Messaging, Malware and Mobile Anti-Abuse Working Group

M^{3}AAWG Best Common Practices for the Use of a Walled Garden

Criteria for Exit, Entry, Remediation and Subscriber Education When Using a Walled Garden to Remediate Virus and Bot-infections in Subscriber Devices
Version 2.0

Originally published October 2007
Updated March 2015

I. Executive Summary

As subscriber-originating network abuse increases, ISPs (Internet Service Providers) have been required to enforce more proactive measures in an effort to protect their networks. Bots and bot networks, i.e. botnets, have become an increasingly popular mechanism for spammers and hackers to abuse the network through the propagation of spam, viruses and other forms of malware, infections that often result in the botnet obtaining control of a subscriber's device. This malware is surreptitiously planted on one or more of the subscriber's personal computers without the owner's knowledge, resulting in subscribers being overwhelmingly targeted as the unwitting accomplices in these malicious networks.

In an effort to reinforce the M^{3}AAWG mission to protect electronic messaging and Web browsing from online exploits and abuse, the M^{3}AAWG Technical Committee recommends the following best practices as they relate to the implementation of a walled garden. A walled garden refers to an environment that controls the information and services that subscribers' devices are allowed to utilize and to the network access permissions that are granted. The primary goal of these practices is to provide immediate and highly visible communications to the subscribers' account; to help them become aware of unwanted programs or malware residing on their personal computers and facilitate their removal; and to stop the network from being used for abusive purposes.

II. Criteria for Enabling and Disabling Walled Garden Status Must Be Concise

In an effort to educate subscribers on the risks and issues associated with malware infected personal computers, ISPs MAY implement a walled garden for new subscriber accounts or any account that they deem as being risky or generating suspicious traffic. The entry and exit criteria for the walled garden MUST be clear and concise so that it can be understood by the subscribers.

Hereafter, "subscriber" refers to the account holder or a technically receptive alternative assigned by the account holder. "Personal computers" denotes the collection of PCs, Macs, tablets and smartphones using the ISP's Internet connection on an account. Additionally, unless stated otherwise, all recommendations are the responsibility of the ISP to implement, and the uses and definitions of key words like MUST, SHOULD and MAY used throughout this document are to be interpreted as described in RFC 2119[1].

[1] Key words for use in RFCs to Indicate Requirement Levels (RFC 2119), http://www.faqs.org/rfcs/rfc2119.html

1. **Recommendations Summary:**

a) MUST provide a clear notification of the suspected problem; e.g., that the account holder is using the network outside of the AUP (Acceptable Use Policy). MUST also provide an explanation for the notification and an overview of the recommended process to remediate or clean the account computers of malware. Because a number of independent devices may be active and associated with the account, any or all may be infected and causing problems. Consequently, the education of a technically receptive representative of the account on the problem, the measures taken and steps to remediation MUST be carefully presented.

b) MAY redirect HTTP [80] to the appropriate quarantine Web address or website respectively.

c) MAY redirect botnet command and control traffic to a honey network for analysis.

d) SHOULD manage all outbound SMTP [25] to a quarantine area, to a honeypot MTA (Message Transfer Agent) or SHOULD block altogether during this process.

e) SHOULD allow instant escape based on trust. Trust can be asserted through an action that indicates a clean personal computer or the result of a request to use the network "as is" for a configurable period of time.

f) MAY provide exit if certain ISP-approved cleanup or security software is downloaded and installed.

g) The ISP MAY use internal subscriber reputation metrics determined by using detection techniques such as content filters, deep packet inspection, and behavior usage patterns to trigger entry or exit events from the walled garden.

h) The ISP MAY use technologies to automatically identify the subscriber's security posture as advertised by installed and trusted subscriber client software.

III. Remediation Experience Must Be Convenient to the Subscriber

As ISPs continue to make efforts to protect their networks and subscribers from malicious abuse, it is important for ISPs to do it in a way that is not unreasonably cumbersome to the subscriber. In order to recoup the investment, the ISP MAY also choose to make remediation tools available at a cost to the subscriber. Those tools MUST be made available via means that are consistent with the ISP's typical support environment. Additionally, the walled garden MUST allow access to websites - either through direct access or via indirect proxy connection mechanisms - so that the subscriber can download critical, applicable software updates and patches. Access to remediation tolls presents the possibility to the provider or the contracted application provider of making available remediation via a single portal, like Microsoft does with its Windows Update and the multiple new driver downloads it initiates on the user's behalf.

1. **Recommendations Summary:**

a) MUST be able to provide remediation alternatives either free, fee-based or both, or links to existing online tools.

b) MUST present recognizable information that legitimizes the experience as an official ISP Notice and Remediation Process. Examples of this information include data such as an account number or a secret question answer and maintaining the consistency with the style and logo of the ISP.

c) MUST provide details on how to exit the walled garden, including method and any actions that are a prerequisite for exit. Examples may include how to contact customer support if needed or how to navigate out of the walled garden.

d) SHOULD not require a reboot of the subscriber's personal computer for the remediation experience to take effect.

e) MUST provide links to URLs and domains that help resolve the unwanted condition with OS patches and, if appropriate, with security updates.

f) SHOULD provide "Click to Chat with Customer Support" or a third-party providing customer service on behalf of the ISP.

g) SHOULD provide ISP support or abuse contact information, e.g. a phone number.

h) SHOULD instruct subscribers sending malicious SMTP [25] traffic to reconfigure Mail User Agents (MUAs) to send outbound email traffic over port 587. When that takes place, the ISP SHOULD thereafter block the account from access to SMTP [25].

i) SHOULD present unique remediation experiences depending on the unwanted condition and past account actions, i.e. an account holder SHOULD see an experience that provides a fix for the exact problem or type of malware suspected.

j) SHOULD provide a security client that is minimally intrusive, downloads quickly, easily installs without conflicting with other security application software already configured by the client. Additionally, it SHOULD not require a reboot nor require a full scan of the computer to detect and remove malware, unless the resolution renders it necessary.

k) MUST allow for redirection exceptions so that the users, e.g. operators of an Internet accessing device on the account, are permitted to utilize emergency online services. These services MUST include at least a temporary escape from browsing constraints and MUST not interfere with VoIP telephone service to avoid interference with emergencies and 911 calls.

IV. Subscriber Education Should Be a Primary Focus

Since account representatives are typically the weak link in the security chain, the ISP SHOULD make reasonable efforts, by way of documentation available on their website, that subscribers can proactively educate themselves on how to mitigate risk of malware infection. As such, documentation in the form of FAQs, support videos, tutorials and a searchable knowledge base SHOULD be made available to all the subscribers on the account. If provided, these materials MUST be made available to the subscriber via a method that is consistent with the look and feel of the ISP's customer service interface. Additionally, the available documentation SHOULD be broad enough to cover applications across several different types of Internet technologies and across several different types of computer and device operating systems, e.g. Windows, MacOS, Linux, iOS and Android.

1. Recommendations Summary

a) MUST present recognizable information that legitimizes the experience as an official ISP Notice and Remediation Process. Examples of this information include data such as an account number or secret question answer and to be consistent with the style and logo of the ISP.

b) SHOULD provide intuitive education via FAQs and tutorials.

c) SHOULD provide alternative learning center tools such as a simple video greeting and search knowledge centers.

d) SHOULD provide educational information for multiple types of applications including email (POP3/SMTP) and browsing (HTTP).

V. Conclusion

The provisioning of Internet connectivity for subscribers is more sophisticated today. Concurrently, the complexity of the providers' networks and the customers' networks has grown. Both require more service and are in a position to cause harm to the other. The clear direction would be to implement reliable communications so they can be better partners in the process.

The system was initially architected, and continues, with simple communication from the subscriber to the provider via call centers and portals that are manned 24/7. Communication from the provider to the subscriber, e.g. informing them of a need to upgrade a modem, to tend to a dangerous virus, or to alert them of planned outages, is more difficult. Most providers may not have a reliably accessed email address for their subscribers. Telephone calls are frequently not answered.

A walled garden or similar system on the provider's network can place information on the subscriber's screen when the subscriber is at a device (PC, tablet, smartphone, etc.). The walled garden best practices outlined in this document provide an implementation to better assure customer security.