CLOUDMARK®

Mobile Broadband Solution Overview

OUTBOUND MESSAGING SECURITY FOR BROADBAND NETWORKS

Benefits Carrier-Grade Security for Outbound Messaging Threats and Abuse

INTRODUCTION

Mobile Broadband adoption is experiencing rapid growth. In 2009, worldwide subscriber counts exceeded 250 million users with nearly 100 million users concentrated in Asia alone–by far the fastest growing region in terms of subscribers. This represents more than a 93% increase from a year earlier, with an even faster adoption trajectory expected in 2010 and beyond.

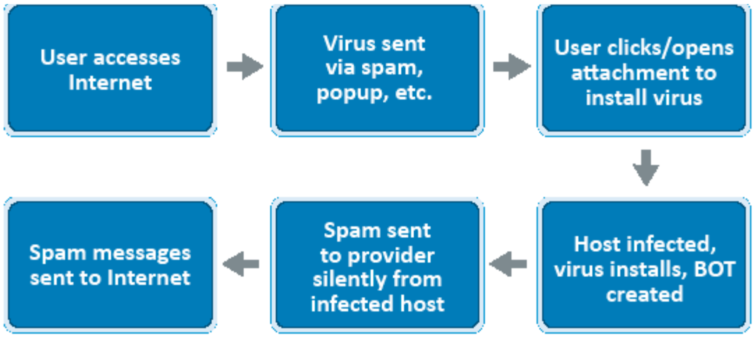
In regions where terrestrial infrastructure is not readily available due to high infrastructure costs, an increased number of operators are launching mobile broadband services. With improved radio access technologies, increased bandwidth availability, lower cost of service, and greater consumer dependence on the internet, mobile broadband is experiencing rapid adoption in these developing areas. This growth is being further reinforced by several government subsidies, reducing the initial cost burden on the operator.

Mobile Broadband providers face the following challenges with messaging threats:

1. Proliferation of outbound spam causes operator IPs to be added to worldwide real-time blocklists (RBLs). As a result, legitimate users can no longer send email, generating support calls and significant costs to the operator. This is especially true in emerging markets like Latin America, Africa, China, and India.

2. Mobile operators are launching broadband services but do not have internet service provider (ISP) expertise. With inadequate outbound messaging security, spammers compromise and infect hosts connected to their networks, and send spam from these compromised systems, a method called reputation hijacking. Sending operator is identified as a spam sender, and their brand reputation is tarnished.

Cloudmark's unique solution offers preventative layers of protection to address outbound spam and threats. With its combination of best-in-class content and message filters, and its intelligent throttles and protocol filters, Cloudmark minimizes the risk of loss and network burden to mobile operators while maximizing profits (i.e. volume-based billing for spammers).


User accesses Internet
Virus sent via spam, popup, etc.
User clicks/opens attachment to install virus
Host infected, virus installs, BOT created
Spam sent to provider silently from infected host
Spam messages sent to Internet

CHALLENGES WITH OUTBOUND SPAM

Outbound spam problems on broadband networks are the result of a key trend in messaging abuse - the convergence of spam and viruses to create "zombie hosts." Spammers create viruses that silently infect these hosts creating a masked channel for messaging abuse. When these infected hosts connect to mobile broadband, their accounts are leveraged to send massive spam attacks that appear to come from the operator's IP-space. See Figure 1. This results in global RBLs detecting and blocking the source of spam identified as the operator, causing a significant negative impact on an operators' reputation, and increases operational and customer support costs.

User impact varies depending upon the chosen network architecture:

1. With NAT deployed at the Internet gateway, valid users' webmail and email services are adversely affected, because an entire block of NAT addresses is blacklisted by commercial and private RBLs. A potentially large block of valid users could be impacted.
2. With DHCP, without NAT at the Internet gateway, valid users could be adversely affected, by receiving a blacklisted IP, previously assigned to a spammer.

THE SOLUTION

Outbound messaging abuse is best fought at the broadband network edge for maximum visibility as packets leave the network. Cloudmark's outbound messaging security is deployed in several modes (in-line or policy-based redirect) and runs in a standalone, low-latency and high-performance platform deployed in-between the mobile edge router (i.e. GGSN, PDSN, ASN GW, BRAS) and the Internet gateway. There are two primary components in Cloudmark's outbound messaging security solution:

1. Network and Protocol-level Controls – These controls monitor connections, inspect sender-IP and leverage a real-time reputation database to block messaging abuse from known spammers or botnets located inside the network. Additionally, for those suspect senders, the platform can throttle or rate limit connections to make any potential attack ineffective

2. Content or Message Scanning and Filtering – In the event a spam message successfully passes through the network and protocol-level controls, an additional layer of protection scans the full message and implements filtering solutions for spam, viruses, and malware to block infected messages from being sent out to the internet. A global threat network of trusted reporters shares threat intelligence to further ensure maximum accuracy.

A comprehensive, carrier-class, messaging security solution delivers:

1. Increased trust through a secure messaging network. Operators around the world would have an increased level of confidence in traffic sourced by the protected operator.

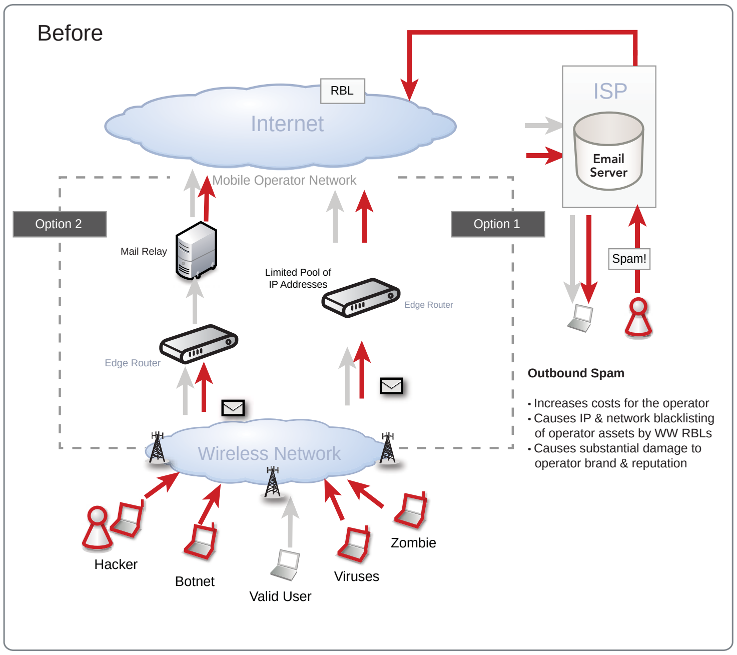
2. An infrastructure that deters spammers from maliciously leveraging the network. Network and Protocol controls can be implemented so operators can charge spammers for all traffic generated by them and rate-limit traffic to levels where it is ineffective for spammers to generate spam.

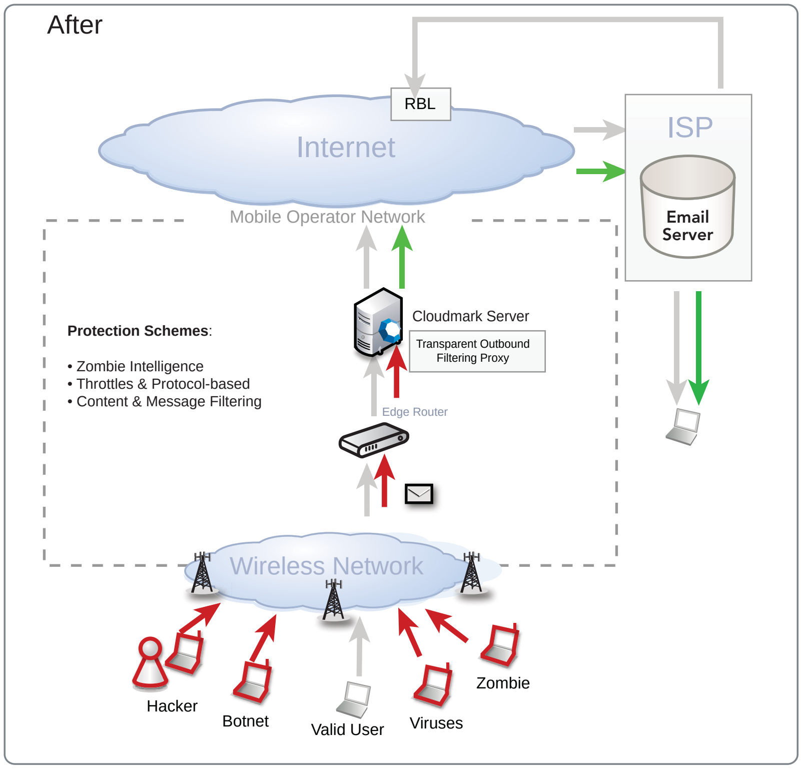
Cloudmark's solution for mobile broadband is a network-layer solution that leverages a carrier grade content filtering solution with full protocol transparency for SMTP, to effectively filter outbound email with no impact to the end-user. With the Cloudmark solution, the reputation of operator IP addresses are protected, ensuring continuous service to their customers.

With Cloudmark's carrier-grade messaging security solution for broadband networks, all emails go through an SMTP protocol transparency layer and are scanned by Cloudmark Authority, with over 99% filtering accuracy. Cloudmark Authority® delivers the industry's most effective and highest performing anti-spam, anti-phishing and anti-virus protection. Because the solution is fully transparent, the end user does not see a header indicating mail was scanned. Mobile operators who deploy Cloudmark's solutions for broadband will not experience a relay, or extra 'hop' within their network.

HOW IT WORKS

Cloudmark's solution for broadband integrates in transparent mode into the SMTP message stream to filter outbound email. Cloudmark prevents mobile broadband users, who may be infected by botnets, from sending spam to other service providers.


Before
RBL
Internet
ISP
Email Server
Mobile Operator Network
Option 2
Option 1
Mail Relay
Limited Pool of IP Addresses
Edge Router
Edge Router
Spam!
Outbound Spam
• Increases costs for the operator
• Causes IP & network blacklisting of operator assets by WW RBLs
• Causes substantial damage to operator brand & reputation
Wireless Network
Hacker
Botnet
Valid User
Viruses
Zombie



Solution Benefits

1. Protects Reputation

   Spam impacts operators with limited IP space and puts them at high risk of becoming blacklisted. Cloudmark protects brand reputation by mitigating the risk of outbound spam, thus protecting operator's IP space.

2. Ensures Satisfied Customers

   Blacklisting from outbound spam prevents delivery of email from legitimate customers, disrupting the user experience. Cloudmark ensures customer satisfaction by delivering continuous email service and protection.

3. Optimizes Network Traffic and Saves Money

   Spam takes up precious and expensive 3G network resources. Cloudmark optimizes traffic by eliminating bad traffic due to spam.

CONCLUSION

We described the architecture and operation of the Cloudmark Global Threat Network service and illustrated the emergent properties of the reputation system underlying the classifier. We also presented a framework for evaluating the efficacy of spam fingerprinting algorithms.

Finally, we also contrasted the GTN approach with other popular methods for classifying spam. The actual architecture and algorithms currently used in the Global Threat Network service are quite complex. The descriptions above have been simplified to highlight the central themes. We hope that we have conveyed the importance of reputation-based methods in the fight against spam.

REFERENCES

1. Availability heuristic. http://en.wikipedia.org/wiki/Availability_heuristic. Accessed on September 28, 2005.
2. DomainKeys Identified Mail. http://mipassoc.org/dkim/. Accessed on September 28, 2005.
3. The rise of reputations in the fight against spam. http://linuxworld.sys-con.com/read/48128.htm. Accessed on September 28, 2005.
4. Sender Policy Framework. http://spf.pobox.com/. Accessed on September 28, 2005.
5. Vipul's Razor. http://razor.sf.net/. Accessed on September 28, 2005.
6. A Plan for Spam. http://www.paulgraham.com/spam.html, August 2002. Accessed on September 28, 2005.
7. D. Chaum. Untraceable electronic mail, return addresses, and digital pseudonyms. Communications of the ACM, February 1981.
8. R. Dingledine, N. Mathewson, and P. Syverson. Tor: The second-generation onion router. In Proceedings of the 13th Usenix Security Symposium, 2004.

For more information
visit us at www.cloudmark.com