

A Day in the Life of a BotArmy

Introduction – What’s so threatening about a Bot?

It’s just a bot. A little piece of software code that isn’t supposed to be there and operates without the owner’s permission.

This little bot sits on a system and doesn’t do much. It serves up an ad or two to a Web browser, but that appears to be mostly it. The system’s antivirus and antispyware might know it’s there, but it’s a low level threat.

It’s been there for months. It doesn’t slow down the system. It lets normal work take place. It knows it’s not wanted, so it’s quite content to be overlooked. And so enterprise defenses leave it alone.

This bot has a couple of cousins on that same computer. They’re a little fancier. They hide themselves by sneaking into legitimate software applications, or making themselves look like they’re a real program. There they sit and wait, like the first bot, doing nothing to draw unwanted attention to themselves.

How did they get there? It’s hard to say. It might have been an email. It might have come from an unauthorized chat or instant messaging client. It might have been from a phony Web site or another compromised system inside the network perimeter. With so many devices and applications being added and deleted on the corporate network every hour of every day, it’s not all that hard to slip in unnoticed.

What’s important is that they are there, waiting to betray the trust that networks require to protect the confidentiality, integrity and availability of proprietary trade secrets or customer information. And they are very, very patient.

Danger in Numbers

Bots are sneaky. They know how signature-based defenses, such as antivirus or antispyware operate, so they know how to avoid being found. Every once in a while, they call out to a pre-arranged IP address across the Internet. And they wait for an answer.

Sometimes they hear it. Sometimes they don’t. It’s not enough activity to trip intrusion detection/intrusion protection or network behavior alarms, so the communications occur without interruption. That’s why, when these bots do get an answer, these individual bots turn into something much more sinister – a BotArmy.

A BotArmy is a coordinated group of up to hundreds of thousands – or even millions – of bots. BotArmies act as one, using the resources of many individually compromised machines to create a giant distributed supercomputer. The legitimate owners of these systems typically don’t realize that their computers have been hijacked. And that makes a BotArmy something very, very dangerous.

When the BotMaster Pulls the Strings

BotArmies are controlled by BotMasters. When a BotMaster sends a message to a bot, he tells it several things. First, he tells the bot where to find fresh code. These updates allow bots to change their appearance and capabilities. It's how bots continue to remain invisible to antivirus, antispymware and antimalware scans.

Next, the bots are assigned a mission. These tasks cover a wide range of criminal behaviors, including:

- Keystroke logging, to acquire legitimate user IDs and passwords
- Spamming and phishing
- Propagating by compromising other machines, both inside the network perimeter and across the Internet
- Looking for documents, spreadsheets or database records with specific words or phrases, then sending that information to a predetermined IP address somewhere on the Internet
- Launching an attack against an unsuspecting third party

Why does the BotMaster do this? Profit, pure and simple. Unlike older security threats, which enhanced the hacker's reputation and notoriety, BotMasters use these targeted attacks to make money – a lot of money. For example, a successful BotArmy specializing in spam can be leased for as much as \$5,000 per day. BotMasters also use BotArmies to steal anything of value that they can, or to shut down targeted companies as part of industrial espionage or online blackmail.

Secrecy is the Key

BotMasters usually work for highly structured criminal organizations. As a result, they want to stay as hidden as possible. That's why they use the distributed nature of a BotArmy. If a few bots are discovered, it doesn't damage the BotArmy's overall effectiveness. Furthermore, enterprises continue to be compromised by new bots even as they stamp out the one they know about. It's a race and, for too many companies, the BotMasters are winning.

This secrecy extends to how bots talk to their BotMasters. There's never a direct connection. Instead, bots talk to an intermediary computer out on the Internet, where the BotMaster leaves messages. This intermediary system makes it very difficult to track down who the BotMaster is, or what other systems he may illicitly control. In effect, the BotMaster commands a shadow network within the Internet, one that spans many corporate boundaries and can't be traced from within any individual organization.

The Damage Done

Suddenly, one unassuming bot represents a very dangerous threat – one that can operate with impunity and little chance of discovery. Even if network security staff catches up with any single bot, it can take days or weeks before other bots can be found and eradicated. Even then, the chances of catching every bot are very low.

That single bot becomes the equivalent of an active hacker inside the network perimeter. This hacker has complete, near-invisible control of the compromised system, access to any data to which the authorized user has privilege, and a platform to steal other credentials and penetrate other mission critical systems.

Multiply even a few bots on a few systems by the tens of thousands of PCs and devices connected to the typical enterprise network, and it suddenly becomes clear how much damage even one little bot can represent. For enterprise organizations, the economic threat comes from several directions:

- Proprietary trade secrets will be leaked from trusted internal networks without any trace of the theft, and confidential information such as Social Security or credit card numbers are stolen and sold on the black market
- Denial of Services (DoS) and other attacks against companies originate from inside the network perimeter
- Stolen user IDs and passwords enable a direct attack against internal corporate resources, or rapidly spread the reach of a BotArmy within the enterprise
- A business can't prove compliance with industry and government regulations such as HIPAA, SOX, or PCI when protected assets that come under those regulations are compromised by bots.
- A business is embarrassed publicly when it becomes clear that security has been breached, even after passing a compliance audit
- Legal and financial liability, along with very public and negative publicity, immediately follows when the damage from a BotArmy compromise becomes known

Even worse, the longer a BotArmy is able to operate without discovery, the more a company's own computers operate outside of the IT Department's control. Everything looks normal on the surface, but the trust that companies rely on to drive business has been thoroughly betrayed.

How a BotArmy Sneaks Information Away

Executives trust their IT staff, and IT staff trusts the security infrastructure. However, silence is not security. The key thing to understand about a BotArmy is that security defenses inside the corporate network perimeter are unlikely to see, let alone stop, a BotArmy's activity. Here's why.

A compromised computer calls out to another computer on the Internet, looking for instructions from the BotMaster. The outbound message uses the same port that Web browsers use, so the firewall allows it to proceed. The bot's code doesn't match known signatures for malicious software, so antivirus and antimalware also certify everything as OK.

When the bot connects to that Internet address, there is no hardware or software on the internal network that can identify that address as malicious. In truth, however, that external system is another compromised computer. Subsequent communications between the two look like normal Web traffic. No files have been sent or received. There's no reason for internal defenses to go on alert.

What the bot learns from this communications session is that the BotMaster wants it to change its code and take part in an attack. The BotMaster downloads this code to a different intermediate system, and the bot looks for the update at this new address.

As before, all traffic takes place over the same ports that Web browsers use. Even though a file is transferred with the new code, the code itself doesn't match the profile of any known malware. There's nothing suspicious that internal resources such as antivirus, antispyware, firewalls or intrusion detection/intrusion prevention can identify. The bot then integrates the code into its structure and gets ready to execute its new task.

At a predetermined time, all the bots in this BotArmy launch a coordinated attack against a single target. The enterprise's network behavior sensors analyze the traffic, but the small number of hijacked computers on the network do not generate sufficient volume to generate an alert. As a result, security staff remains unaware of the attack.

End result? A successful attack, in which tens or hundreds of thousands of individual computers spread all across the Internet act in unison. All without being noticed.

Real-world implications? The BotMaster might have attacked an online store, to pick just one scenario among many. With proof that the BotMaster could bring down that business at will, the store owner pays a ransom. The BotMaster makes a lot of money and plans for his next victim.

The Damballa Solution

There is a fast, cost-efficient way to protect enterprise networks from targeted attacks such as BotArmies. That solution is Damballa. Damballa recognizes that the only way to stop BotArmies is to find the links between bots and BotMasters across the Internet that can't be hidden and rarely change. Once those links have been identified and isolated, it becomes possible to disrupt the BotArmy and neutralize its threat.

Damballa knows that bots change rapidly and easily evade signature-based defenses such as antivirus and intrusion detection/intrusion prevention. That's why Damballa uses the Internet itself to locate the command-and-control communications that BotMasters must use to organize their BotArmy.

Damballa's global system of sensors reaches across the Internet to recognize BotArmy communications and isolate the specific locations to which bots must connect to in order to receive their commands. Highly specialized algorithms separate bot communications from normal Internet traffic, and Damballa uses this intelligence to protect clients in real-time.

Damballa's intelligence system works across corporate boundaries to develop a level of insight into global BotArmy activity that internal resources can never match. In addition, Damballa coordinates this insight with internal and external sensors that recognize BotMaster attempts to contact compromised internal systems, or attempts by compromised internal systems to reach out to BotMasters or attack external targets.

Conclusion

Many businesses underestimate the severity of the BotArmy threat. The reason why is understandable – BotArmies are designed specifically to evade firewalls, antivirus and intrusion detection/intrusion prevention systems. This stealth hides the presence, severity and intent of the threat.

The best way to identify BotArmies that span the Internet is to build a security solution that also spans the breadth of the Internet. And yet, the best any single corporation can do is watch what happens inside its own networks.

Damballa is the only network security solution that knows how to track and isolate BotArmy activity, anywhere across the Internet. This powerful combination of real-time insight into the structure of bots, BotArmy capabilities and the communications between BotArmies and BotMasters delivers the edge that corporations need to win the war against bots.

No other security vendor has this ability to deliver global insight into BotArmy activity, severity and intent. Businesses need this information to protect themselves from the BotArmy threats. In short, Damballa represents a very cost-efficient way to extend the effectiveness of any company's network security without adding layers of complexity or extra demands on staff.

About Damballa, Inc.

Damballa protects businesses from targeted attacks used for organized, online crime by using the Internet cloud to identify and isolate threats that evade other technologies. Our unique, global approach monitors the Command-and-Control (CnC) needed to launch these attacks as well as compromised systems, which enables immediate identification and mitigation of malicious activity. Global 1000 corporations, large Internet service providers, OEM partners and government agencies use Damballa's signatureless solutions and industry-leading research to reinforce existing security infrastructure and stop hidden Internet attacks. The result is dramatically improved security both inside and outside the network perimeter. Damballa is privately held and headquartered in Atlanta, Georgia.

Copyright © 2008, Damballa, Inc. All rights reserved worldwide.

This page contains the most current trademarks for Damballa, Inc., which include Damballa, the Damballa logo, BotArmy and BotMaster. The absence of a name or logo on this page does not constitute a waiver of any and all intellectual property rights that Damballa, Inc. has established in any of its products, services, names, or logos. All other marks are the property of their respective owners in their corresponding jurisdictions, and are used here in an editorial context, without intent of infringement.