SOPHOS
Security made simple.

How to Ensure You're Not Part of the Next Botnet

Botnets are covert armies of compromised networked computers and devices (bots) that have been subverted by malware to enable remote control by a cybercriminal. Botnets are bred and nurtured by hackers to provide a powerful, dark cloud computing network used to conduct cybercrime attacks, like the recent DDoS attack against popular Domain Name Service (DNS) provider Dyn. This attack took down several flagship websites and significant parts of the internet for hours. The good news is, it's relatively simple to ensure your computers and devices aren't part of the next Botnet attack. This paper shows how you can protect yourself against the risk of botnet infection and easily identify any bots operating on your network and clean them up before they become part of the next cyberattack.

Botnets and the Internet of Things

The proliferation of mobile and network devices has created enormous benefits for us. We can now remotely access not only our computers, but our security systems, cameras, appliances, and a growing list of other devices that are now all interconnected with the cloud, enabling us to monitor and control them wherever we happen to be. Collectively referred to as the "Internet of Things" or IoT, these very affordable and easy-to-use devices enable a whole new level of control and efficiency in managing our world. However, as you can imagine, this massive collection of interconnected devices also represents an enormous opportunity for hackers who are continually looking to exploit new systems into their botnets.

The most troubling aspect to the growth of internet-connected devices is the lack of basic security considerations. It's bad enough that nearly every IoT device comes from the factory with default credentials (that owners rarely change), which provides malware direct login access in many cases. Recent estimates place the number of IoT devices out there still using default credentials at around 500,000.

However, what's particularly troubling is that many of these devices also have back-door support or diagnostics access credentials via Telnet or SSH that owners don't even know about. This enables devices to be exploited even if their owners do the right thing and use complex login credentials. And nearly every IoT device uses some variant of Linux, making it easy for hackers to find exploits or install malware on the devices to do their bidding.

With this massive new army of IoT devices joining the legions or previously compromised computers, cybercriminals are now armed with an unprecedented amount of computing power — computing power that can have a devastating effect when brought to bear, as we've just witnessed recently. As an example, the Marai-botnet, who's recent DDoS attack brought down much of the internet for a day, was estimated to be generating about 1Tbps.

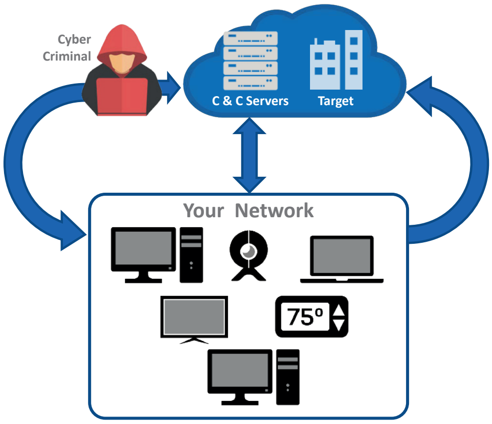
How botnets work and how to stop them

In order to understand how to identify and stop botnets, it's important to understand how they work — how they get started, how they spread, and how they operate.

Like any other malware, botnets start by entering your network through one of a few different conventional means:

- **Email attachments:** malware is often delivered as an email attachment as part of a spam or phishing campaign that attempts to have the user execute the attachment to kick off the initial exploit.

- **Web sites:** compromised websites often contain malware that can be silently executed by the browser, kicking off a chain of events that ends up exploiting a vulnerability on the system and infecting it.



- **Remote access:** IoT devices that are exposed to the internet, allowing direct login access with factory credentials, are the worst offenders, but hackers are not beneath brute force password hacking or exploiting known vulnerabilities in web interfaces to gain control of a device.
- **USB sticks:** while this infection technique is now almost legendary, there's still a clear and present danger that a user will foolishly plugin a USB device of unknown origin into their computer to see what it contains, only to introduce malware onto their system.

The malware used to infiltrate your organization can be extremely sophisticated and evasive. At Sophos, 70% of the malware samples we receive are unique to a single organization which is an unprecedented level of personalization. And the most sophisticated malware is constantly changing. This new breed of targeted malware makes protection more challenging, requiring behavioral analysis rather than historical signatures.

On the other hand, malware designed to exploit IoT devices can be extremely rudimentary, simply port scanning large portions of the internet looking for access opportunities and relying on default credentials or brute-force hacking to gain access. This is much easier to defend against, as it merely requires proper firewall configuration and protection.

Once malware has a foothold in your organization it will typically call home to the hacker's command and control (C&C) server to register its success and request further instructions. It may be told to lie low and wait, attempt to move laterally on the network to infect other devices, or participate in an attack. This attempt to call-home presents an ideal opportunity to detect infected systems on your network that are part of a botnet, but it requires the right technology to be effective.

Unfortunately, other than the call home communications, a bot on your network may be extremely difficult to detect. In most cases, the infected device will continue to operate normally or perhaps experience a slow-down in performance that might easily be attributed to any number of factors.

When a bot on your network is called into action to participate in an attack, it will typically communicate with the C&C server to get instructions such as the target and type of attack. This presents another ideal opportunity to identify the botnet hosts on your network. However, once an attack is underway, the attack itself can be very difficult to detect. From a network traffic perspective, the device will simply be sending emails (spam), transferring data (stealing information or mining bitcoins) or doing DNS lookups or performing a variety of other mundane traffic requests (used in DDoS attacks). None of these types of activities in isolation is particularly noteworthy or cause for alarm. Such is the nature of a botnet: any single bot in isolation is relatively harmless, it's the coordination of massive numbers of botnet devices all attacking the same target in parallel that makes the attack devastating.

Another very concerning aspect of botnets is that they are now being sold and rented on the dark web for very reasonable prices with full 24/7 tech support, enabling a new breed of unqualified cybercriminal with a fraction of a bitcoin to undertake malicious botnet attacks with little or no experience.

Location	Price
Botnet – Canada	$270 for 1,000 computers
Botnet – France	$200 for 1,000 computers
Botnet – Russia	$200 for 1,000 computers
Botnet – United Kingdom	$240 for 1,000 computers
Botnet – United States	$180 for 1,000 computers
Botnet – Worldwide	$35 for 1,000 computers

Source: http://www.havocscope.com/black-market-prices/hackers/

The impact of botnets

Botnets not only have a massive effect on the greater internet such as we witnessed recently with the crippling series of DDoS attacks, but they can also have a devastating impact on your organization, particularly if the objective is to steal sensitive information. Consider the impact the botnet had on the US retailer Target in 2013 that continuously siphoned millions of customer credit cards off point-of-sale systems over a period of months. And even if the botnet operating on your network is not after your data, it could be using your devices and network resources for nefarious purposes and cause devastating harm to another organization – perhaps an organization you do business with. So don't let your network become part of the next botnet attack.

How to protect your organization

The essential ingredient to effective protection from botnets is your network firewall. Look for the following components in a next-gen firewall to ensure you're getting the best protection possible:

- **Advanced Threat Protection:** Advanced Threat Protection can identify botnets already operating on your network. Ensure your firewall has malicious traffic detection, botnet detection, and command and control (C&C) call-home traffic detection. The firewall should use a multi-layered approach that combines IPS, DNS, and Web to identify call-home traffic and immediately identify not only the infected host, but the user and process. Ideally, it should also block or isolate the infected system until it can be investigated.

- **Intrusion prevention:** IPS can detect hackers attempting to breach your network resources. Ensure your firewall has a next-gen intrusion prevention system (IPS) that's capable of identifying advanced attack patterns on your network traffic to detect hacking attempts and malware moving laterally across your network segments. Also consider blocking entire Geo IP ranges for regions of the world you don't do business with to further reduce your surface area of attack.

- **Sandboxing:** Sandboxing can easily catch the latest evasive malware before it gets onto your computers. Ensure your firewall offers advanced sandboxing that can identify suspicious web or email files and detonate them in a safe sandbox environment to determine their behavior before allowing them into your network.

- **Web and email protection:** Effective web and email protection can prevent botnet recruiting malware from getting onto your network in the first place. Ensure your firewall has behavioral-based web protection that can actually emulate or simulate JavaScript code in web content to determine intent and behavior before it's passed to the browser. And ensure that your firewall or email filtering solution has top-shelf anti-spam and antivirus technology to detect the latest malware in email attachments.

- **Web Application Firewall:** A WAF can protect your servers, devices, and business applications from being hacked. Ensure your firewall offers WAF protection for any system on your network that requires remote access from the internet. A web application firewall will provide a reverse proxy, offload authentication, and harden systems from being hacked.

Best-practices to consider (both for your organization and for your home):

- Immediately change the default passwords for all your network devices to a unique complex password, and use a password manager if necessary.

- Minimize the use of IoT devices and keep your essential devices up to date. Disconnect any unnecessary devices, upgrade older devices to newer more secure models, and keep all your devices up to date with the latest firmware updates.

- Avoid IoT devices that require ports opened in your Firewall or router to provide remote access. Instead, use cloud-based devices that connect only to the cloud provider's servers and don't offer any direct remote access.

- Do not enable UPnP on your firewall or router. This protocol enables devices to open ports on your firewall on demand without your knowledge increasing your surface area of attack.

- Use secure VPN technologies to manage devices remotely.

The Sophos Advantage

Sophos XG Firewall provides all the latest advanced technology you need to protect your network from botnets, attacks and threats. You get Advanced Threat Protection, IPS, Sandboxing, web and email protection and a Web Application Firewall all in a single, high-performance network protection appliance that's easy to setup and manage.

Sophos XG Firewall also supports a wide variety of VPN technologies for secure remote access, including our unique Remote Ethernet Device (RED) technology that is like a secure virtual extension of your network to a remote device or branch office.

Sophos XG Firewall is also the first to introduce Synchronized Security with Sophos

Security Heartbeat™ that takes advanced threat protection and response to a whole new level, allowing you to immediately identify potential bots on your network and automatically isolate them until you have a chance to clean them up.

Only Sophos offers all the features you need plus features you can't get anywhere else in an appliance that's lightning fast and easy to manage.

Sophos can also protect your home

Sophos XG Firewall Home Edition and Sophos Home for your Macs and PCs offer business-grade protection for your home network... for free. You get the same trusted security that protects millions of business computers and networks world-wide free for your personal non-commercial use.

Start your free trial
of XG Firewall
www.sophos.com/xgfirewall

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

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

Australia and New Zealand Sales
Tel: +61 2 9409 9100
Email: sales@sophos.com.au

Asia Sales
Tel: +65 62244168
Email: salesasia@sophos.com

Oxford, UK

Registered in England and Wales No. 2096520, The Pentagon, Abingdon Science Park, Abingdon, OX14 3YP, UK