CyberGreen

A global community to measure and improve cyberhealth

Risk Mitigation for SpamBot Infections

Dec 2016

Agenda

1. Introduction
2. About SpamBot Infections
3. Mitigation recommendations for spam and other botnet infections
4. Making the case for implementing mitigations and securing email services

Introduction

When cyber infrastructure is insecure there is a risk to the global Internet community

Securing all end-user computing devices is critical to business productivity, but often overlooked

- Devices not properly secured are easily compromised, then controlled by third parties as part of a “botnet”
- When botnets send spam and viruses, it can represent a risk not just to the organization that owns those devices, but to the broader Internet community

About CyberGreen

- Global non-profit and collaborative organization focused on helping improve the health of global Cyber Ecosystem
- Working to provide reliable metrics and mitigation best practice information to Cyber Security Incident Response Teams (CSIRTs), network operators, and policy makers
- Mission: help CSIRTs and others focus remediation efforts on the most important risks
  - Help understand where improvements can be made
  - How we can achieve a more sustainable, secure, and resilient cyber ecosystem

Copyright (c) 2016, CyberGreen

CyberGreen

About Spambot Infections

What is a Botnet?

A botnet is a collection of computers which interact to accomplish some distributed activity on the Internet

Botnets are typically compromised devices that are under the control of an unauthorized and anonymous person, often called a botnet herder

Owners of compromised devices generally have no idea someone else controls their device

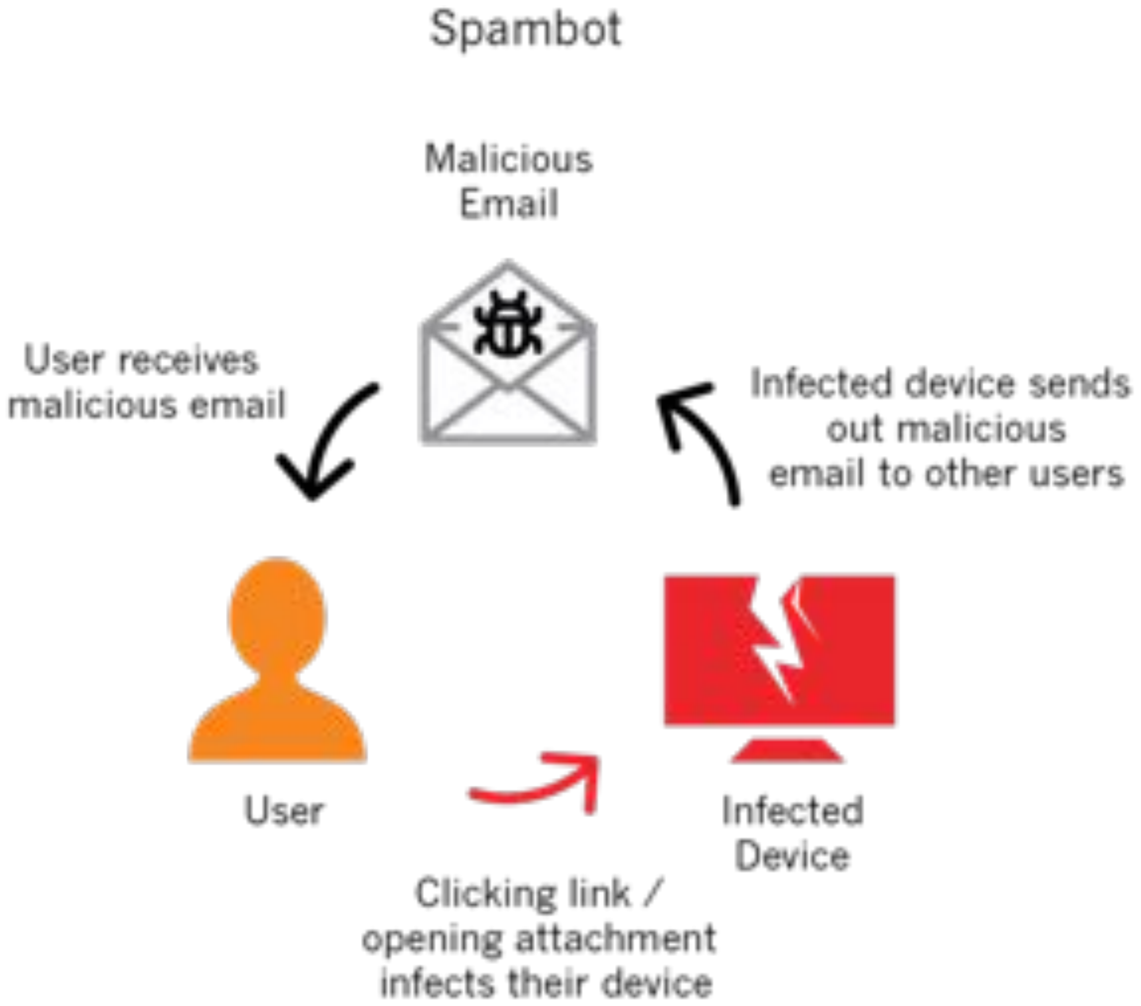
Spam Botnet Infections

Spam botnets send spam and malware, delivering a malicious payload either through a file attached to spam messages or by embedding a link to an infected website

Criminals use both traditional email, instant messages (IMS) and text messages in their spam campaigns

A company with many compromised devices that are part of spam botnets has a “spambot infection”

The spambot cycle


Spambot
Malicious Email
User receives malicious email
Infected device sends out malicious email to other users
User
Infected Device
Clicking link / opening attachment infects their device

Risks posed by spambots

A compromised machine in a botnet may have other malware installed, spread malware to other machines in your network or to other targets outside your network

- Adversaries get further inside your network
- Service degradation, interruption or failure
- User credentials or other sensitive data exposed

Botnets can affect Windows, Mac and Linux operating systems, as well as mobile devices

Spambots in Distributed Denial of Service (DDoS) attacks

In DDoS attacks, the attacker abuses tens of thousands of spambot devices to create large floods of traffic with the goal of exhausting the victim's bandwidth

DDoS attacks also abuse the User Datagram Protocol (UDP) traffic, using protocols such as DNS allow spoofing of sender IP addresses

- UDP responds to requests without validation of sender identity, i.e. IP address
- UDP traffic can be spoofed (i.e. have a misleading apparent source IP address): attacker can hide true identity

Real life botnet infection

A hospital[1] had a botnet infection so severe, activity from infected machines interrupted the hospitals computer network with impacts including:

- Doors to operating rooms would not open
- Pagers were interrupted
- Computers in the intensive care unit were shut down

[1] http://www.eweek.com/c/a/Security/DOJ-Indicts-Hacker-for-Hospital-Botnet-Attack (accessed 9/16)

Real spambot in DDoS attack

In 2009,[2] an Internet Service Provider was on the receiving end of a 25 Gb/s DDoS attack (DNS amplification and reflection), which peaked at 30 Gb/s in aggregate

- Over one million spam botnet infected devices were used in this attack, which totally flooded the victim's network and took them offline, thereby disrupting their business

[2] http://www.team-cymru.org/Open-Resolver-Challenge.html (accessed 9/16)

Potential impacts from spambot infections

Productivity

- Sending spam and viruses consumes processing power and bandwidth on infected hosts, causing poor performance
- In large infections, spam botnets can consume enough bandwidth that services are disrupted for legitimate users, a particular concern for:
  - — Seasonal operations, *e.g. online retailers where most sales happen between Thanksgiving and New Years*
  - — Time sensitive operations, *e.g. healthcare, colleges with limited onli registration periods or online wagering on sporting events, etc.*

Other potential spambot infection impacts

Brand

- Loss of reputation with customers and partners
- Becoming known as a “spam magnet” in global community

Technical

- Network services interrupted
- “Blacklist” and isolation of infected network by network providers from the rest of Internet as part of the Internet community’s effort to stop email spamming

CyberGreen

Mitigate risks from spambot infections

Mitigation options vary by environment

Not all mitigation best practices are appropriate for all environments

CyberGreen provides information relevant to four basic environmental profiles

Look for these icons to find mitigations for your environment

1. Consumers
2. Companies
3. ISPs
4. Policy Makers

Find out if your network is already infected with botnets

Shadowserver will provide any network with daily reports on the botnet infections seen for a specific IPv4 or IPv6 address block: http://www.shadowserver.org/wiki/pmwiki.php/Involve/GetReportsOnYourNetwork

Note: Shadowserver scans will only hit IP space that is not firewalled and they do not claim 100% accuracy in their Command & Control downloads, so there may be false positives in Shadowserver IRC intelligence

Is your IP address part of a blacklist?

Identify your IPv4 or IPv6 address by visiting these websites:

- http://ipv4.whatismyv6.com/
- http://ipv6.whatismyv6.com/

Check those IPs at http://multirbl.valli.org/

- Or click on individual IP address links that appear on the site

Stay alert for new or increasing infections

A complete list of all techniques is beyond the scope of this document

- Shadowserver has a comprehensive list of tools and techniques to monitor your network and detect botnets

https://www.shadowserver.org/wiki/pmwiki.php/Information/BotnetDetection

Mitigation: Notify users and clean up infected machines on your network

All organizations, including ISPs, need to clean up infected hosts

Use “nuke and pave” to be sure the device is secure:

1. Reformat or reinstall system from scratch using original media
2. Ensure that operating system patches are applied
3. Ensure adequate host protections (anti-virus and host firewall) are installed and configured with updated signatures/definitions
4. Restore user files and applications from clean backups or original media. Be sure to patch *all* installed applications

Do each step BEFORE connecting the host to the Internet

If you don’t already have this software available locally on your network, you should connect to the Internet via a hardware firewalled-connection to download software and/or updates

ISPs: Communicate with customers

Communicate with customers about what you are doing and WHY, using these notification methods

- Email
- Phone calls
- In-browser notifications such as "walled gardens" (i.e. notify customer "your account is temporarily suspended due to…")

Actively educate customers about the threats, their responsibility as computer owners, and measures taken by ISP to reduce risks

Mitigation: Practice basic computer hygiene

Practicing basic computer hygiene is essential to reducing the risk of all malware infections

It also enables you to recover quickly when a computer does become infected

Basic computer hygiene protects against many different types of malware used to create today's botnets

Computer hygiene: Backups

Regular, complete backups of all devices and data are essential

Multiple generations of backups should be retained:

- If most recent backup is no good, a prior version exists
- Minimizes amount of data that may be lost

Computer hygiene: Host-based firewall

Modern operating systems come with a basic host-based firewall that should be turned on **BEFORE the computer is connected to the Internet,** particularly if there is no separate firewall at the point of connection to the Internet

Stand-alone firewall applications from reputable firewall vendors:

- http://www.pcmag.com/article2/0,2817,2487059,00.asp
- http://www.techradar.com/news/software/applications/the-best-free-firewall-software-of-2015-stop-malware-before-it-gets-you-1284587
- http://www.techradar.com/news/software/applications/7-of-the-best-linux-firewalls-697177

Computer hygiene: Anti-virus

If you don't already have anti-virus (AV) software, or if you believe a computer is infected but your current AV does not detect a virus, find an AV here:

- http://www.pcmag.com/article2/0,2817,2388652,00.asp
- http://www.techradar.com/news/software/applications/best-free-antivirus-1321277

DO NOT run MORE THAN ONE anti-virus at a time

If you want to try running multiple products, download one, run it, uninstall it, download the next, run it, uninstall it, etc.

Computer hygiene: Images with secure configurations

Build Operating System images with secure configurations, i.e. with anti-virus and firewalls already installed

- Greatly reduces time needed to completely rebuild a computer from a trusted source
- Often the only way to ensure all malware is eliminated on a device and that it is able to protect itself from re-infection

Computer hygiene: Protect mobile devices

Mobile devices may be infected and used as Spam bots, particularly if they connect to insecurely configured wireless networks (Wi-Fi)

Mobile devices may also send SMS text messages through cellular networks to other mobile devices or Premium SMS numbers

- High volume usage may result in additional charges
- Premium SMS numbers always result in additional charges

Computer hygiene: Protect mobile devices

Mitigations for mobile similar to PCs:

- Always keep device operating system and installed applications up-to-date
- Don't download or install software from non-approved sources
- Be aware of flash scam messages with fake AV or other content that directs you to a fake store with fake AV or other malicious software
- Ask cell provider to block all Premium SMS messages to mobile device

Mitigation: Implement email authentication with SPF and DKIM

Sender Policy Framework (SPF) and Domain Keys Identified Mail (DKIM) email authentication protocols that make it harder for spammers and cyber criminals to spoof where an email comes from

Domains with email authentication are less attractive to phishers

- Less likely to be blacklisted by spam filters
- Ensures legitimate email from that domain is delivered

Mitigation: Implement email authentication with SPF

SPF allows domain owners to specify which mail servers are used to send email from that domain

- Provides a mechanism to allow receiving mail exchangers to check that incoming mail from a domain comes from a host authorized by that domain's administrators

SPF specifications, configuration and deployment information:

https://tools.ietf.org/html/rfc7208

http://www.openspf.org/Project_Overview

https://www.digitalocean.com/community/tutorials/how-to-use-an-spf-record-to-prevent-spoofing-improve-e-mail-reliability

Mitigation: Implement email authentication with DKIM

DKIM allows messages to be transmitted in a way that can be verified through cryptographic authentication by mailbox provider

- Email providers who validate DKIM signatures can use information about signer to limit spam, spoofing, and phishing
- DKIM can ensure messages not modified or tampered with in transit

DKIM specifications, configuration and deployment details:

https://tools.ietf.org/html/rfc6376

http://dkim.org/

Mitigation: Implement secure configuration of email services

The Messaging Anti-Abuse Working Group (MAAWG) recommendations to implement a secure configuration of email services focus on:

- Locking down access to SMTP port 25
- Requiring authentication for email as provided in Internet Engineering Task Force (IETF) RFC 2254
- Use email submission services on port 587 as described in IATF RFC

Recommendations available at: https://www.m3aawg.org/sites/default/files/document/MAAWG_Port25rec0511.pdf

Additional configurations for ISPs

Block email ports at the customer’s modem, i.e. block outbound port 25 to prevent direct-to-mx spam

Block outbound port 25 from residential users to any mail server other than the ISP’s; this forces spam bots to use ISP-owned mail servers

Perform outbound spam filtering and bot detection on ISP mail servers - this can be particularly effective in conjunction with the prior blocking tactics

Other mitigations for ISPs

If blocking ports isn't possible, ensure that recipients can distinguish residential IP addresses from commercial ones

Assign reverse DNS to residential IPs that marks them as such, and publish the naming convention

Proactively provide residential CIDR block lists to blocklist providers such as the Spamhaus Policy Block List (PBL) at https://www.spamhaus.org/pbl/

Rate limit UDP fragments

Mitigation: Implement RFC 7489 DMARC

IETF RFC 7489, “Domain-based Message Authentication, Reporting, and Conformance (DMARC)

DMARC designed to help combat spam and phishing by enabling email senders and receivers to determine whether or not a given message is legitimately from the sender, and **what to do if it isn’t**

Builds on widely deployed DKIM and SPF validation systems: if message satisfies checks it is sent through to recipient, otherwise it’s quarantined or rejected

DMARC

DMARC is supported by all four major email providers: Google, Microsoft, Yahoo and AOL. It has also been implemented by services like Facebook, PayPal, Amazon and Twitter.

More information about DMARC is available at:

- https://dmarc.org/
- https://dmarc.org/overview/
- https://dmarcguide.globalcyberalliance.org
- https://tools.ietf.org/html/rfc7489

Verify your fix

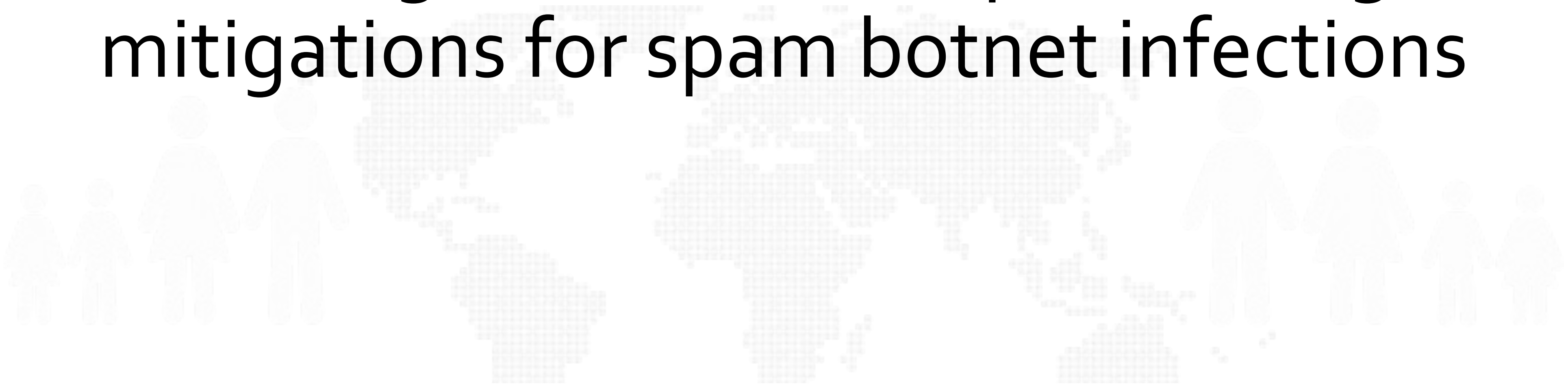
After implementing your mitigation measures, monitor your infrastructure to prevent re-occurrence by subscribing to free reports from Shadowserver:

https://www.shadowserver.org/wiki/pmwiki.php/Involve/GetReportsOnYourNetwork

Additional resources about spambots

- Check your local CERT and your AV vendor announcements for identified malware infection
- https://www.shadowserver.org/wiki/pmwiki.php/Information/Botnets
- http://www.senki.org/sp-security/monitoring-network-malware-spam-botnet-infections/
- https://www.spamhaus.org/

Making the case for implementing mitigations for spam botnet infections



Making the case for mitigations

Help everyone understand the level of effort needed to improve cyber health in their community

Why should you implement the mitigations in your environment?

1. It is the right thing to do as a good Internet neighbor
2. Your organization may be next to be attacked

Let's join together and stop bad guys from winning!

Changing risk landscape

Increased need to demonstrate "due care"

- Obtaining cyber insurance
- Complying with risk frameworks to win business with local / national governments and large corporations

If we (***you!)*** don't do a better job of securing our own infrastructure and reducing cyber risk, government regulation may force additional mandates and/or penalties

Anticipated organizational benefits

Increased productivity

- Fewer service interruptions and failures

Improved network performance

- Existing network more reliable and resilient, with greater capacity

Improved brand reputation

- Technical reliability and security a selling point to customers

More anticipated benefits

Decreased budget uncertainty

- Fewer unanticipated usage costs for IT
- Budget can be used as planned, e.g. upgrading technical capability / capacity, personnel, etc.

System admins may spend less time spent trying to deal with unexpected problems

- May improve their productivity and reduce unexpected overtime

Benefits for ISPs and Email Providers

Identify the party responsible for submitted messages

Reduced costs for abuse help desk, customer support, and network operations centers

Improved deliverability for legitimate email messages, due to reduced risk of being blacklisted

New abilities:

- Enforce acceptable use policies, terms of service for email submission
- Monitor and limit transmission rates, per customer and/or in aggregate
- Offer premium tiers of service to customers with business need to operate email servers with direct access to port 25

What do you need to implement these mitigations?

Commands and configuration details for most important mitigations are publically available

- No additional software must be purchased
- Implementing mitigations does not require any special knowledge, skills, or abilities

Note: All mitigations should be carefully reviewed in light of your specific business requirements and infrastructure environment before proceeding

All organizational change management processes, including testing, should be followed

How long will mitigations take?

Clean restore of a host may take an hour or two when secure OS images readily available for automatic rebuild

- Does not include time to install or restore user applications and data, assuming data was backed up

Manual installation from media will take several hours per host

ISPs and large entities can automate administration of changes via configuration management systems with task execution (Salt, Ansible)

How long will it take?

Technical teams may need several days to weeks to plan and execute each individual component of the secure configuration for email services recommended by MAAWG or to implement DMARC

Bonus: with no real maintenance, the recurring cost is effectively zero!

Acknowledgement

CyberGreen would like to thank the experts who made the creation of this document possible:

Written by:

- Laurin Buchanan, Applied Visions, Inc. – Secure Decisions Division

Contributed and Reviewed by:

- Matt Carothers, Cox Communications
- Baiba Kaskina, CERT.LV
- Moto Kawasaki, JPCERT/CC
- Art Manion, CERT/CC
- Yoshinobu Matsuzaki, IIJ
- Joe St Sauver, Farsight Security
- David Watson, ShadowServer Foundation

Disclaimer: CyberGreen believes this guidance and the advice from our experts should be of benefit to anyone mitigating a risk conditions, but it is not advice specific to any reader or network. Ultimately, each reader is responsible for implementing his or her own network remediation strategy and we assume no responsibility or liability therefore.

CyberGreen

For more information about risk mitigation best practices please contact: contact@cybergreen.net