SNMP Reflected Amplification DDoS Attack Mitigation

A BROADBAND INTERNET TECHNICAL ADVISORY GROUP
TECHNICAL WORKING GROUP REPORT

A Near-Uniform Agreement Report
(100% Consensus Achieved)

Issued:
August 2012

Copyright / Legal Notice

Copyright © Broadband Internet Technical Advisory Group, Inc. 2012. All rights reserved.

This document may be reproduced and distributed to others so long as such reproduction or distribution complies with Broadband Internet Technical Advisory Group, Inc.’s Intellectual Property Rights Policy, available at www.bitag.org, and any such reproduction contains the above copyright notice and the other notices contained in this section. This document may not be modified in any way without the express written consent of the Broadband Internet Technical Advisory Group, Inc.

This document and the information contained herein is provided on an “AS IS” basis and BITAG AND THE CONTRIBUTORS TO THIS REPORT MAKE NO (AND HEREBY EXPRESSLY DISCLAIM ANY) WARRANTIES (EXPRESS, IMPLIED OR OTHERWISE), INCLUDING IMPLIED WARRANTIES OF MERCHANTABILITY, NON-INFRINGEMENT, FITNESS FOR A PARTICULAR PURPOSE, OR TITLE, RELATED TO THIS REPORT, AND THE ENTIRE RISK OF RELYING UPON THIS REPORT OR IMPLEMENTING OR USING THE TECHNOLOGY DESCRIBED IN THIS REPORT IS ASSUMED BY THE USER OR IMPLEMENTER.

The information contained in this Report was made available from contributions from various sources, including members of Broadband Internet Technical Advisory Group, Inc.’s Technical Working Group and others. Broadband Internet Technical Advisory Group, Inc. takes no position regarding the validity or scope of any intellectual property rights or other rights that might be claimed to pertain to the implementation or use of the technology described in this Report or the extent to which any license under such rights might or might not be available; nor does it represent that it has made any independent effort to identify any such rights

Executive Summary

A BITAG member and Internet Service Provider (ISP), Comcast, has observed large-scale Simple Network Management Protocol (SNMP) Reflected Amplification Distributed Denial of Service (DDoS) attacks. These attacks are significant and have been observed to result in tens of gigabits to over one hundred gigabits per second of SNMP traffic sent to attack targets from multiple broadband networks. These attacks have been hours long in duration, disruptive for attack targets, and very challenging for targets to mitigate. The conditions that make this attack possible exist on many types networks, regardless of access network technology (DOCSIS, DSL, fiber, etc.), and regardless of geographic location.

The general conditions making this possible include:

- Some networks do not perform ingress filtering, which makes it possible for users of those networks to spoof packets, making it appear that the packets originated elsewhere.
- Networks have hosts that are infected with malware, and are under the control of bot networks.
- Some home gateway devices (a.k.a. routers) ship with SNMP turned on by default, using a well-known community string such as "public."

To conduct the attack, the following steps are taken by an attacker:

- Initiation: An attacker sends instructions to a bot network to conduct the attack. These instructions include the bots to use to distribute the attack, the home gateways to reflect and amplify the attack, and the IP address of the attack target.
- Distribution: Infected hosts participating in a bot network, which happen to be located in a network that cannot or has not taken sufficient steps to prevent spoofing, receive the attack instructions. Thus, one attacker distributes the attack activity to many individual hosts. Each of the multitude of bots sends a small SNMP query to home gateway devices that are listening for particular SNMP queries on their public Internet network interface. This query is forged to make it appear that it was sent from the victim's IP address, so that all responses will be directed to the target rather than back to the bot network's hosts.
- Reflection: Home gateways that were listening for SNMP queries, receive the forged queries from the bot network's hosts. They then send an SNMP response to the target.
- Amplification: The size, in bytes, of the SNMP response is larger than the SNMP query sent by the bot network. So the bot network is able to amplify the amount of data directed at the attack target, compared to a smaller amount of data sent by the bot network.

Device makers as well as Internet Service Providers (ISPs) and Application Service Providers (ASPs) should be aware of this issue and may need to consider a range of potential network management or other responses. The recommendations of the BITAG include:

- End-user devices should not be configured with SNMP on by default.
- End-user devices should not be routinely configured with the “public” SNMP community string.
- ISPs, ASPs, and other network or systems administrators should not routinely use the “public” SNMP community string on an unsecured basis.
- Users should be allowed and encouraged to disable SNMP.
- ISPs should take reasonable steps to prevent address spoofing.
- ISPs may implement appropriately targeted filtering/blocking of SNMP traffic.
- ISPs should be transparent with respect to network management policies that may impact SNMP traffic.
- ISPs should provide mechanisms to re-enable SNMP on a case-by-case basis.
- ISPs and attack targets should be willing to share relevant and non-proprietary information related to SNMP-based attacks with appropriate communities.

Table of Contents

1. About the BITAG

The Broadband Internet Technical Advisory Group (BITAG) is a non-profit, multi-stakeholder organization focused on bringing together engineers and technologists in a Technical Working Group (TWG) to develop consensus on broadband network management practices and other related technical issues that can affect users' Internet experience, including the impact to and from applications, content and devices that utilize the Internet.

The BITAG's mission includes: (a) educating policymakers on such technical issues; (b) addressing specific technical matters in an effort to minimize related policy disputes; and (c) serving as a sounding board for new ideas and network management practices. Specific TWG functions also may include: (i) identifying "best practices" by broadband providers and other entities; (ii) interpreting and applying "safe harbor" practices; (iii) otherwise providing technical guidance to industry and to the public; and/or (iv) issuing advisory opinions on the technical issues germane to the TWG's mission that may underlie disputes concerning broadband network management practices.

BITAG TWG reports focus primarily on technical issues. While the reports may touch on a broad range of questions associated with a particular network management practice, the reports are not intended to address or analyze in a comprehensive fashion the economic, legal, regulatory or public policy issues that the practice may raise.

BITAG welcomes public comment. Please feel free to submit comments in writing via email at comments@bitag.org.

2. Issue Overview

A BITAG member and Internet Service Provider (ISP), Comcast, has observed large-scale Simple Network Management Protocol (SNMP) Reflected Amplification Distributed Denial of Service (DDoS) attacks [A Look Inside the Anonymous DDoS Attack Code] [Inside Anonymous DDoS Code] [SNMP DDoS Vector] [SNMP Reflected Denial of Service] [Team Cymru on SNMP Attacks] [Threat Advisory: SNMP Amplification DDoS]. During such attacks, broadband Internet subscriber devices can in some cases be used unwittingly to generate significant and sustained levels of traffic directed against targeted networks or sites. This can have a severe and/or service-affecting impact on any targets. Device makers as well as Internet Service Providers (ISPs) and Application Service Providers (ASPs) should be aware of this issue and may need to consider a range of potential network management or other responses. Some responses may have side effects that impact legitimate uses of the network, so it is important for the community to have consensus on how such attacks can be deflected or mitigated.

2.1. What is SNMP?

SNMP [RFC1157] [RFC2571] [RFC3411] [RFC3412] [RFC3413] [RFC3414] [RFC3415] [RFC3416] [RFC3417] [RFC3418] is a service that runs on a host system and can be used by a remote administrator to ascertain the host's health status at a moment in time and perform maintenance functions. Such host systems can include a wide range of devices, including network routers, firewalls, load balancers, web or other application servers, customer broadband connectivity devices, customer home gateway devices, personal computers, mobile devices, Internet cameras, and many more.

When either SNMP polling or requests are configured on a device, the device is set to listen for SNMP queries that match the device's read or write "community strings." The community strings are a sort of access code sent in clear text. If the query matches the community string on a device, then a response is sent back. In consumer-grade devices, which are typically owned and administered by broadband Internet users (end users), SNMP is infrequently used, although it is often included as a feature. Administrators or, more typically, automated monitoring systems, send queries to SNMP-enabled devices. SNMP enables administrators to track a range of statistics such as the temperature of a device, whether a network interface is functioning properly, CPU utilization levels, network interface utilization rates, the current number of transactions being processed, or a range of other measurements.

In essence, SNMP enables administrators to keep track of the current health and state of a device or system, as well as utilization levels and errors. This can be used to alert administrators of problems, as well as to perform technical functions such as capacity planning or usage analysis.

2.2. How Are Devices Configured to Use SNMP?

When SNMP is configured on a device or system, at a minimum it must be configured to listen for specific community strings (additional access controls may also be possible to configure). If no community strings are specified, one may be automatically selected by default when turning on SNMP, as configured by the device maker or software developer. The community strings "public" and "private" are common defaults for read and write community strings, but good security practices dictate that administrators avoid these default community strings [RFC3512] [RFC3871] [SANS Top 20 Most Critical Internet Security Threats 2000-2001].

SNMP is typically used within a Local Area Network (LAN), a Service Provider Network (such as an ISP network or application data center), or an enterprise's Wide Area Network (WAN). SNMP is generally not used on public-facing Internet devices in an unsecured and open manner, rather it is the case that some sort of security controls are typically in place, such as IP address access control lists. This is partly because of security issues with the protocol and risks of exposing server and networking information to the general public. In addition, access controls are typically used to disallow SNMP from being polled on publicly accessible network interfaces of devices or systems used in a Service Provider Network.

SNMP versions 1 and 2 are based on clear text community strings. SNMP version 3 corrects security shortcomings in earlier versions by using encryption, authorization, and other mechanisms. However, SNMPv3 has not been deployed as widely as earlier versions.

Unfortunately, many SNMP security mechanisms are not used or are not configured properly. For example, with SNMPv1 and v2, if no community strings are specified, one may be automatically selected by default when turning on SNMP, as configured by the device maker or software developer. The community strings “public” and “private” are common defaults for read and write community strings and can be easily guessed. For SNMPv3, if the security level is “noAuth,” all the security benefits of this version are lost.

2.3. How SNMP Is Exploited to Conduct Reflected Amplification DDoS Attacks

When SNMP is enabled for use by the general end user population, those end users are unlikely to: (1) be aware of or care what SNMP is, (2) know whether or not it is on by default, (3) understand what turning it on may mean, (4) know what a community string is used for, or (5) know that default community string names should be avoided. In general, typical consumers should not be expected to know about or care about such things; end user device vendors and software developers usually assume no such knowledge and design solutions accordingly.

End users typically access the Internet using a home gateway device (a.k.a. home router, which is typically connected to or integrated with an access device such as a cable or DSL modem) to enable multiple devices on their home LAN to connect to the Internet.

SNMP Reflected Amplification DDoS Attacks occur when devices running SNMP are used to direct large amounts of traffic at targets whose IP addresses have been spoofed in SNMP requests. The danger of the reflected amplification DDoS attack is present when SNMP is enabled on the home gateway device’s Internet-facing network interface (a.k.a. Wide Area Network interface). In such cases, those devices will typically respond to any SNMP queries sent from any host anywhere on the Internet that uses the appropriate community string. If a well known or default community string is used, this significantly increases the likelihood that hosts unknown to the end user (and potentially malicious) will be able to successfully query their device(s) or system(s).

In addition, SNMP uses UDP port 161 [IANA Service Name and Transport Protocol Port Number Registry]. Unlike TCP [RFC793], UDP [RFC768] is a connectionless protocol.
The use of a connectionless protocol makes it relatively easy for a host to spoof the

source address of an SNMP query, as no bi-directional communication is required to elicit a meaningful response.

Address spoofing is possible on networks that do not enforce source address verification, a practice that restricts network accesses to traffic from non-spoofed addresses [BCP38] [BCP84] [RFC2827] [RFC3704] [Network Hygiene Pays Off] [Securing the Edge]. It is important to understand that the impact of any attack will usually be on networks other than the one where spoofing originates. Thus, even if networks implement ingress filtering, they can be subject to the effects of spoofing-related attacks originating from less well-managed networks.

In addition to preventing the identification of their hosts and redirecting response traffic to the target of an attack by using source address spoofing, an attacker can further obfuscate identification and magnify the attack traffic by using a distributed network of hosts infected with malware that are operating as part of a bot network. Using a bot network also enables the attacker to harness significantly more attack power (potential processing power and network capacity) than the individual attacker otherwise could. This is why bot networks are frequently the source of Distributed Denial of Service (DDoS) attacks.

In the typical form of this attack, an attacker uses a bot network comprised of many hosts to send an SNMP "GetBulkRequest" query (although any other SNMP queries could also be used, including a simple "Get"). As seen below, this query generates a very powerful attack because the size of the response to the query is much larger than the query itself. The SNMP query is sent to a large number of reachable devices with the default community string of public (or another well known community string). When sending this query the attacker spoofs the IP address of the query source, setting the source as the IP address of the intended victim.

Any device listening for SNMP queries that are configured with the matching community string will then automatically respond. In the case of GetBulkRequest queries for example, typical queries (over IPv4) may range between 60 – 102 bytes [RFC3416] [Digging into SNMP in 2007] [Threat Advisory: SNMP Amplification DDoS]. Such requests will generally result in responses ranging between 423 – 1,560 bytes [RFC3416] [Digging into SNMP in 2007] [Threat Advisory: SNMP Amplification DDoS]. This means that there is an amplifying effect, since the response, in bytes, is larger than the query.

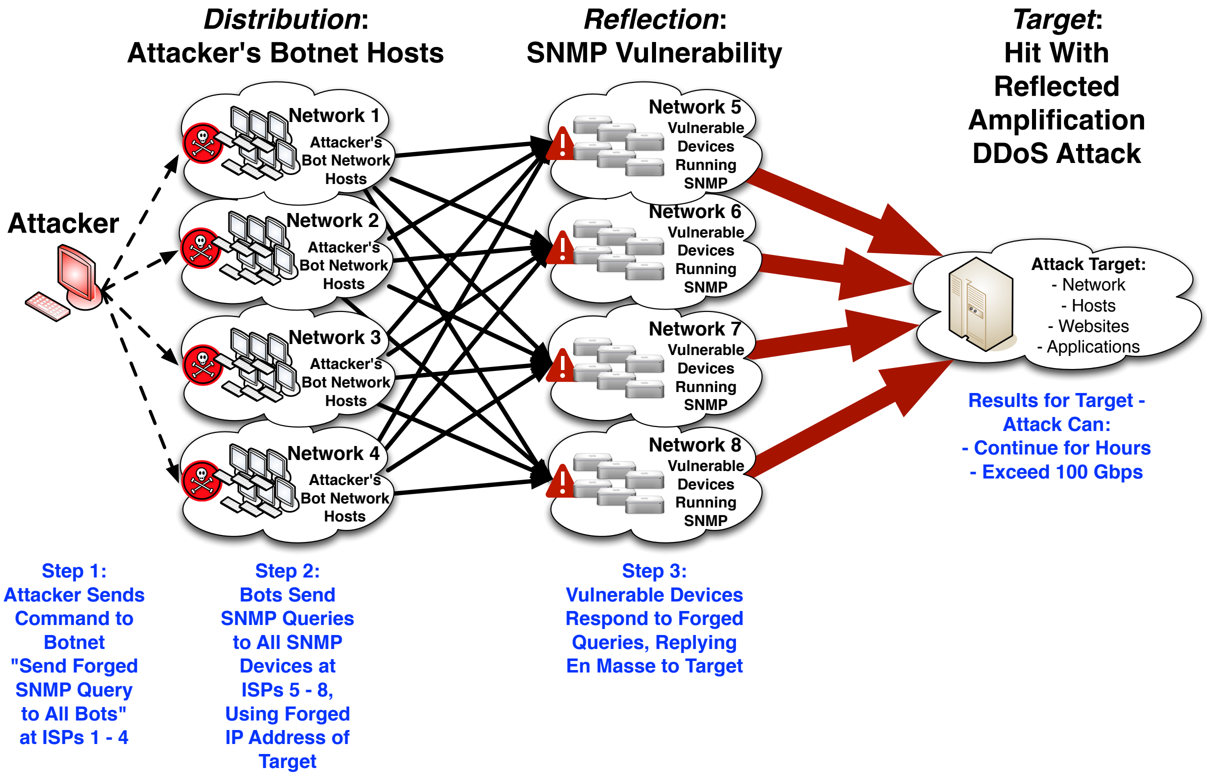
Because the attacker is sending very little data from its hosts or a bot network's collection of hosts, the identification of the source of the attacker's hosts or the bot network's hosts is very difficult. That is, the attack does not generate any large or unusual traffic pattern from the actual source. It also may be difficult for end users to notice that their systems are being used as bots in an attack, or that their home gateway devices are being used in an attack.

Thus, in summary, the conditions that can lead to an SNMP Reflected Amplification DDoS attack are:

1. An end user's home gateway device is connected to the Internet.
2. That end user device has an SNMP agent running on it listening on the Internet interface to any IP address.
3. A well known or default SNMP community string (such as "public") for SNMPv1 or SNMPv2 or a noAuth security level for SNMPv3 is used.
4. Any host on the Internet can then send a query to the end user device.
5. Since SNMP uses UDP, it is easy to spoof the source of the query.
6. Some networks do not enforce address source validation, which enables hosts on those networks to spoof packets.
7. The spoofed IP address used is that of an intended target.
8. A small amount of SNMP query traffic is sent, resulting in a much greater amount of response traffic, which is sent to the target (amplification).
9. When enough hosts are involved (distribution) and enough spoofed query traffic sent, the resulting amplified and distributed response traffic can overwhelm targeted hosts and networks, as well as some intervening or connected networks.

The attack is illustrated in *Figure 1*.

Figure 1 – Diagram of an SNMP Attack


Distribution:
Attacker's Botnet Hosts
Reflection:
SNMP Vulnerability
Target:
Hit With
Reflected
Amplification
DDoS Attack
Attacker
Network 1
Attacker's Bot Network Hosts
Network 2
Attacker's Bot Network Hosts
Network 3
Attacker's Bot Network Hosts
Network 4
Attacker's Bot Network Hosts
Network 5
Vulnerable Devices Running SNMP
Network 6
Vulnerable Devices Running SNMP
Network 7
Vulnerable Devices Running SNMP
Network 8
Vulnerable Devices Running SNMP
Attack Target:
- Network
- Hosts
- Websites
- Applications
Results for Target - Attack Can:
- Continue for Hours
- Exceed 100 Gbps
Step 1: Attacker Sends Command to Botnet "Send Forged SNMP Query to All Bots" at ISPs 1 - 4
Step 2: Bots Send SNMP Queries to All SNMP Devices at ISPs 5 - 8, Using Forged IP Address of Target
Step 3: Vulnerable Devices Respond to Forged Queries, Replying En Masse to Target

2.4. How Severe Can Attacks Be for Targets?

Since a large number of end user systems infected with malware [Microsoft Security Intelligence Report Vol. 11] are used to conduct this kind of attack, attackers have a large platform from which to launch spoofed SNMP amplification attacks. In addition, as broadband Internet access speeds have steadily increased and the processing power of end user systems has increased, the capacity to generate spoofed SNMP queries and in turn to amplify them across a large number of devices, means that a significant volume of data can be generated.

ISPs in the United States and in Europe that have observed their end users' home gateway devices being unwittingly used in such attacks have individually recorded in excess of 60 Gbps of SNMP traffic directed at targets. In aggregate, across multiple ISP networks, such attacks have been observed to exceed 100 Gbps. These attacks have been observed to last several hours, making them far from fleeting. Attacks have also been observed in several successive months and these attacks have been growing over time [Threat Advisory: SNMP Amplification DDoS] [SNMP DDoS Vector].

While a target could temporarily block all SNMP traffic, this could impact its ability to use SNMP to manage its own network, systems, and services. Furthermore, even if the target can configure its routers, firewalls, or hosts to filter out SNMP traffic, the volume of traffic being sent to it can be so significant that upstream links are saturated or routers or firewalls are overwhelmed with so many packets that the target cannot successfully filter the traffic.

Finally, any intervening networks may also be impacted. This may include a target's upstream ISP and networks with which it interconnects or peers.

Thus, targets of the attack and connected networks may experience a disruptive volume of traffic. Targets in particular, depending on the design of their network and services and applications, may find such attacks create debilitating denial of service conditions.

Once a target detects an attack, it will only be able to trace the attack back to those networks that contain the "innocent" hosts being used as SNMP reflectors and amplifiers. Neither the target nor those networks with end user devices unwittingly used in the attack will likely be able to trace the true origin of the attack (the network used to send commands to the bot network or to the attacker).

3. How Devices Are Exploited

3.1. The Attack Exploits Shortcomings in Device Management

The devices affected in observed attacks appear to be customer-owned and administered home gateway devices, rather than ISP-managed devices. Because such home gateway devices are customer-owned and administered, and do not automatically update their firmware (or do not have users that understand how to do so or are motivated to do so), an ISP is unable to remotely update or reconfigure such devices; only the end user has this control.

As a result, poorly configured devices (whether due to end users, device makers, software developers, or a combination thereof) have infrequently updated or not updated firmware (which may supply the necessary curative fixes). This in sum represents a weak device administration model. This weakness is then exploited at large scale and for little cost by attackers.

3.2. Devices Known to Be Exploited

Network logs provided to a BITAG member, Comcast, from some of the attack targets indicate that a range of devices can be affected by this issue, primarily because end users can turn on SNMP on nearly any home gateway or other Internet-connected device.

However, the most susceptible devices are those that have SNMP enabled by default and that also use the public community string. Worryingly, Comcast has also observed that in some such devices, the end user does not even have the ability to disable the SNMP service or to change the default community string.

4. Networks Are Failing to Apply Address Source Verification

This attack exploits basic shortcomings in the configuration of some networks: the fact that some networks fail to implement address source verification. While it is quite clearly a recommended practice [BCP38] [BCP84], not all networks take steps to allow only “verified” source IP addresses that are not spoofed. This leaves networks that do not take steps to prevent spoofed packets vulnerable to contributing to attacks originating from hosts in their networks, and makes all other network vulnerable to such attacks. Without this critical shortcoming, source address spoofed attacks would not be possible.

5. BITAG Interest in This Issue

The BITAG believes ISPs may be observing the early phases of this type of attack being used at a large scale, and that this could soon be observed by many other ISPs. In addition, because ISPs may undertake various network management responses to this issue, it is important to understand possible implications of those network management responses. In addition, the BITAG believes it is important to understand the role that device makers and other groups play in this issue.

Furthermore, this issue may potentially affect many elements of the Internet community, such as:

- Equipment Manufacturers that make home gateway devices and provide updated firmware for existing devices.
- ISPs that can have their users unwittingly participate in these attacks.
- End users that can be unwitting participants in one of the stages of the attack, or be affected by mitigation efforts.
- Any Internet-connected entity that may become a target of such an attack.

6. Implications and Concerns Relating to the Issue

6.1. Deterring Source IP Address Spoofing

If a network operator does not take reasonable steps to detect and prevent IP address spoofing [BCP38] [BCP84], then SNMP attacks (and a variety of other attacks) are more easily initiated, broader in scope and more difficult to prevent. Accordingly, network operators should take technically sound and cost-effective steps to assure that packets with spoofed source addresses do not originate from the networks they manage.

6.2. Supplying Devices that Enable the Attack

It appears to be a somewhat common practice for new devices to ship with either SNMP on by default and/or the 'public' SNMP community string in use by default. This is contrary to advice in Section 6.2 of RFC 3512, which states that "[v]endors should not ship a device with a community string 'public' or 'private', and agents should not define default community strings except when needed to bootstrap devices that do not have secondary management interfaces" and that "[d]efaults lead to security issues that have been recognized and exploited."

Device makers have little incentive to update firmware for old devices that have this vulnerability, since they may have sold a given device years earlier and such consumer-grade devices do not generally come with a support and maintenance contract that would directly fund software updates for many years after equipment is purchased. Even when firmware updates are available, very few end users ever upgrade their firmware, know how to do so, or are motivated to do so.

6.3. Allowing Bots on a Network to Be Used As a Launchpad for Attacks

Networks do not control end-user devices and so have relatively limited tools with which to solve the problem of bots. However, there is a range of potential steps that a network operator can take, such as those recommended in a recent FCC Anti-Bot Code of Conduct [U.S. Anti-Bot Code of Conduct].

6.4. Allowing Devices on a Network to Be Used to Reflect and Amplify an Attack

Networks can take reasonable steps to secure SNMP on devices that they own or administer. Many devices are, however, controlled by end-users, and are therefore outside of the direct control of a network. It is unreasonable to expect a network to bar access to a user with a device that has SNMP security problems as a matter of course, especially since some devices lack a mechanism for disabling or reconfiguring SNMP.

6.5. Blocking IP Traffic to an Attack Target to Mitigate Attacks

A network could choose to mitigate an attack by blocking (blackholing) all traffic destined for the attack target. Unfortunately, this prevents legitimate end user access to the target's IP addresses. In the case of shared cloud-based services, shared hosting services, and Content Delivery Networks, temporarily blocking traffic destined to them can have a potentially significant impact on legitimate traffic that is not part of the attack.

6.6. Blocking SNMP Traffic to Mitigate Attacks

A network could choose to mitigate an ongoing attack or prevent a future attack by blocking the use of SNMP on the network. Such an action could block SNMP traffic overall as a prophylactic measure, or could reactively block SNMP traffic destined to an attack target. Depending upon how this is configured, this could have the side effect of blocking the network's own use of SNMP or, more problematically, blocking the legitimate use of SNMP by enterprise and other business users.

7. Technical Working Group (TWG) Suggested Practices

This section enumerates some suggested practices. The BITAG recognizes that this may not be an exhaustive list, and that the requirements and needs of operating certain types of networks may preclude some of these practices. The BITAG also recognizes that these suggested practices are long-term in nature and that immediate and acute security issues may dictate that other practices are used for some period of time.

7.1. End-User Devices Should Not Routinely Be Configured with SNMP On By Default

The BITAG suggests that device makers not enable SNMP by default on newly produced devices that are commonly used in an environment where they could receive unsolicited traffic from the Internet, unless SNMPv3 with appropriate authentication is used. Note that with the deployment of IPv6, all devices not protected by a firewall that does stateful packet inspection will be in such an environment. For IPv4, the Network Address Translation (NAT) function prevented unsolicited traffic from reaching devices with private IPv4 addresses. With IPv6, all devices will receive globally routable (and thus reachable) addresses.

7.2. End-User Devices Should Not Routinely Be Configured with the Public SNMP Community String

The BITAG suggests that device manufacturers, ISPs, and ASPs do not use the “public” SNMP community string. Furthermore, the BITAG suggests that device manufacturers update any applicable firmware for current and past products to disallow the “public” SNMP community string. The BITAG further suggests that all devices produced in the future should be similarly configured.

7.3. ISPs, ASPs, and Other Network or Systems Administrators Should Restricted Access to SNMP

The BITAG suggests that ISPs, ASPs, and other network or systems administrators restrict access to SNMP on hosts or network elements that they administer. Access can be restricted such as via IP address access control lists or other methods to apply some level of security control on SNMP queries.

7.4. Users Should Be Allowed and Encouraged to Disable SNMP

The BITAG suggests that if SNMP (predating SNMPv3) is present on a device, the device maker should provide an easy way for a user to disable SNMP.

7.5. ISPs Should Take Reasonable Steps to Prevent Address Spoofing

ISPs should allow only “verified” source IPs that are not spoofed [BCP38] [BCP84] where feasible. While some ISPs already enforce this policy on their networks, many other ISPs do not appear to enforce this policy. This leaves the Internet vulnerable to spoofing-related attacks and other malicious behavior that originates from hosts in those networks.

Verification of source IPs can be accomplished through ingress filtering and there are several ways an ISP can implement this [BCP84]. Special attention should be given when implementing these techniques for multi-homed customers (those with more than one upstream Internet connection).

Encouraging other ISPs to implement this policy is a long-term effort for the good of the Internet, although it may not have a near-term impact on this particular issue.

7.6. ISPs May Implement Appropriately Targeted Filtering/Blocking of SNMP Traffic

An ISP with devices that are used in reflection and amplification attacks could take steps to block the SNMP protocol (UDP port 161) in some or all devices on its network. This strategy can minimize the size and scope of these attacks, but its side effects depend on the extensiveness of the blocking.

Blocking SNMP for all customers on a network could negatively affect business users, some of whom appear to regularly use SNMP. A better approach may be to block SNMP only in residential devices, where the use of SNMP appears to be negligible to non-existent, based on samples of traffic by Comcast on its network.

It may also be reasonable for an ISP to scan attached devices and take mitigation actions only for those that use non-secure community strings, or to otherwise place requirements on users who wish to use SNMP (such as using SNMPv3, for example). In adopting any approach that includes limiting the use of SNMP, ISPs should seek to minimize the impact of the approach on legitimate SNMP use.

If ISPs filter or block SNMP traffic -- other than on a temporary basis to mitigate an on-going attack or on a targeted basis (affecting users observed participating in an attack or identified as running SNMP in a network scan) -- then the recommendations in Sections 7.7 and 7.8 apply as well.

7.7. ISPs Should Be Transparent with Respect to Network Management Policies that May Impact SNMP Traffic

The BITAG suggests that ISPs that choose to filter or block SNMP traffic should disclose this practice as part of being transparent with respect to network management policies. Information about how users can re-open access to SNMP should be disclosed and easy to find and understand.

7.8. ISPs Should Provide Mechanisms to Re-Enable SNMP on a Case-by-Case Basis

If ISPs choose to filter or block SNMP traffic on a permanent basis, and across all subscribers or classes of subscribers (such as residential or commercial), then the BITAG recommends that they provide a mechanism for users to re-open access to SNMP, if this is reasonably technically feasible and cost efficient.

Depending upon the implementation, including the particulars of the access network technology (i.e. DOCSIS, DSL, LTE, etc.), the technical feasibility and costs can vary greatly. For example, there may be cases where SNMP blocking is only feasible in an access router or other aggregation point, some distance from the end user's equipment, which may make per-user controls infeasible.

7.9. ISPs and Attack Targets Should Be Willing to Share Relevant and Non-Proprietary Information Related to SNMP-Based Attacks With Appropriate Communities

To aid attack investigation and further assist with implementing the above recommendations, sharing of information by the affected organizations is important. These organizations should share information with relevant parties as appropriate and as allowed by rules, regulations, and laws governing their customer relationships and maintaining customer privacy.

Information that is useful to share includes notification of the attack once it is detected, as well as its specific characteristics. Also, sharing of Netflow [RFC3954] data for all of the ingress interfaces on the path to the reflectors (with the victim's IP address as the source IP address), could help tracing back the actual attackers or mitigating the attack. It is important that accurate time (sourced via Network Time Protocol, NTP) is used for timestamps.

This information could be shared with, for example, other ISPs that may be or are being used in conducting attacks, the targets of the attacks, security researchers, security solution providers, and network equipment suppliers. The IETF has published a Best Current Practices document [BCP 46] that may be worth reviewing when considering this topic further.

8. References

[BCP38] Ferguson, P. and D. Senie, "Network Ingress Filtering: Defeating Denial of Service Attacks which employ IP Source Address Spoofing", BCP 38, May 2000, <http://tools.ietf.org/html/bcp38>.

[BCP46] Killalea, T., "Recommended Internet Service Provider Security Services and Procedures", BCP 46, November 2000, <http://tools.ietf.org/html/bcp46>.

[BCP84] Baker, F. and P. Savola, "Ingress Filtering for Multihomed Networks", BCP 84, March 2004, <http://www.ietf.org/rfc/rfc3704.txt>.

[RFC768] Postel, J., "User Diagram Protocol", RFC 768, August 1980, <http://tools.ietf.org/html/rfc768>.

[RFC793] Postel, J., "Transmission Control Protocol", RC 793, September 1981, <http://www.ietf.org/rfc/rfc793.txt>.

[RFC1157] Case, J., M. Fedor, M. Schoffstall, and J. Davin, "A Simple Network Management Protocol (SNMP)", RFC 1157, May 1990, <http://www.ietf.org/rfc/rfc1157.txt>.

[RFC2571] Harrington, D., R. Presuhn, and B. Wijnen, "An Architecture for Describing SNMP Management Frameworks", RFC 2571, April 1999, <http://www.ietf.org/rfc/rfc2571.txt>.

[RFC2827] Ferguson, P. and D. Senie, "Network Ingress Filtering: Defeating Denial of Service Attacks which employ IP Source Address Spoofing", RFC 2827, May 2000, <https://tools.ietf.org/html/rfc2827>.

[RFC3411] Harrington , D., R. Presuhn, and B. Wijnen, "An Architecture for Describing Simple Network Management (SNMP) Frameworks", RFC 3411, December 2002, <http://www.ietf.org/rfc/rfc3411.txt>.

[RFC3412] Case, J., D. Harrington, R. Presuhn, and B. Wijnen, "Message Processing and Dispatching for the Simple Network Management Protocol (SNMP)", RFC 3412, December 2002, <http://www.rfc-editor.org/rfc/rfc3412.txt>.

[RFC3413] Levi, D., P. Meyer, and B. Stewart, "Simple Network Management Protocol (SNMP) Applications", RFC 3413, December 2002, <http://www.ietf.org/rfc/rfc3413.txt>.

[RFC3414] Blumenthal, U. and B. Wijnen, "User-based Security Model (USM) for version 3 of the Simple Network Management Protocol (SNMPv3)", RFC 3414, December 2002, <http://tools.ietf.org/html/rfc3414>.

[RFC3415] Wijnen, B., R. Presun, and K. McCloghrie, "View-based Access Control Model (VACM) for the Simple Network Management Protocol (SNMP)", RFC 3415, December 2002, <http://www.rfc-editor.org/rfc/rfc3415.txt>.

[RFC3416] Presuhn, R., J. Case, K. McCloghrie, M. Rose, and S. Waldbusser, "Version 2 of the Protocol Operations for the Simply Network Management Protocol (SNMP)", RFC 3416, December 2002, <http://tools.ietf.org/html/rfc3416>.

[RFC3417] Presuhn, R., J. Case, K. McCloghrie, M. Rose, and S. Waldbusser, "Transport Mappings for Simply Network Management Protocol (SNMP)", RFC 3417, December 2002, <http://www.rfc-editor.org/rfc/rfc3417.txt>.

[RFC3418] Presuhn, R., J. Case, K. McCloghrie, M. Rose, and S. Waldbusser, "Management Information Base (MIB) for the Simple Network Management Protocol (SNMP)", RFC 3418, December 2002, <http://www6.ietf.org/rfc/rfc3418.txt>.

[RFC3512] MacFaden, M., D. Partain, J. Saperia, and W. Tackabury, “Configuring Networks and Devices with Simply Network Management Protocol (SNMP)”, RFC 3512, April 2003, <http://tools.ietf.org/html/rfc3512>.

[RFC3704] Baker, F. and P. Savola, “Ingress Filtering for Multihomed Networks”, RFC 3704, March 2004, <http://www.ietf.org/rfc/rfc3704.txt>.

[RFC3871] Jones, G., “Operational Security Requirements for Large Internet Service Provider (ISP) IP Network Infrastructure”, RFC 3871, September 2004, <http://tools.ietf.org/html/rfc3871>.

[RFC3954] Claise, B., “Cisco Systems NetFlow Services Export Version 9P”, RFC 3954, October 2004, <http://www.ietf.org/rfc/rfc3954.txt>.

[RFC4732] Handley, M. and E. Rescorla, “Internet Denial-of-Service Considerations”, RFC 4732, November 2006, <http://tools.ietf.org/html/rfc4732>.

[RFC5101] Claise, B., “Specification of the IP Flow Information Export (IPFIX) Protocol for the Exchange of IP Traffic Flow Information”, RFC 5101, January 2008, <http://tools.ietf.org/html/rfc5101>.

[RFC5102] Quittek, J., S. Bryant, B. Claise, P. Aitken, and J. Meyer, “Information Model for IP Flow Information Export”, RFC 5102, January 2008, <http://tools.ietf.org/html/rfc5102>.

[RFC6204] Singh, H., W. Beebee, C. Donley, B. Stark, and O. Troan, “Basic Requirements for IPv6 Customer Edge Routers”, RFC 6204, April 2011, <http://tools.ietf.org/html/rfc6204>.

[RFC6561] Livingood, J., N. Mody, and M. O’Reirdan, “Recommendations for the Remediation of Bots in ISP Networks”, RFC 6561, March 2012, <http://tools.ietf.org/html/rfc6561>.

[A Look Inside the Anonymous DDoS Attack Code] InfoSec Island, “A Look Inside the Anonymous DDoS Attack Code”, August 2011, <http://infosecisland.com/blogview/16065-A-Look-Inside-the-Anonymous-DDoS-Attack-Code.html>.

[Digging into SNMP in 2007] Rey, E. and D. Mende, “Digging into SNMP in 2007 – An Exercise on Breaking Networks”, HackintheBox Security Conference 2007, April 2007, <http://www.ernw.de/content/e7/e181/e671/download690/ERNW_026_SNMP_HitB_Dubai_2007_ger.pdf>.

[Egress Filtering FAQ] Brenton, C., “Egress Filtering FAQ”, SANS Institute InfoSec Reading Room, April 2006,

<http://www.sans.org/reading_room/whitepapers/firewalls/egress-filtering-faq_1059>.

[IANA Service Name and Transport Protocol Port Number Registry] Internet Assigned Numbers Authority (IANA), "IANA Service Name and Transport Protocol Port Number Registry", April 2012, <http://www.iana.org/assignments/service-names-port-numbers/service-names-port-numbers.xml>.

[Inside Anonymous DDoS Code] Holden, A., "Inside Anonymous DDoS Code", August 2011, <http://www.cyopsis.com/news/news-topic-a/45>.

[Microsoft Security Intelligence Report Vol. 11] Faulhaber, J., et al., "Microsoft Security Intelligence Report Volume 11: An in-depth perspective on software vulnerabilities and exploits, malicious code threats, and potentially unwanted software in the first half of 2011", 2011, <http://download.microsoft.com/download/0/3/3/0331766E-3FC4-44E5-B1CA-2BDEB58211B8/Microsoft_Security_Intelligence_Report_volume_11_English.pdf>.

[Network Hygiene Pays Off] Damas, J.L.S. and D. Karrenberg, "'Network Hygiene Pays Off': The Business Case for IP Source Address Verification", RIPE Network Coordination Centre, May 2008, <http://www.ripe.net/ripe/docs/ripe-432>.

[SANS Top 20 Most Critical Internet Security Threats 2000-2001] SANS Institute, "The Top 10 Most Critical Internet Security Threats – (2000-2001 Archive)", Version 2.504, May 2002, <http://www.sans.org/top20/2000/>.

[Securing the Edge] Vixie, P., "Securing the Edge", ICANN SECSAC 004, October 2002, <http://www.icann.org/en/committees/security/sac004.pdf>.

[SNMP DDoS Vector] Thompson, C., "SNMP DDoS Vector – Secure Your Network NOW!", The Spamhaus Project, December 2011, <http://www.spamhaus.org/news/article/678>.

[SNMP Reflected Denial of Service] Bechtsoudis, A., "SNMP Reflected Denial of Service", Personal Blog, August 2011, <https://bechtsoudis.com/hacking/snmp-reflected-denial-of-service/>.

[Team Cymru on SNMP Attacks] Team Cymru Video, "Episode 107 – DDoS mitigation & visualization + conference and training updates", March 2012, <http://youtu.be/6sufNXgsUxY>.

[The Secret Behind LOIC? Simple!] Passeri, P., "The Secret Behind LOIC? Simple!", August 2011, <http://hackmageddon.com/tag/rdos/>.

[Threat Advisory: SNMP Amplification DDoS] Prolexic, "Threat: SNMP Amplication DDoS (SAD)", Prolexic Threat Advisory, March 2012,

<http://www.prolexic.com/pdf/ProlexicThreatAdvisorySNMP.pdf>.

[U.S. Anti-Bot Code of Conduct] Communications Security, Reliability and Interoperability Council (CSRIC), "U.S. Anti-Bot Code of Conduct (ABCs) for Internet Service Providers (ISPs) – (A Voluntary Code)", Working Group 7 – Botnet Remediation, March 2012, <http://transition.fcc.gov/bureaus/pshs/advisory/csric3/CSRIC-III-WG7-Final-Report.pdf>.

[Wikipedia – SNMP] Wikipedia, "Simple Network Management Protocol", April 2012, <http://en.wikipedia.org/wiki/Simple_Network_Management_Protocol>.

9. Glossary of Terms

- Access Control List (ACL): A technique for restricting access to a service or network element using IP addresses or other information available in a data packet.

- Bot: Short for Internet bot or malicious robot. The term is used to refer to a computer that has been infected with malicious software that allows for an untrusted source to remotely control and manage the device. [See also RFC 6561, Section 1.1.1 and 1.1.2]

- Bot Network: A collection of remotely controlled bots operating together. [See also RFC 6561, Section 1.1.2]

- Home Gateway Device: A network element that creates, connects to, or extends a home network for an end user. These devices can perform a range of functions, such as connecting to the Internet, creating or extending a wireless network, providing backup and storage, etc. [See also RFC 6204]

- Ingress filtering: A network technique to prevent source IP address spoofing on inbound traffic. [BCP 38] [BCP 84]

- Malware: Short for malicious software. Applications used for nefarious purposes. [See also RFC 6561, Section 1.1.4]

- NetFlow and IPFIX: NetFlow [RFC 3954] and IPFIX, Internet Protocol Flow Information eXport [RFC 5101] [RFC 5102], are methods to export network traffic data. This data can then be analyzed and studied by network administrators in order to troubleshoot problems, for example.

- Reverse Path Forwarding: The use of a route table to determine the reasonableness of a source IP address. [See also RFC 3704]

- SNMP: Simple Network Management Protocol. The protocol used to manage and monitor network elements such as routers, switches, customer premise equipment, and more. Most elements have both read only and read/write SNMP access.

- UDP: Universal Datagram Protocol. UDP is a communication method which does not require the receiving end to validate information is arriving in a proper sequence or if packets were lost.

10. Document Contributors and Reviewers

- Fred Baker, Cisco
- Uma Chandrashekhar, Alcatel Lucent
- William Check, NCTA
- Mark Clougherty, Alcatel Lucent
- Alissa Cooper, Center for Democracy and Technology (CDT)
- Leslie Daigle, Internet Society (ISOC)
- Chuck Dvorak, AT&T
- Michael Fargano, CenturyLink
- Ken Florance, Netflix
- Amer Hassan, Microsoft
- Trace Hollifield, Bright House Networks
- Kevin Kahn, Intel
- Jason Livingood, Comcast
- Larry Menten, Alcatel Lucent
- Andrei Robachevsky, Internet Society (ISOC)
- Raymond Sliteris, Time Warner Cable
- Donald Smith, CenturyLink
- Barbara Stark, AT&T
- William Sweeney, Comcast
- Jeff Swinton, Verizon
- Jason Weil, Time Warner Cable
- Steven Weinstein, Motion Picture Laboratories
- Damon Yuhasz, Viacom