M3AAWG
MESSAGING MALWARE MOBILE

Solutions from Around the Globe

Moderated by Kevin Sullivan, Microsoft
October 29, 2012

Global Solutions: Patterns & Practices

M3AAWG
MESSAGING MALWARE MOBILE

- Botnets (and other online threats) are criminal problems that require a multidisciplinary approach to solve. No one part of the Internet ecosystem can adequately address botnet and malware threats.
- Criminals move fast and face few of the constraints that we do as businesses and governments. We need to address barriers to collaboration to ensure that we are keeping up with changing threats.
- The most interesting solutions may come at the intersection of different sectors and require careful balancing of social, economic and political concerns.
- Opportunity to build upon others' success, refine ideas, and foster greater adoption of practices that help protect customers.

Shared Responsibility

M³AAWG
MESSAGING MALWARE MOBILE

Everyone Plays a Role

Anti-virus and security vendors, application and operating system developers, device manufacturers, domain registrars and registries, end users, Internet service and cloud service providers, IT departments, public-private partnerships, search engines, website owners and others

Employ relevant technologies and practices across lifecycle phases

PREVENT	DETECT	NOTIFY	REMEDIATE	RECOVER

Educate and empower customers

Share information, lessons learned and resources

Source: http://industrybotnetgroup.org/

Preview of today's topics

- Adopting models from other sectors, such as public health
- The science of cybersecurity
- Cleaning up spam and other issues to improve international reputation rankings
- Global metrics programs to asses the size of malware and spam problems and efficacy of efforts to address them
- Specific practices from ISPs, ESPs, CERTs, software vendors, and other stakeholders to curb malware, mobile and messaging abuses.

Today's Panelists

- Dr. Greg Shannon, Chief Scientist, CERT at Carnegie Mellon
- Samarth Saxena, Co-founder & COO, Octane Marketing (P) Ltd
- Jerry Upton, Executive Director, M^{3}AAWG

Outcome Validity for Best Practices

- Operational Validity
  A result (report, technology, capability, practice, policy, or process) is operationally valid when it delivers in practice the measurable properties it was intended to deliver.
- Hygiene, Hygiene, Hygiene – know, watch, tweak

M3AAWG
MESSAGING MALWARE MOBILE

Messaging & Bot Metrics

Jerry Upton
M3AAWG Executive Director
October 29, 2012

Messaging Abuse Metrics Program

- Quarterly report intended as a *guide to understanding the industry's efforts in obstructing abusive emails* before they reach users and to identify related trends over time

- 1st report covered Q4 2005. M3AAWG only reports if more than 100 million mailboxes are reported

- Provides an unbiased look at the scope of email abuse prevention from the mailbox operator's perspective

- Measurement seen to be key to evaluating "effectiveness" of policies, legislation, technical solutions, and to determine "effectiveness" of strategy and future changes

Basic Rules

- Voluntary participation
- Participants must be M³AAWG members and be responsible for operating end-user mailboxes
- Should commit to report metrics quarterly for 2 years, though a company may drop out if there are reporting problems
- Companies may be added anytime and should provide at least 2 quarters of reports for consistency
- All reports confidential; Executive Director receives reports and aggregates data
- Publication on M³AAWG website

What's being collected?

- **Number of mailboxes represented**
  - total # of mailboxes at the end of the quarter
- **Number of unaltered delivered email**
  - not blocked or tagged in any way by mailbox operator's anti-abuse efforts
- **Number of dropped connections & blocked / tagged inbound email**
  - using Anti-Spam/Anti-Viral framework, other recipient or message based rules, but not MUA (Mail User Agents)
  - now assuming 1 email per dropped connection

Please note: We now only publish the data as percentages or ratios. The aggregate raw date is not shown as the revisions of the raw data are frequent.

Metrics Report

M³AAWG
MESSAGING MALWARE MOBILE

The metrics in the report do not represent spam, but indicate the volume of email identified as "abusive." This report covers more that 400 million mailboxes with 300 billion unaltered emails delivered.

Key Historical Ratios	Report #16 Q2 2012	Report #16 Q1 2012	Report #16 Q4 2011	Report #15 Q3 2011	Report #15 Q2 2011
Dropped Connections & Blocked/Tagged Inbound Emails per Delivered Mail Or Ratio of Dropped Connections & Blocked/Tagged Inbound Emails to Unaltered Delivered Email	7.64 or 88.4% abusive email	7.14 or 87.7% abusive email	6.83 or 87.2% abusive email	7.90 or 88.8% abusive email	7.22 Or 87.8% abusive email

Bot Metrics: What and Why?

M3AAWG
MESSAGING MALWARE MOBILE

What?

A quorum of global ISPs who will anonymously submit data to permit factual sizing of botnets and their locations around the world. The published metrics will serve as an objective tool for tracking the industry's and governments' efforts at controlling the spread of botnets.

Why?

- Educate public policy makers with M3AAWG bot metrics to help frame the policy debate
- To assess the efficacy of efforts to reduce bot infections
- Provide a reliable view of the problem from those who own the data and see the issue first hand
- Avoid prescriptive regulatory approaches that will impede innovation in fighting botnets and other malware

How Does the Program Work?

M3AAWG
MESSAGING MALWARE MOBILE

Basic Rules

- Voluntary participation
- Participants must be responsible for providing Internet access
  - We also work with non-ISPs who have a view of the problem (OS, AV, DNS, etc.)
- Should commit to report metrics quarterly for 2 years, though a company may drop out if there are reporting problems
- Companies may be added anytime and should provide at least 2 quarters of reports for consistency
- All reports confidential; Executive Director receives reports and aggregates data
  - Should have a standard NDA available
- Publication on M^{3}AAWG website
  - After formal program established

Pilot Phase

- Requesting monthly data to tune the program
- Targeting 50 million aggregate subscribers
- Send data to M^{3}AAWG Executive Director starting with November data set

The Data Collected

Phase 1 - Pilot

M3AAWG
MESSAGING MALWARE MOBILE

Metric	Notes
Total # of subscribers	This should be the number of subscribers for the business division being reported here. For example, you might not collect metrics from fiber links, etc.
Infected Subscribers	Count of unique subscribers with infections discovered in reporting period.
Percent of base infected	*(calculated from above)*
Total number of infection notices delivered	How many unique subscribers were notified of a problem by any means (SMS, phone call, email, web redirection/browser notification etc.) Multiple notices to the same subscriber count as one. This does not imply that the subscriber has read/received the notice.
Percent Notified	(*calculated from above)*

Bot Metrics Pilot Data

- Pilot Data for 2012 – not for publication as the sample needs additional validation

Where We Stand & Next Steps

M³AAWG
MESSAGING MALWARE MOBILE

Initial Findings

- This is difficult, but possible!
- … but we've identified some challenges
  - Definition of a bot (vs. malware, adware, etc.)
  - Differing detection methods
  - Frequency of measurement
  - How to normalize data sets

Next Steps

Email KevSull@microsoft.com for more answers

Begin submitting pilot data

– contact Jerry Upton, jerry.upton@m3aawg.org

Messaging Abuse Metrics

- **Questions**

Thank You

M3AAWG
MESSAGING MALWARE MOBILE

DISCUSSION

Call to Action

- Evaluate cross-sector solutions and document your experiences and successes.
- The data to help you get started largely exists. Use it, share feedback with the providers of data. Feedback loops improve our overall effectiveness!
- Contribute to global metrics efforts that help build a baseline for size of the problem and benchmarks to evaluate potential solutions.

M3AAWG
MESSAGING MALWARE MOBILE

THANK YOU!