Denial of service attacks have been around since the Internet was commercialized and some of the largest attacks ever launched relied on DNS, making headlines. But every day a barrage of smaller DNS-based attacks take down targets and severely stress the DNS ecosystem. Although DNS servers are not usually the target of attacks they are often disrupted so attention from operation teams is required. There is no indication the problem is going away and attackers continue to innovate. Most disturbing is bot-based DNS DDoS malware is already infiltrating consumer devices like home gateways and web connected cameras. It’s likely malware used in attacks is portable so more “Things” may be inducted.

This paper covers changes in DNS DDoS tactics over the last two years and offers brief perspective on remediation (details can be found in Nominum Whitepaper “Industry Best DNS-based DDoS Protection”)

- Early 2013 - Nominum data shows spikes in DNS queries that amplify at Vantio resolvers. Open Resolver Project shows around 30 million open resolvers on the Internet. Further analysis connects the dots, uncovering 10s of millions of home gateways with open DNS proxies.
- Mid 2013 - “Purpose built” domains specifically designed for amplification attacks found by Nominum researchers, large population of open home gateways enables massive attacks.
- Early 2014 - New attacks discovered sending queries with randomized subdomains to open home gateways, query
spikes cause authorities to fail. About 10% of attacks target popular domains (Alexa 1000)
• Late 2014 - Bot-based DNS DDoS malware running in home gateways and web cams first observed sending queries with randomized subdomains. Popular domains continue to be targeted.
• Early 2015 - Attackers refine their exploits, carefully regulating activity to fly under the radar. Nominum researchers observe new attacks combining random subdomains with amplification.

The Rise of Reflection and Open DNS Proxies
DNS amplification is useful for DDoS because a small DNS query – a few tens of bytes – can produce a large answer of several thousand bytes. In early 2013 Nominum researchers evaluating data collected from Vantio resolvers around the world saw large increases in DNS queries that amplify. Malicious activity regularly created 100s of Gigabits of unwanted traffic. DNS servers suffered considerable collateral damage. What was puzzling was most providers supplying data had “closed” their resolvers, limiting queries to IP addresses within their own network ranges. This meant queries from IPs outside provider ranges would be dropped without any processing and thus not show up in any of the data logs.

Also in early 2013 the Open Resolver Project began to publish results of their scans for open resolvers, initially reporting around 30 million on the Internet. Subsequent collaboration with the researcher revealed data showing nearly 500,000 open Vantio resolvers. Although Vantio resolvers have enjoyed considerable success they hadn’t reached 500,000 installations!

Further analysis provided answers: some home gateways used for provisioning consumer Internet service answered DNS queries coming in on their WAN interface, proxying them to the resolver they are configured to use, in most cases a provider’s resolver. This meant attackers everywhere could send DNS queries to “open” home gateways and get responses. By spoofing source addresses huge waves of amplified DNS traffic could be sent to any target, anywhere. Redirection introduced by home gateways also made it much harder to understand attacks, since only home gateways see spoofed IPs provider resolvers have no visibility into targets which are the ultimate recipient of the traffic.

The massive installed base of open home gateways provided a convenient backdoor to access high performance ISP resolvers. Since legitimate queries were intermingled with malicious ones simply blocking IPs sending malicious queries to resolvers would severely disrupt subscriber communications. Fine-grained filters are needed in resolvers to target troublesome traffic at ingress. Properly configured filters protect good traffic while
eliminating amplification as well as excess work by resolvers processing unwanted queries, and all of the impact on authoritative servers. Filters are needed that can match against any query parameter, and be combined with logical operators such as AND OR NOT etc. For instance: Query Type AND Query Name being attacked.

“Purpose-built” Amplification Domains
In mid-2013 Nominum researchers found another attack innovation: newly registered domains with excessively large resource records, as much as 4000 bytes. Evaluation of the domains and analysis of typical query patterns revealed these “purpose built” domains were heavily correlated with attacks and actively exploiting the vast installed base of open home gateways.

New purpose built domains can appear at any time and resolvers need to be equipped with dynamic threat lists that include purpose built amplification domains to track and deter unwanted traffic they create. Incoming queries can be matched against lists and dropped before consuming additional resolver resources or burdening authoritative servers. Multiple policy actions – BLOCK, REDIRECT, LOG, TRUNCATE provide even more options for managing diverse or unfamiliar suspicious traffic.

Random Subdomain Attacks
Beginning in early 2014 a completely different kind of DDoS attack emerged using use hundreds of millions of randomized labels prepended to targeted domains as shown below:

wxctkzubkb.liebiao.800fy.com
random                 target name

Because names with randomized subdomains are never in-cache, resolution requires more computationally expensive recursion which can substantially spike a resolvers workload. Authoritative servers also often fail, since they don’t benefit from queries being cached at the resolution layer. Cascading authoritative failures result when resolvers navigate around unresponsive name servers, increasing the load on remaining servers. This also increases the load on resolvers themselves. Equipment in front of resolvers like load balancers and firewalls are also stressed and prone to fail because queries either don’t resolve at all or take far longer than normal, resulting in resource exhaust maintaining state.

Activity was relatively light in late January with around 100M queries observed across Nominum’s worldwide data set (estimated at around 3% of ISP resolver traffic). It began to escalate in June with major spikes in November and December - peaking at around 5 billion attack related queries per day.
Target names used for random subdomain attacks typically change every day. As with amplification attacks, equipping resolvers with dynamic threat lists that include new targets offers the best protection. Incoming malicious queries can be dropped before consuming additional resolver resources or burdening authoritative servers.

**Bots Driving DNS DDoS**
Large spikes in queries in November and December 2014 correlated with yet another change in attack tactics: Nominum research observed bots sending queries with randomized subdomains. Bots are software running remotely on compromised devices with centralized “command and control”. Initial research showed bot malware residing in home gateways (this is a different vector than the open DNS proxies) and online surveillance cameras sending DDoS queries. Weak passwords have been implicated as the vector to infect these devices. Consumer device software has an unfortunate history, additional exposure may be created with as yet unknown vulnerabilities.

New DNS DDoS bots were impressively powerful, sustaining 8,000 queries per second, so attacks only needed a few devices to be extremely effective. A large network in Europe was taken down with 100 devices. DDoS bots also seem to be targeting more popular web sites more commonly than earlier attacks.

The bot problem can potentially get much larger because bot infections are widespread in most networks. Consumer PCs become infected with bots in a variety of ways, such as phishing or “drive-by” downloads. Many bots can modify their behavior by simply loading new software so it is possible in-place infections could morph into even more, and more powerful, DDoS participants.

Mitigating DNS DDoS driven by bots has unique challenges. Since queries originate in the network blocking DNS at borders will not be effective. Nor will in-place DDoS equipment help because it lacks DNS specific features to properly cleanse traffic. Fortunately this new bot based variant can also be mitigated with dynamic threat lists and fine grained policies. Robust lists can protect resolvers before they even see attack traffic.

**Emerging Threats**
Attackers continue to innovate. In 2015 more changes have already been observed. There have not yet been large malicious query spikes as in late 2014, instead attackers do their damage by understanding target weaknesses and launching highly intense and focused attacks. It appears they’re trying to make exploits harder to detect, and evading simple defenses.

New techniques are also appearing, like combining randomized labels with queries that amplify. This would seem futile, an NXD answer is
not a good amplifier. But some domains answer, possibly because the domain owners have wildcarded entries.

Again fine-grained ingress filters and matching against dynamic threat lists in resolvers have proven to be the best method for deterring unwanted DNS traffic. An extensible policy framework and carefully curated threat lists can consistently adapt to changing threats.

**Summary**

DNS-based DDoS has rapidly evolved over two years and there is no indication it will stop. Lists of IP addresses of the very large installed base of home gateways with open DNS proxies are available on the Internet, as are turnkey DDoS services that use them. The recent transition to bot driven DDoS malware changes the landscape. Malware infected home gateways are already widely used with devastating impact as are cameras capable of powerful DDoS attacks. It’s likely DDoS malware is highly portable so other devices may be inducted, which could mean as the Internet of Things flourishes it may bring with it unwanted baggage.

Stopping malicious traffic at ingress to DNS resolvers is the best way to address DNS-based DDoS. It prevents attacks from working while minimizing processing work for resolvers. Authoritative servers never see malicious queries. ISP networks and the ultimate targets of DNS-based DDoS are protected. Fine-grained filters and dynamic threat lists are needed to protect good queries while blocking bad ones. Strong foundational capabilities will consistently stand up against fast changing attacks and continue to adapt as attacks evolve.

**About Nominum**

Nominum’s N2 Platform is an integrated suite of applications for service providers that leverages the power of DNS to drive subscriber value. Nominum enables service providers to reduce operating costs, protect networks and subscribers from threats, provide innovative services that engage and retain subscribers, and deliver more effective customer care and marketing campaigns with in-browser messaging that reaches every subscriber, and insights that make cross-sell and upsell promotions more relevant. Nominum is the DNS leader among service providers with deployments at nine of the top 10 service providers and in over 40 countries worldwide. Nominum is a global organization headquartered in Redwood City, California, USA.