It Takes a Village to Defend a Network

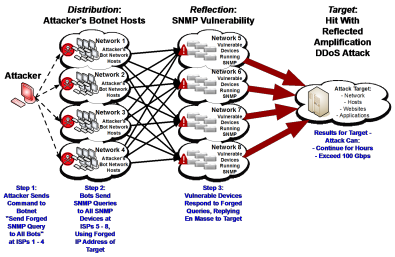
by Alissa Cooper [1]
August 1, 2012

Defending networks from malicious hacking exploits depends in large part on the voluntary, cooperative efforts of network operators, device makers, and Internet users.

Today the Broadband Internet Technical Advisory Group (BITAG) -- a group of technical experts dedicated to building consensus about broadband network management -- has released a series of targeted, balanced recommendations [2] to help stifle an emerging type of network attack. That attack has been used in recent years by the hacker collective Anonymous (among others) to swamp web sites with traffic, knocking them offline.

The attack, shown below, exploits two Internet vulnerabilities: the failure of some network operators to apply recommended protections that prevent users from impersonating ("spoofing") other users' IP addresses, and the lack of adequate authentication in certain home router software that implements the Simple Network Management Protocol ("SNMP").

The attack begins with an army of zombie computers (a "botnet") that the attacker can control. The attacker instructs the computers in the botnet to send traffic to users whose home routers may contain the SNMP vulnerability. That traffic is sent with a spoofed return address to make it look as if it came from the web site that is the intended victim (say, www.example.com [3]). When the users' home routers respond, their responses flood www.example.com [3], taking it offline.



[4]

BITAG recommends a set of highly targeted actions that network operators, device makers, and end users can take, together and separately, to help prevent this kind of attack in the future while having minimal effects on legitimate uses of the network. The set of suggestions reflects just the kind of focused, balanced, user-empowering response to network management and security issues that we would hope to see out of voluntary forums like BITAG. The recommendations fall into four categories:

- **Secure SNMP** – or leave it turned off in the first place. Many home networking devices are shipped with an insecure version of SNMP turned on by default, even though it sees little use among residential end users. BITAG makes a number of recommendations to encourage the use of secure versions of SNMP, to discourage insecure SNMP from being on by default, and to allow users to turn off SNMP themselves.
- **Prevent address spoofing.** BITAG suggests that network operators take reasonable steps to prevent address spoofing on their networks – a well-understood best practice [5] in the engineering community.
- **Filter or block SNMP traffic if necessary, but do so in a targeted, transparent, user-friendly way.** Some network operators may feel the need to simply block SNMP traffic (in the middle of an attack, or perhaps on a more persistent basis) in a similar fashion to how some operators already block certain network ports [6] used to send spam. BITAG recommends a number of strategies for limiting the collateral damage from such filtering/blocking and for ensuring that users understand what is happening and how to have SNMP re-enabled if they wish.
- **Share attack information.** When done with an eye towards safeguarding customer

privacy, network operators and attack victims can help mitigate attacks by sharing attack traffic information with each other, other network operators, security researchers and product vendors, and device makers. BITAG suggests a limited set of specific information that may be useful for sharing.

BITAG's work shows that while the debate about legislating for cybersecurity rages on, experts from across the Internet industry and the public interest community are working together to defend against the latest network attacks while ensuring minimal impact on legitimate network use.

-
- botnets

Links:
[1] https://www.cdt.org/personnel/alissa-cooper
[2] http://www.bitag.org/documents/SNMP-Reflected-Amplification-DDoS-Attack-Mitigation.pdf
[3] http://www.example.com
[4] https://www.cdt.org/files/inline/botnet.png
[5] http://tools.ietf.org/html/bcp38
[6] http://customer.comcast.com/help-and-support/internet/list-of-blocked-ports