Messaging, Malware and Mobile Anti-Abuse Working Group

M3AAWG Companion Document: M3AAWG Bot Metrics Report — Report #1 — 2012 and 2013

Version: 1.0

September 2014

The direct URL to this paper is: www.m3aawg.org/dns-crypto-recipes

This document is intended to accompany and complement the companion document, "M3 AAWG Tutorial on Third Party Recursive Resolvers and Encrypting DNS Stub Resolver-to-Recursive Resolver Traffic" (www.m3aawg.org/dns-crypto-tutorial).

This document was produced by the M3 AAWG Data and Identity Protection Committee.

Table of Contents

Messaging, Malware and Mobile Anti-Abuse Working Group

781 Beach Street, Suite 302
San Francisco
California 94109
United States of America

www.m3aawg.org

1. Executive Summary

This is the first industry report with data provided directly by service operators and ISPs detailing the number of subscribers identified as having a system infected by malware, also known a “bot,” and the percentage of those subscribers notified of the problem. It is the first cooperative effort by network service providers to quantify the extent of malicious bots infecting their subscribers. The Messaging, Malware and Mobile Anti-Abuse Working Group will periodically issue updated reports.

Based on the data provided to M^{3}AAWG, in 2012 participating network operators reported the number of infected subscribers ranged from .84 % to 1.18 % with 99.13 % to 99.21 % of those subscribers being notified they had a bot. In 2013, the number of infected subscribers varied from 1.04 % to .80 % with 99.82 % to 93.99 % of consumers being notified.

2. About the M[3]AAWG Bot Metrics Program

These metrics are the first cooperative effort by the network companies that directly provide end-users Internet access, and thus see the data first hand, to quantify the extent of malicious bots afflicting their subscribers. The metrics cover only end-user connections and do not include enterprise business networks.

This is a voluntary program with data provided confidentially by ISPs and service providers. The data is shared at the discretion of each company and is reported here as aggregated monthly metrics summarized by quarters. While the report represents the contributions of ISPs and network operators working within M[3]AAWG to address malware and bots, M[3]AAWG members are under no obligation to supply this information or to participate in this program.

The M[3]AAWG Bot Metrics Program is an objective tool for tracking industry and government efforts at controlling the spread of bots and we are committed to continuing this important work. Similar to the M[3]AAWG Email Metrics Report on abusive messaging, we expect these reports will become an important resource for understanding the extent of bot infections and to measuring the effectiveness of the industry's efforts to protect end-users.

3. Observations

While definitions of bots can differ from country to country, the metrics below report on malware, or malicious code, discovered by a network operator while processing a subscriber's email or other Internet activities. Bots are installed directly on end-users' systems, often without their knowledge. Once deployed, the "botted" machine can be controlled by commands from a "bot master," a person who uses infected machines as a network to send spam or carry out fraudulent activities. The malicious code is often designed to run in background mode, so subscribers are usually unaware their systems are infected.

While Internet service providers and network operators are able to identify infected users on their networks, subscribers must remove the malware from their systems. Based on the data in this report, network operators are notifying about 98.7 % of end-users when they are infected. This points out the importance of the entire Internet ecosystem working together to address this problem, including security software vendors and end users.

4. Report #1—2012 and 2013 Results Summarized by Quarter

The statistics reported below are compiled from confidential monthly data provided by participating M[3]AAWG member ISPs and network operators summarized here by quarter from 2012 through 2013. Our reporting basis covers a quarterly average of up to 43.5 million subscribers.

2012	**Q1 2012**	**Q2 2012**	**Q3 2012**	**Q4 2012**
Subscribers Represented	37,707,435	37,358,206	36,991,516	37,383,662
Subscribers Deemed Infected	317,064	402,585	249,492	440,746
% Infected	0.84 %	1.08 %	0.67 %	1.18 %
Infected Subscribers Notified	314,295	400,439	245,522	437,253
% Notified	99.13 %	99.47 %	98.41 %	99.21 %
2013	**Q1 2013**	**Q2 2013**	**Q3 2013**	**Q4 2013**
Subscribers Represented	37,270,265	37,735,195	37,639,022	43,550,674
Subscribers Deemed Infected	388,152	435,921	493,572	346,615
% Infected	1.04 %	1.16 %	1.31 %	0.80 %
Infected Subscribers Notified	387,221	435,149	492,382	325,787
% Notified	99.76 %	99.82 %	99.76 %	93.99 %

5. What is Measured?

- **Number of Subscribers**
  The number of specific subscribers on a network. Each subscriber may represent more than one end-user or include multiple devices.
- **Infected Subscribers**
  This is the count of unique subscribers identified to be infected in each reporting period.
- **Percent of Base Infected**
  Calculated from above: Infected Subscribers divided by Number of Subscribers
- **Total Number of Infected Subscribers Notified**
  The number of unique subscribers notified of a bot by any method, including text message, phone call, email, Web redirection or browser notification, and postal mail. Multiple notices sent to the same subscriber are counted as one. This does not imply that the subscriber received or read the notice.
- **Percent Notified**
  Calculated from above: Infected Subscribers Notified / Infected Subscribers

As with all M3AAWG documents that we publish, please check the M3AAWG website (www.m3aawg.org) for updates to this paper.