



# Are Bots About to Bring Down Your Business?

## INTRODUCTION

There's some good news these days on the IT security front: Cybercriminals don't want to knock your network offline. The bad news? They want to use it for launching attacks that are more distributed, more profitable, and potentially more damaging to your business than ever before.

Cybercriminals need enterprise systems to maximize the effectiveness of bots—the rogue, hard-to-detect programs they use to seize computers and rope them into larger collections of similarly compromised machines known as botnets. And they have far more in mind than flooding servers or propagating worms: Botnets provide an efficient, distributed architecture for staging large-scale raids on information and blasting spam. As such, they're reflective of the evolution of cybercrime from mischievous hacking and malware-writing to well-organized schemes for stealing data on a global scale and selling it for maximum profit. Witness the bust in February 2008 of a 17-person Canadian ring running a one-million-computer botnet that led to nearly \$50 million in business losses.

Clearly, bots and botnets pose yet another threat to valuable corporate data. A potentially bigger worry: the as-yet undetermined liability of companies whose systems are unknowingly used in the theft of data or delivery of spam. What's more, any time that the security of confidential information is compromised, organizations run the risk of noncompliance with the numerous regulations now on the books—not to mention losing the trust of their customers and business partners. In short, bots and botnets may not necessarily lead to expensive downtime, but they could be a lot more costly to your company in other ways.

Fortunately, there are ways to defend against the threat of bots. As always, educating users is a great place to start, since bots usually download themselves from sites they shouldn't be visiting from work in the first place, or from e-mailed links they have no reason to click. A necessary corollary to that strategy: Update acceptable use policies, and make it clear that violators will face the consequences.

Of course, finding the right security technology is also essential in the fight against bots. Implementing a Web filtering solution that stops bots at the gateway—before they even have a chance to land on corporate systems—gives organizations the protection they need, and the assurance that bots won't spell the end of their business.

Cybercriminals need enterprise systems to maximize the effectiveness of bots—the rogue, hard-to-detect programs they use to seize computers and rope them into larger collections of similarly compromised machines known as botnets.

## THE BOT BASICS

As IT professionals are aware, bots aren't bad by their nature. Also known as Web robots, crawlers, or spiders, they are at their most basic simple software scripts used to run automated tasks over the Internet.

These include searching for content, posting messages to multiple newsgroups, or sifting through data to make online comparison shopping possible. Bots serve numerous, legitimate commercial purposes, as well as charitable ones. The FreeRice site, for example, relies on bots to run an online vocabulary game that helps raise money to fight world hunger.

As with all things online, however, bots can be used for less noble purposes. Ticket brokering agencies, for example, may deploy bots against entertainment or sporting event sites to gather up as many of the best seats possible for reselling at maximum profit. Participants in multiplayer, online role-playing games also have been known to use bots to seek and gather information for competitive advantage—information that would otherwise require too much time or effort to obtain.

## BOTS BEHAVING BADLY

But those endeavors are tame in comparison to the nefarious, large-scale operations in which cybercriminals now specialize. They know there's a lot of valuable information stored on employee and corporate systems, and they know that bots can help them get it. Once in possession of this data, they turn around and sell it to the highest bidder. This has helped turn an underground market for stolen and re-sold information into a global business involving tens of millions of dollars.

What kind of information? E-mail addresses that spammers can target with their come-ons for pornography, pharmaceuticals, and shady financial schemes. Social security numbers and other private data that can be used for everything from simple fraud to full-scale identity theft—with potential implications for national security. Sensitive corporate or government data that can be held for ransom or sold to competitors, foreign governments, or even terrorists.

Bots can land on user systems in by-now familiar ways: via drive-by downloads from visits to unauthorized sites, by clicking on links in suspicious e-mail messages, or even by mousing over compromised banner advertising. Bots are built to elude detection, morphing as they travel so that most anti-spyware, -spam, and -virus packages can't catch them; and by lying dormant on computers, without affecting performance or otherwise calling attention to themselves. If the opposite were true, cybercriminals would be robbed of the weapon that's truly vital to their mission: the user computer itself.

That's because they group those individually infected machines together in huge, linked pools known as botnets. Using Internet Relay Chat (IRC) protocol as their command-and-control, these so-called bot-herders then summon the bots into action, creating a vast network of "zombie" computers that exponentially increases the power of a single bot to complete repetitive tasks like searching for e-mail addresses. Botnets also supply the distributed architecture that cybercrime rings need to maximize the impact of their attacks.

Many of the largest bot operations are run out of Russia and former Eastern Bloc nations, where corruption is rampant and oversight lax. It is believed that one in four PCs worldwide is now part of a botnet; some estimates place that number higher. Most infected computers belong to home users working without proper security; bot-herders in search of potential zombies thus typically target and make use of the blocks of dynamic IP addresses ISPs set aside for these subscribers.

**Bots can land on user systems in by now familiar ways: via drive-by downloads from visits to unauthorized sites, by clicking on links in suspicious e-mail messages, or even by mousing over compromised banner advertising.**

Just six botnets are thought to generate 85% of the world's spam, but they're also used in everything from phishing and distributed denial of service (DDoS) attacks to pump-and-dump stock scams. Some botnets are more notorious than others: Mega-D, Srizibi, and Rustock are among the most infamous. A botnet known as Storm, however, probably tops them all.

First detected in January 2007, Storm by September 2007 was estimated to be running on anywhere from 200,000 computers to as many as 50 million—putting it on par (if not ahead of) advanced supercomputers in terms of power. Spread as a Trojan horse through spam, it at one point accounted for

8% of all malware, according to the Institute for Ethics and Emerging Technologies. It's been used in crimes ranging from bank fraud to identity theft, and its controllers—still unknown—not only take active steps to thwart detection and disabling, but have also used the botnet to launch DDoS attacks against security vendors investigating it. Some security experts said in late 2007 that the power of Storm was diminishing as its operators began to decentralize control, but the U.S. FBI still considers it a major threat to enterprise and government systems.

Part of what makes Storm and botnets like it so hard to detect and disable is that their operators have gone beyond IRC command-and-control and adopted a technique known as fast-flux. This refers to the ability of botnet operators to constantly register and de-register the DNS addresses of individual nodes within the botnet, so that an ever-changing list of destination addresses—up to thousands of entries long—is created. When Web and e-mail servers are being moved around this quickly, IP access control lists (ACLs) are essentially useless in identifying the attacking botnet.

Fast-flux first came to the attention of security experts in 2006, which already makes it a relatively mature approach. Indeed, in January 2008, ICANN released an advisory on double-flux, which ups the ante by moving the actual domain name server (DNS) from machine to machine and exploiting name resolution services. This added layer of "evasive redundancy" is expected to make botnets even harder to detect.

Meanwhile, there's an extensive underground market in botnets themselves, as operators now carve out portions of their botnets for lease or sale, making them available to the highest bidder. Experts note that this began to happen with Storm in late 2007. They warn of a sharp rise in the number of botnet-launched attacks thanks to the availability of so-called botnets as a service, or what one industry observer refers to as "criminal business-to-business software."

Security experts also note there's little honor among these particular thieves: Bot-herders have been known to set their botnets loose against rival bot-herders, seeking an edge in a market that's become increasingly competitive as the potential for profit has grown. But this doesn't necessarily work to the benefit of enterprises; rather, it enables the stronger botnet to become even more dangerous.

## **WHY BOTS AND BOTNETS ARE SO BAD FOR BUSINESS**

Simply put, any security vulnerability is potentially damaging to your business, and bots and botnets definitely fit the bill. When rogue programs are running on employee machines, companies are right to worry about the safety and integrity of their data and their systems, and whether compromised information and performance could affect not just their competitiveness—but their viability.

## Liability

Botnets raise a major new concern for companies: their potential liability. What happens when a bot-herder uses a company's computers in service of criminal activity? No one really knows, since this is one area where the legal ramifications have not been worked out.

Still, it's not hard to imagine the potential exposure your company would face if it was determined that its machines were marshaled to bring down an ISP, trigger a massive spam blast, steal intellectual property, or snoop around government systems in search of classified intelligence. The costs directly associated with litigation and possible fines would probably be damaging enough, but then there are the costs associated with loss of reputation and damage to the brand as well. Potential liability is probably the biggest danger that botnets pose to the business, and thus it will require special attention in terms of formulating new security strategies.

## Data Leakage and Regulatory Compliance

When bots reside on employee systems, corporate data is at risk. Whether it's customer records or user passwords, companies can't afford to let this information fall into the wrong hands.

Yet it happens a lot. In a Ponemon study of 700 C-level executives and IT security professionals in 2007, 85% reported a security breach. And not surprisingly, a large majority—74%—said it resulted in a loss of customers. Another 59% faced potential litigation, while 33% faced fines. Network World says the average breach can cost a company \$5 million. But many organizations might want to keep the experience of ChoicePoint in mind: When the data integrator lost 163,000 private records at the end of 2004 and in early 2005, the U.S. Federal Trade Commission imposed a \$15 million fine that had to be paid in 10 days. The InfoWatch Analytical Center, however, pegs the total direct and indirect costs to ChoicePoint much higher—as much as \$55 million, once negative publicity and the impact on profit are taken into account.

Regulatory compliance is also a concern when it comes to bots and botnets. Complying with everything from HIPAA and Sarbanes-Oxley to various Securities and Exchange Commission rules means ensuring the confidentiality of personal, medical, and financial information. And disclosure of that information becomes more likely when a rogue script resides on an employee's computer.

## Performance

Even though bot-herders rely on the health of computers and computer networks to run their activities, the presence of bots is likely to have an impact on network performance. That's exactly what companies don't need when availability, speed, and optimal use of capacity are essential to the day-to-day operations of the business.

Some organizations have learned this first hand. In one case, a CTO discovered that an employee had inadvertently created a botnet within the company's network after surfing real estate sites in search of a new home. The botnet was stealing bandwidth and processing power from the company's resources—impacting the productivity of other employees.

**Regulatory compliance is also a concern when it comes to bots and botnets. Complying with everything from HIPAA and Sarbanes-Oxley to various Securities and Exchange Commission rules means ensuring the confidentiality of personal, medical, and financial information.**

## Fighting Bots and Botnets

Defending your organization against bots and botnets is in many ways similar to warding off malware. Still, this threat poses particular changes so companies should consider the following comprehensive approach.

- Deploy security solutions like anti-virus and anti-spyware, which could help in stopping bots at the end-point
- Deploy gateway security solutions that can scan e-mail and Web traffic to prevent users from accidentally downloading bots. These solutions can also be used to detect outbound traffic from bots, helping identify bot-infected machines on the network
- Set up a proactive security response group, and assign them responsibility for dealing rapidly with infected machines, keeping patches current and the security infrastructure up to date
- Conduct frequent user training, educating employees on how to recognize e-mail and IM scams and avoid falling for the social engineering techniques used to propagate bots

The M86 Professional Edition Internet Filter from Marshal8e6 can supplement your company's efforts in defending against bots and botnets. This high-performance appliance, optimized for speed and scalability, is deployed at the gateway and includes more than 100+ categories and millions of Web sites from the Marshal8e6 database, including known bot sites and IP address net blocks taken over by bot-herders. It also monitors FTP, HTTP, and IRC communications to detect botnet traffic heading out, helping detect the presence of zombie computers on the network.

In addition to detecting and defending against bots and botnets, the M86 Professional Edition delivers a complete range of security features, giving companies comprehensive protection against today's most dangerous Internet threats:

- Filters for URLs and/or IP addresses, file types (MP3, HTTP, HTTPS, FTP, Newsgroups (NNTP), and TCP
- Blocks Internet threats like spyware, malicious code, and botnets (IRC, command-and-control)
- Blocks instant messaging and P2P by signature or
- Blocks anonymous proxies using signature-based/network detection
- Enforces SafeSearch on major search engines (Google, AOL, and Ask)
- Sends frequent, non-categorized URLs from participating back to M86 on a daily basis, so they can be reviewed and added to M86's standard library categories
- Allows administrators to monitor user Internet activity
- Locks down a user's workstation when thresholds for inappropriate Web sites are exceeded

That all translates into a range of business benefits. The M86 solution helps improve employee productivity by reducing visits to unauthorized Web sites, IM, and P2P applications; aids in complying with regulations like CIPA, HIPAA, and Sarbanes-Oxley; reduces the potentially costly liability associated with exposure to inappropriate content; secures confidential information; and controls access to bandwidth-intensive sites.

Further, the M86 Professional Edition runs in "pass-by" (or transparent mode), sitting outside the flow of network traffic so there is no impact on network performance. And simple, centralized configuration frees IT staff to focus on issues directly related to the business.

## CONCLUSION

As organized crime rings target online information, they're using increasingly sophisticated methods to get control of the valuable data they want. Bots and botnets have emerged as their primary method of getting this information—and for mounting large-scale, distributed attacks or blasting spam.

This poses a range of concerns for enterprises. Some, like the vulnerability of data and regulatory compliance, are familiar; others, like the as-yet undefined liability issues, are relatively new. As with all potential security threats, companies need to respond with a range of measures, including educating users on how to avoid downloading bots and creating a rapid-response team to deal with the dangers bots and botnets present. Also essential to the effort is a gateway security solution that can stop bots before they land on the network and that can detect outbound botnet traffic. The M86 Professional Edition Internet Filter appliance fills this role, delivering a range of business benefits even as it protects companies from the sophisticated techniques today's cybercriminals employ.

## ABOUT M86 SECURITY

M86 Security is a global provider of Web and messaging security products, delivering comprehensive protection to more than 20,000 customers and over 16 million users worldwide. As one of the largest independent internet security companies, we have the expertise, product breadth and technology to protect organizations from both current and emerging threats. Our appliance, software and cloud-based solutions leverage real-time threat data to proactively secure customers' networks from malware and spam; protect their sensitive information; and maintain employee productivity. The company is based in Orange, California with international headquarters in London and offices worldwide. For more information about M86 Security, please visit [www.m86security.com](http://www.m86security.com).

---

### TRY BEFORE YOU BUY

M86 Security offers free product trials and evaluations. Simply contact us or visit [www.m86security.com/downloads](http://www.m86security.com/downloads)



**Corporate Headquarters**  
828 West Taft Avenue  
Orange, CA 92865  
United States

Phone: +1 (714) 282-6111  
Fax: +1 (714) 282-6116

**International Headquarters**  
Renaissance 2200  
Basing View, Basingstoke  
Hampshire RG21 4EQ  
United Kingdom  
Phone: +44 (0) 1256 848080  
Fax: +44 (0) 1256 848060

**Asia-Pacific**  
Suite 1, Level 1, Building C  
Millennium Centre  
600 Great South Road  
Auckland, New Zealand  
Phone: +64 (0) 9 984 5700  
Fax: +64 (0) 9 984 5720

Version 09.01.09