AUG 2014

In the Boxing Ring

Network Box Technical News

from Mark Webb-Johnson, CTO Network Box

Welcome to the August 2014 edition of In the Boxing Ring

This month, we discuss in detail Domain Name System (DNS) Amplification and other Attacks. The DNS is the Internet facility primarily responsible for converting name into IP addresses. A typical DNS amplification attack involves the attacker sending a DNS lookup request to an open DNS server, but spoofing the source address to be the IP address of the target. This and how to mitigate against other forms of DNS attacks are discussed further on pages 2-3

On pages 4-5, we highlight the features and fixes to be released in this month's patch Tuesday for Network Box 5 and Network Box 3. We continue to develop, and will continue to support, Network Box 3 for the foreseeable future (several years).

Finally, we are pleased to that Network Box has been listed as one of only fifteen **Notable Vendors** in the latest Global Managed Security Services Provider (MSSP) report, published by Gartner. For a summary of the report, use the link in the article. To purchase the report, please contact Gartner directly as only Gartner clients have full access.

Mark Webb-Johnson
CTO, Network Box Corporation Ltd.
August 2014

You can contact us here at HQ by eMail (nbhq@network-box.com), or drop by our office next time you are in town. You can also keep in touch with us by several social networks:

Twitter http://twitter.com/networkbox

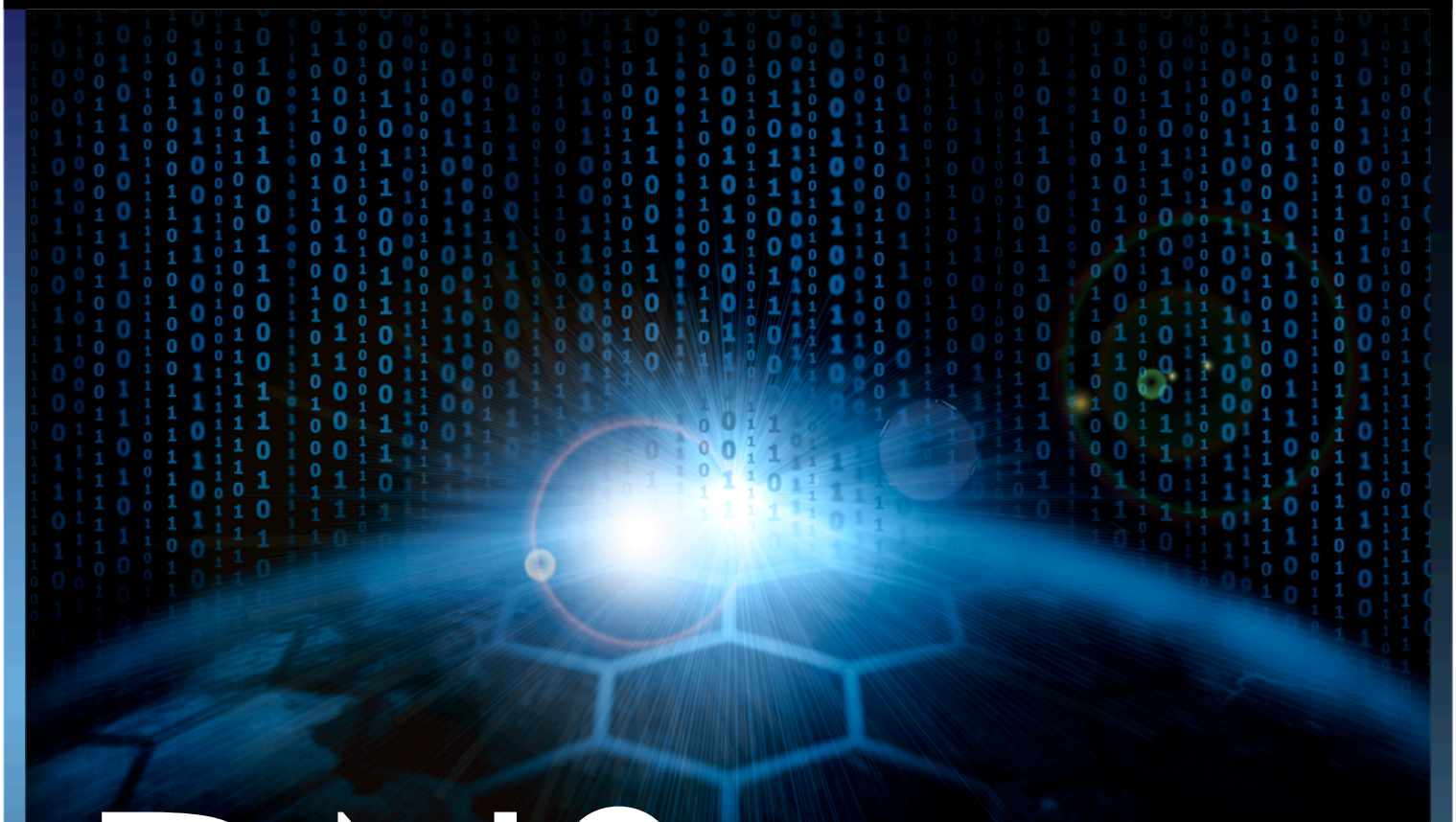
facebook http://www.facebook.com/networkbox
http://www.facebook.com/networkboxresponse

LinkedIn http://www.linkedin.com/company/network-box-corporation-limited

Google+ https://plus.google.com/u/0/107446804085109324633/posts

In this month's issue:

NETWORK BOX



DNS AMPLIFICATION (and other) Attacks

In recent months Network Box Security Response has been monitoring an increasing number of DNS Amplification Attacks both targeting, as well as attempting to leverage, our customers' DNS infrastructure. This article gives some background information on these attacks, along with advise for how to survive.

The Domain Name System (DNS)

The Domain Name System (aka DNS) is the Internet facility primarily responsible for converting name (www.network-box.com) into IP addresses (218.213.64.30 and 2001:df0:a5::18). It can also be used to store textual records, mail routing records, and other information. Applications using DNS typically connect over UDP port 53, although TCP port 53 is used as a fallback for large records as well as bulk information transfer. Being based on UDP means that the protocol is vulnerable to spoofing attacks (where the sender IP address is not real, but is spoofed to look like someone else), and this is indeed where most of the problems are based.

Open DNS Servers

The core problem, and first to address, is that of 'open' DNS servers. DNS requests typically fall into one of two categories: authoritative and non-authoritative, and the issue is one of recursive lookups to non-authoritative DNS servers.

1. In the case of an authoritative request, a DNS request for a particular domain name is sent to the server directly responsible (authoritative) for that domain name - the response is said to be 'authoritative' because the DNS server represents the authority for that domain and the DNS clients need look no further.

2. In the case of a non-authoritative request, a DNS request for a particular domain name is sent to a server not directly responsible (not authoritative) for that domain name. In such cases, the server can do one of two things - it can either refuse the request, or it can go ahead and look up the domain (recursively) on behalf of the client.

The problem comes from DNS servers that are publicly available and configured to allow recursive requests from public (non-trusted) clients. If your DNS server is configured in such a way, then remote untrusted users can use your server to lookup other people's domains. More importantly, remote malicious users can use your DNS server to attack other people's DNS servers over the Internet. The problem is very similar to that of third-party-relay with SMTP email.

So, the first step in defense is to lock-down the configuration of your DNS server to only permit recursive requests from your own users, and to deny such requests from untrusted IP addresses. In BIND, that is trivial ("allow-recursion { my-networks-only; }", with an appropriate ACL), but in Microsoft DNS server it is tricky and requires the roles of authoritative name servers and recursive name servers to be split across two different machines (either that or use a Network Box and we'll handle the recursive role for you).

I cannot stress enough how important locking down the configuration of any publicly accessible DNS servers is. It is no longer a matter of "if", but more "when" your DNS server will be leveraged by someone malicious to attack someone else, and you will get the blame. Statistically you are vastly more likely to be leveraged as the source of an attack, than to be the target of such an attack, but both have equally disastrous impact on your network service availability.

Mitigation Technique:

Custom IPS rules can be enabled at the perimeter Internet Threat Protection device, to deny recursive DNS lookups coming from untrusted public IP address ranges. Rate limiting can also be used, per source IP (even spoofed).

DNS Amplification Attacks

A typical DNS amplification attack involves the attacker sending a DNS lookup request to an open DNS server, but spoofing the source address to be the IP address of the target. Often, the "ANY" resource type is requested, to return a large amount of information in the response, and the response packets quickly overloads the target server. Such attacks levels open DNS servers, so cannot leverage you if your DNS server is not open to recursive queries. You can still be the target of such an attack.

Mitigation Technique:

Custom IPS and firewall rules can be enabled at the perimeter Internet Threat Protection device, to deny DNS replies as the first packet of a new network connection. Custom rules can also be enabled to detect and block the most common known such DNS attacks (often based on threshold limits for aggressive response).

Conclusion

Longer-term, there are efforts underway to secure the underlying DNS protocol, but those are many years off and will require extensive upgrades to the DNS infrastructure. Short-term, the best solution is to make sure you are not part of the problem by disabling recursive lookups on your public-facing DNS servers, and to make sure you have protection in place so that you can mitigate the attack if you are targeted.

Network Box 5

NEXT GENERATION MANAGED SECURITY

On Tuesday, 5th August 2014, Network Box will release our patch Tuesday set of enhancements and fixes. The regional SOCs will be conducting the rollouts of the new functionality in a phased manner over the next 7 days.

Network Box 5 Features
August 2014

This month, for Network Box 5, these include:

- Improvements to disk space housekeeping, especially on SSD based S-class devices
- Fix to logging of SMTP unexpected negative server responses
- Memory optimizations in web portals (both user and administrative), to reduce memory requirements
- Memory optimizations in mail message scanning engines, to reduce memory requirements
- Memory optimizations in mail envelope scanning engines, to reduce memory requirements
- Improvements to error recovery mechanism in event logging systems
- Enhancements to anti-spam eMail categorization related to large attachments
- New 'rate-a-site' URL categorization facility in administrative web portal
- New facility for periodic report templates in administrative web portal
- New Network / Interfaces screen in administrative web portal
- New Analysis / High Availability screen in administrative web portal
- Improvements to error display in administrative web portal, for invalid widgets on dashboard
- Improvements to support for boxes west of GMT in web client analysis
- Performance improvements in Analysis / Mail and Analysis / WebClient screens of administrative web portal
- Change to administrative web portal to refuse negotiation of non-high security ciphers in HTTPS SSL connections
- Renewal of certificate for administrative web portal
- Minor revisions to wording on user portal reports
- Introduction of a new KPI to track system WORKLOAD
- Introduction of a new KPI to track system MEMORY utilization
- Introduction of a new KPI to track FRONTLINE IPS utilization
- Introduction of a new KPI to track IDS utilization
- Introduction of a new KPI to track IPS utilization
- Fix to mail KPI for incoming/outgoing roles (smtpclient vs smtpserver)
- Improvements to PDF reporting to address issues with rendering some table-based report content
- Support for new regional data centres in UK and New Zealand
- Improvements in Z-SCAN system used by eMail anti-spam categorization
- Introduction of a configuration search mechanism in command line administrative interface
- Improvements to case insensitive searches in command line and web administrative interfaces
- Enforcement of clock synchronization prior to configuration changes being permitted
- Improved support for IDS capture on bridged interfaces
- Improved support for VLANs on bridged and bonded interfaces

In most cases, the above changes should not impact running services or require a device restart. However, in some cases (depending on configuration), a device restart may be required. Your local SOC will contact you to arrange this if necessary.

Should you need any further information on any of the above, please contact your local SOC. They will be arranging deployment and liaison.

NETWORK BOX

Network Box 3 Features August 2014

On Tuesday, 5th August 2014, Network Box will release our patch Tuesday set of enhancements and fixes. The regional SOCs will be conducting the rollouts of the new functionality in a phased manner over the next 7 days. This month, for Network Box 3, these include:

- Revisions to Global Monitoring System test points
- Various (mostly internal) enhancements to several internal support systems

In most cases, the above changes should not impact running services or require a device restart. However, in some cases (depending on configuration), a device restart may be required. Your local SOC will contact you to arrange this if necessary.

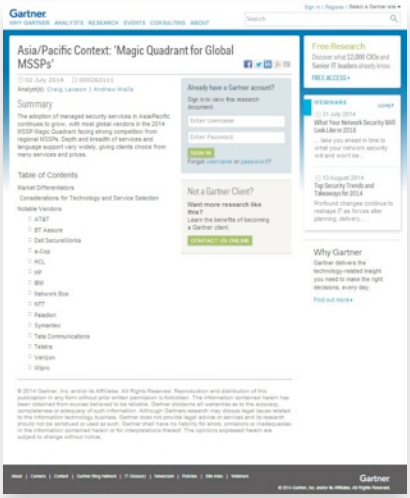
Newsletter Staff	Subscription
Mark Webb-Johnson Editor **Michael Gazeley** **Nick Jones** **Kevin Hla** Production Support **Network Box HQ** **Network Box UK** **Network Box USA** Contributors	Network Box Corporation nbhq@network-box.com or via mail at: **Network Box Corporation** 16th Floor, Metro Loft, 38 Kwai Hei Street, Kwai Chung, Hong Kong Tel: +852 2736-2078 Fax: +852 2736-2778 www.network-box.com

Gartner

Asia/Pacific Context: 'Magic Quadrant for Global MSSPs'

Network Box is proud to announce that the company has been listed as one of only fifteen **Notable Vendors** in the latest Global MSSP report published by Gartner.

LINK: https://www.gartner.com/doc/2788117/asiapacific-context-magic-quadrant-global



Network Box Germany BITKOM

MEMBER OF BITKOM

Network Box Germany has become an official member of BITKOM E.V., Germany's Federal Association for Information Technology, Telecommunications and New Media. BITKOM is the voice of the information technology, telecommunications and new media industry in Germany.

Network Box Korea Official Visit

Network Box visited our Korea office and introduced the latest Network Box 5 technologies, such as Application Control, SSL Proxying, HTML-5 Dashboard, Custom Report Generation, and IPv4 / IPv6 Bridging. Lead by **Young-Man Park**, Network Box Korea has been offering world-class security to the region.