worms in 2004 were e-mail worms that required user interaction in order to spread… and yet they spread like wildfire.

Battling bots and worms is much like protecting a house against rising floodwaters. You are always thinking about the next flood, when it will come and where it will strike. You pinpoint your most vulnerable areas and shore them up before the storm strikes. In the raging waters, you are quick to mitigate leaks that threaten your assets. You are always looking for the weakest link in your line of defenses against the storm. Recognizing that it is a battlefield, and acting as such, will help your organization successfully battle the bot in 2005. You may not win every battle but you will win the war!