Messaging, Malware and Mobile Anti-Abuse Working Group

M^{3}AAWG Feedback Reporting Recommendation

February 2014

Introduction

Fighting abuse on the Internet has long relied in large part on the reporting of abusive behavior to the emitter of that abuse. Evidence presented to a network or domain owner of possibly compromised machines or accounts that are emitting abusive traffic (e.g., spam, phish, viruses, etc.) allows the owner to take necessary action to stop the problematic traffic. Just as speaking a common language allows two people to communicate effectively, standards that define not only the format of abuse reports but also the destination address for them increase the effectiveness of network owners in fighting abusive traffic.

M^{3}AAWG acknowledges the widespread use of the Abuse Reporting Format and recommends:

- Abuse email addresses should support the unfiltered reception of reports in Abuse Reporting Format (ARF).
- Reporters should use ARF to report messaging abuse to the extent of their capabilities.
- All organizations that own a domain name or are responsible for any segment of the public Internet should maintain an RFC 2142 email address for receiving abuse reports (abuse@domain) and should monitor and act on reports made to that mailbox. This address should be published in WHOIS for all to find.

To support a full spectrum of abuse reporting, M^{3}AAWG asks for implementers to also support Extended Abuse Reporting Format (X-ARF) when reporting types of abuse other than email.

This document will not attempt to restate the comprehensive information in RFCs 2142, 3912, 5965, 6449, or 6650, nor what's in the Regional Internet Registries' policies on abuse points of contact. Rather, it is expected that the reader is, or will become, familiar with those documents in order to best understand the context for the recommendations in this document.

Benefits of ARF

The ability to automate repeatable processes leads to gains in the efficiency of those processes, and the ARF standard is designed to allow for automation of the processing of abuse reports. It defines a format for reporting abuse messages that is designed to be easily parsed by machine-based methods. It also encapsulates any potentially dangerous payload in an attachment ensuring it will not be automatically loaded (and executed) if it ends up on a typical email client.

Who Should (and Should Not) Send ARF Reports

M^{3}AAWG strongly recommends that anyone sending automated abuse reports use ARF for reporting emails and X-ARF for reporting other network abuse incidents. The phrase "automated abuse reports" here refers to reports generated when a mailbox provider's customer initiates a "Report Spam" action, usually through a button pressed in the email client interface. Such an action should set in motion a mechanism that causes the complained-about message to be correctly encapsulated in an ARF report and routed to the correct destination for the report with no further action on the part of the customer.

That said, M^{3}AAWG recognizes that not all sites have the resources to put such systems in place; smaller entities (e.g., one that hosts mail for just a handful of users) are unlikely to have the capability to do so. M^{3}AAWG further understands that not all reports are suitable to be reported in ARF (or X-ARF). Unsuitable reports might include those focused on harassment, copyright violations, notice of blocks on IPs and domains, etc. Therefore, M^{3}AAWG recommends that all parties make use of ARF to the extent that their capabilities and circumstances allow.

Where to Send ARF Reports

ARF reports should be sent to entities that are not only responsible for the message that generated the complaint but also are willing to take action in response to the complaint. In many cases, this claim of responsibility will be made through a private agreement between two parties, usually through enrollment by one party in the other's feedback loop (FBL), in keeping with RFC 6449. A FBL enrollee will typically specify an address other than its RFC 2142 abuse@domain address as the destination for ARF reports and M^{3}AAWG strongly recommends that they do so. A separate mailbox for ARF reports both allows full control of traffic into the mailbox, since only known senders are permitted, and enables full automation of the mailbox processing, since all messages to that mailbox should be in ARF.

The obvious limitation inherent in such arrangements is that both parties must have some kind of pre-existing relationship in order to establish the feedback loop. At the time of this writing, there is no standardized method for advertising an address specifically intended to receive and process ARF reports. A currently expired RFC exists that defines such a method (draft-ietf-marf-reporting-discovery-01), but unless and until this work is re-chartered, a prior arrangement is the only way to establish such an address.

If no such arrangement exists and a domain can be reliably identified (e.g., DKIM-authenticated traffic has been seen from that domain), then the RFC 2142 abuse address for this domain is the correct address to send ARF reports. Additionally, whether or not the domain can be reliably identified, the ARF report can be sent to the abuse address associated with the IP address of the last server connecting to the receiving MTA. Those addresses can be discovered through the use of WHOIS (RFC 3912) and automated methods are available to execute WHOIS queries to make report routing decisions. For those who require automated lookups or a high volume of queries, there exist commercial abuse contact databases. These databases can be discovered by doing an Internet search for "abuse contact database."

To further establish their validity and strengthen the trusted relationships established by feedback loops, M^{3}AAWG recommends that organizations generating ARF reports consider authenticating those reports by using SPF, DKIM or other such protocols.

Receiving and Processing ARF Reports

M^{3}AAWG expects that organizations enrolling in FBLs will have a dedicated address or addresses for receiving inbound ARF reports. As stated earlier, such a mailbox allows full control of traffic into the mailbox and full automation of mailbox processing. ARF is, by its nature, designed to be machine-parseable and consumers of ARF reports must take advantage of this.

M^{3}AAWG recognizes that ARF reports may arrive at an organization's published abuse address, rather than the established ARF mailbox, and so recommends that tools be put in place to handle this eventuality. Since ARF reports come in a recognizable, machine-parseable format, it is possible to install a tool to pre-process inbound mail to the abuse address and optionally route ARF reports differently than those not in ARF. Some vendors have dedicated products for handling abuse emails, or such tools can be home-grown. If an abuse desk is receiving a significant volume of ARF reports from a known party, it may be beneficial to engage that party in a private agreement to send such reports to a dedicated ARF mailbox.

Regardless of the existence of dedicated mailboxes for ARF reports or tools for handling them, M^{3}AAWG strongly recommends that all inbound messages sent to an organization's abuse address be processed appropriately, in keeping with their content and format.

Conclusion

ARF is a mature, established standard for reporting abuse and one that makes it easy for all organizations to handle today's volume of abuse complaints by automated means. M^{3}AAWG contributed to the codification of this standard and believes it to be the best currently available scalable framework for exchanging abuse reports. M^{3}AAWG encourages both member organizations and the Internet community at large to follow the abuse reporting recommendations contained in this document and the corresponding RFCs.

References

Relevant IETF RFCs:

- RFC2142 - Mailbox Names for Common Services, Roles and Functions - http://tools.ietf.org/search/rfc2142
- RFC3912 - WHOIS Protocol Specification - http://tools.ietf.org/search/rfc3912
- RFC5965 - An Extensible Format for Email Feedback Reports - http://tools.ietf.org/search/rfc5965
- RFC6449 - Complaint Feedback Loop Operational Recommendations - http://tools.ietf.org/search/rfc6449
- RFC6650 - Creation and Use of Email Feedback Reports: An Applicability Statement for the Abuse Reporting Format (ARF) - http://tools.ietf.org/search/rfc6650

Regional Internet Registry (RIR) policies on abuse points of contact:

- African Network Information Centre (AFRINIC) http://www.afrinic.net/en/library/policies/698-afpub-2010-gen-006
- American Registry for Internet Numbers (ARIN) https://www.arin.net/policy/nrpm.html
- Asia Pacific Network Information Centre (APNIC) http://www.apnic.net/policy/proposals/prop-079
- Latin American and Caribbean Internet Addresses Registry (LACNIC) http://lacnic.net/en/politicas/manual4.html
- Réseaux IP Européens Network Coordination Centre (RIPE NCC) - http://www.ripe.net/ripe/docs/ripe-563

M^{3}AAWG079