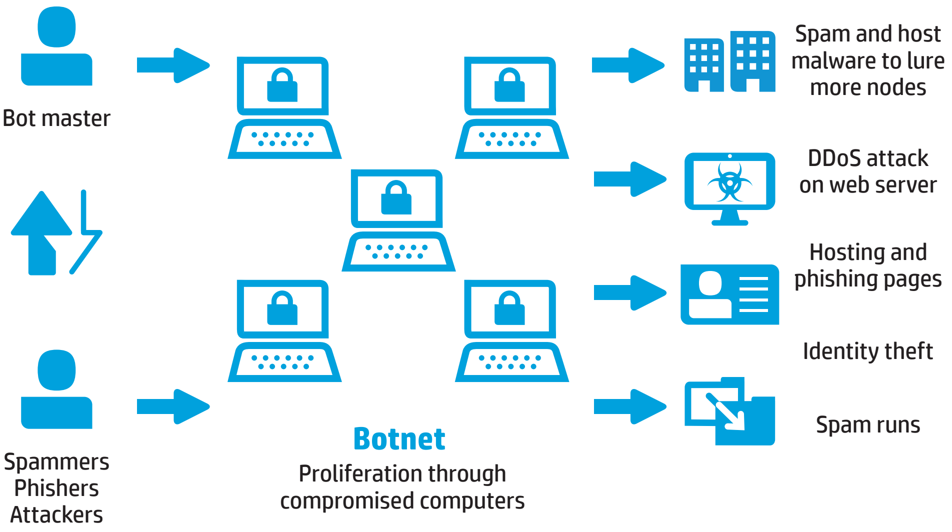
White paper

The bot threat

Enterprise security

The bot threat

Today enterprise networks can be attacked in a number of ways. None are more daunting than the Internet robot or simply, the bot. Bots are malicious code programs that are automated to infect a computer network. They can strike in so many different ways that traditional network security is often ineffective in blocking their destructive payloads. Bot infection methods include the downloading of a virus-infected program, infection via a worm, or more sophisticated methods such as a “drive-by” infection, in which users can self-inflict their systems by simply visiting a website. Since bots are self-propagating, they spread exponentially because each bot, in turn, attempts to infect and compromise more systems. As the collection of infected systems grows, it forms a network of bots, or a botnet.


Bot master
Spammers
Phishers
Attackers
Botnet
Proliferation through compromised computers
Spam and host malware to lure more nodes
DDoS attack on web server
Hosting and phishing pages
Identity theft
Spam runs

How a botnet works

Botnets are controlled by a master who has remote access and control of all the bots in a botnet. The botnet controller creates a command and control (C&C) site or uses Internet Relay Chat, an instant messaging protocol to issue commands to the bots in the net.

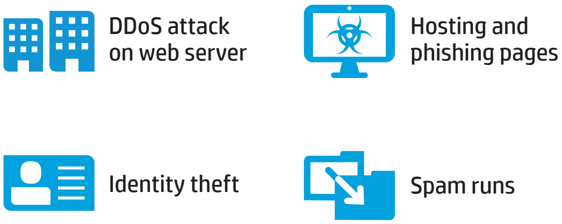
The botnet controller can either utilize this botnet for malicious purposes or sell this control to others who wish to do harm at directed targets. Examples of malicious actions from botnets include distributed denial of service (DDoS) attacks, malware, spyware, spam, and data theft.

Protecting against bots/botnets

Both the automated nature of bots and their varied infection methods make network protection a difficult task. Bots are becoming more sophisticated, tricking users into engaging in seemingly benign actions, such as clicking a link, while the bot is downloading malicious code in the background. Yet the most common method of exploit is also the oldest used by hackers—exploit of an unpatched system. Therefore, protection from bots must be managed across multiple vectors, utilizing devices and processes that act in unison.

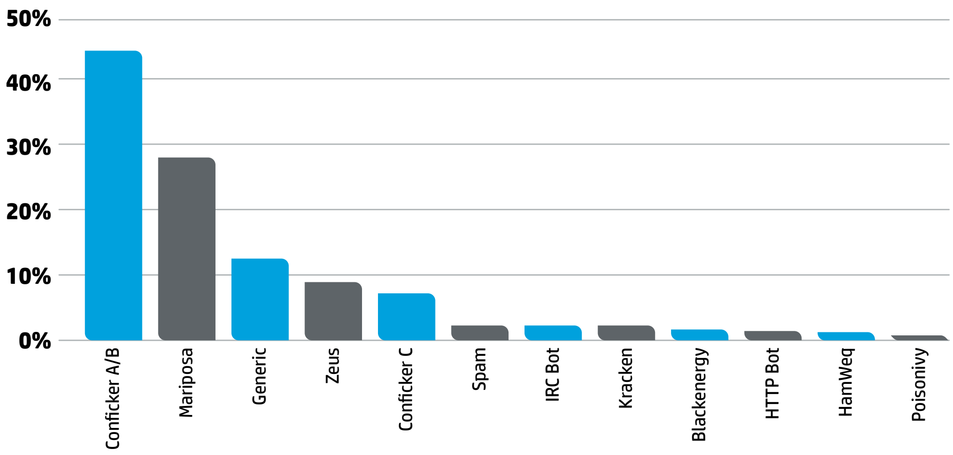
In order to fully protect the network from attacks generated by botnets, security professionals must first understand the dynamics of that threat. A strategic approach to protection starts with defining the methods of infection, and then, by using risk mitigation strategies, implementing protections. In defining the methods of infection, there are key common elements with all bots:

- First, bots exploit client-side vulnerabilities and compromise systems (that is, via binary deployment).
- Second, bots leverage intelligent control and communication most heavily (via various command and control configurations).
- Third, bots utilize variable payloads (malicious code and content, tools, and other means).
- And fourth, bots are controlled by the motives and drivers of the bot master (using directed attack as part of an advanced persistent threat, a consistent, ongoing set of attacks targeted at one organization or a random attack meant for sale or profit).



Botnets use a wide range of attack vectors.

Once those four bot commonalities are understood, organizations can create a strategic and focused plan of action for protecting their networks. The most fundamental is an effective security policy, where processes are in place to ensure that the network is protected through a system of checks and balances. In order to ensure the successful ongoing implementation of any security program, it is imperative to first determine the current state of security in the organization's network. After an assessment of the current security posture, organizations can then devise a step-by-step approach to patching and protecting vulnerable assets before they can be exploited. In addition to securing the physical network, organizations can further mitigate attacks through an educational campaign, promoting recommended procedures to help ensure security for the day-to-day network users.



Number of drones in several well-known botnets; HP 2010 Full Year Cyber Security Risks Report, April 2011.

The right strategy always wins

The key to addressing threats posed by botnets and their underlying attacks is a defense-in-depth security strategy where multiple layers of defense are used to effectively prevent direct attacks against critical systems. A well-designed strategy can block and delay attacks so various security measures have time to mitigate the consequences of a breach.

HP Enterprise Security Products (HP ESP) has invested considerable amounts of time, effort, and resources into formulating solutions for identifying and mitigating the risks posed by botnets and other malicious code attacks.

We enable our customers to protect their networks from infection with our network security solutions such as HP TippingPoint Next Generation IPS (NGIPS), powered by X-Armour, and Reputation Digital Vaccine (RepDV).

Leveraging our purpose-built HP TippingPoint NGIPS appliance, we can evaluate your network traffic and stop malicious content from breaching your network. And for those systems that aren't always up to date with the latest patches, our NGIPS can provide virtual patching to protect you from exploitation of these systems. RepDV enables you to block communication from known malicious actors on the Internet through a database of IP addresses and DNS entries. This database is updated continuously and is automatically delivered to your NGIPS, providing you with protection from rapidly changing threats.

As a respected solution leader in the security industry, HP TippingPoint discovers four times as many critical vulnerabilities as the rest of the market combined[1]. Through an ongoing, diligent security practice, education of users, partnership with the most admired and respected Intrusion Prevention System product company—HP TippingPoint and its DVLabs, and a proactive and pre-emptive service such as RepDV—enterprise organizations can be assured that they will minimize the risk of botnet infection in their networks while they protect both their critical assets and their reputation.

About HP

HP Enterprise Security is a leading provider of security and compliance solutions for modern enterprises that want to mitigate risk in their hybrid environments and defend against advanced threats. Based on market-leading products from ArcSight, Fortify, and TippingPoint, the HP Security Intelligence and Risk Management (SIRM) Platform uniquely delivers the advanced correlation, application protection, and network defense technology to protect today's applications and IT infrastructures from sophisticated cyber threats.

Find out more

For more information about network security, HP TippingPoint NGIPS, HP TippingPoint RepDV, and other industry-leading enterprise security products from HP, please visit the HP Enterprise Security website at **hpenterprisesecurity.com**.

[1] **Source** "Analysis of the Global Vulnerability Research Market," Frost and Sullivan, July 2011.

Sign up for updates
hp.com/go/getupdated