SOPHOS

simple + secure

Botnets: The dark side of cloud computing

By **Angelo Comazzetto,** Senior Product Manager

Botnets pose a serious threat to your network, your business, your partners and customers. Botnets rival the power of today's most powerful cloud computing platforms. These "dark" clouds, controlled by cybercriminals, are designed to silently infect your network. Left undetected, botnets borrow your network to serve malicious business interests.

This paper details how you can protect against the risk of botnet infection using security gateways that offer comprehensive unified threat management (UTM).

Not all clouds are good

What makes up a computing cloud? It's a large collection of computers or processors, memory, storage space, applications and other computing resources connected to the web. These web-connected resources, available simultaneously to millions of customers, can be housed anywhere in the world. The cloud offers many benefits to businesses including lower capital and operational expenditures related to hardware and software ownership and maintenance.

On the other hand, cybercriminals control some of the most formidable cloud computing platforms in existence today. These "dark" for-profit cloud computing networks, known as botnets, can run millions of infected computers, called bots, which spread malware. Undetected, botnets can steal enough computing power to bring down your network and your business.

You need to continuously monitor this insidious threat. Because of its unique architecture, a botnet may continue to run rampant, even if some or most of its bots are destroyed. Without preventive detection on your network, you continually run the risk of infection.

Tempting targets

Today's powerful computers and fast Internet make the business of cybercrime possible. Cybercriminals and the botnets they control seek out the security vulnerabilities in your computer to capture these abundant resources for their own profit. Botnets operate stealthily to infect your computer with a virus without any immediate or noticeable damage. The silent attack turns your computer into a bot or a "zombie slave," which takes commands from an unknown central "master."

Once your computer is compromised, the computer virus will seek to silently infect and copy itself to other machines as well, growing the scope and power of the botnet.

Strength in numbers

Modern cloud computing datacenters maximize performance while minimizing failure. In contrast, a botnet operates with sheer scale and brute force. A botnet controls millions of computer processors, countless gigabytes of storage and memory, and enough combined bandwidth to overwhelm the largest multi-gigabit commercial Internet connections. Botnets have an advantage over a legitimate commercial cloud—they can grow at alarming speed, unhindered by failures.

How botnets spread

Botnets don't target and infect a specific business. Instead, botnets spread by systematically working through a list of IP addresses or dynamically scanning the machines and network space around them, seeking specific vulnerabilities.

For example, a bot program might find a business computer it can infect using an unpatched Windows vulnerability. It then moves on, sifting through the entire network while probing other machines for vulnerabilities. At the same time, the newly infected machine becomes a functional bot. The bot may infect other computers on the network, which can include other businesses or customers. The cycle continues.

In this example, none of the affected businesses were specifically targeted by an individual. The botnet spreads anywhere it finds a vulnerability. Spending money on extensive forensics to identify the individuals involved in the "breach" would be a waste of your time and money.

A new web threat is detected every 4.5 seconds.

SophosLabs, published in Sophos Security Threat Report Mid-Year 2011

Who benefits from botnets

Botnets spread for the purpose of giving the botnet owners massive dark cloud computing power that they can use to conduct highly profitable cybercrime.

Botnet owners may rent out the botnet to criminal enterprises. For example, a spam operation might use the botnet to blast out millions of spam messages. Unscrupulous businesses could use a botnet to knock down a competitor's website with a crippling DoS attack. Botnets can also crack open encrypted information, testing trillions of binary keys in order to "brute force" the encryption on a stolen protected work or encrypted database.

This kind of activity is not only highly profitable but fuels development of ever more capable botnets. Botnet designers also increase the sophistication of their bot programs by analyzing the security industry's response to their previous efforts.

The consequences

Botnet infection has both immediate and potentially long-term consequences. Network failure is the most devastating of the potential consequences. This significantly impacts IT operations, sales, customer account management, employee productivity and more. Today every department and every revenue-generating channel is negatively impacted by network failure. The cost of lost business can skyrocket. But perhaps the heaviest burden falls upon IT. Responsible for the health of their business network and its users 24/7, IT admins must often drop all other strategic priorities to restore network performance and combat an often recurrent botnet infection.

But some of the more insidious long-term consequences can impact a company's public reputation, competitive edge or viability. Because botnets are built for the purpose of conducting illegal business activities, any company with infected computers in the botnet's destructive path can be at risk for liability. Legal costs, court proceedings, negative public relations and more can result even if the business pleads, "I didn't know." Moreover, customers, partners and other key stakeholders could be infected by their trusted business partner.

If found responsible for security breaches, a company can be held liable if its computers are used as part of the botnet to hack into websites, disrupt communications via DoS attacks, share pirated files or attack machines with hacker scripts.

Cybercrime costs the global economy $338 billion each year, more than the illicit drug trade.

ZDNet

The best defense

As we've discussed, botnets pose a significant threat to businesses, randomly attacking vulnerable computers or nodes without being traced back to an operator.

But you can protect yourself against attack with the right solutions and a few simple best practices.

To protect your business against the threat of botnets, we recommend you do the following:

- Ensure your operating systems and their programs are patched and updated.
- Utilize an effective gateway defense solution to prevent bots from entering your computers.
- Test the perimeters of your workstations and servers.

If infected, avoid spending money researching the culprits behind an attack; instead invest in better securing your resources in order to prevent the next round of assaults.

You can easily and cost-effectively prevent intrusion of bots with the right protection. Sophos Astaro Security Gateways are equipped with intrusion detection systems that detect and stop bot programs. All you need to do is list what type of computers and resources you use. This solution prevents attacks in real time. And it will identify existing infections so they can be cleaned and eradicated. We can shield your network from threats and attacks, leaving you free to conduct your business with confidence.

Find out more

visit sophos.com/network.

United Kingdom Sales:
Tel: +44 (0)8447 671131
Email: sales@sophos.com

North American Sales:
Toll Free: 1-866-866-2802
Email: nasales@sophos.com

Boston, USA | Oxford, UK

A Sophos Whitepaper 12.11v1.dNA

SOPHOS