nominum

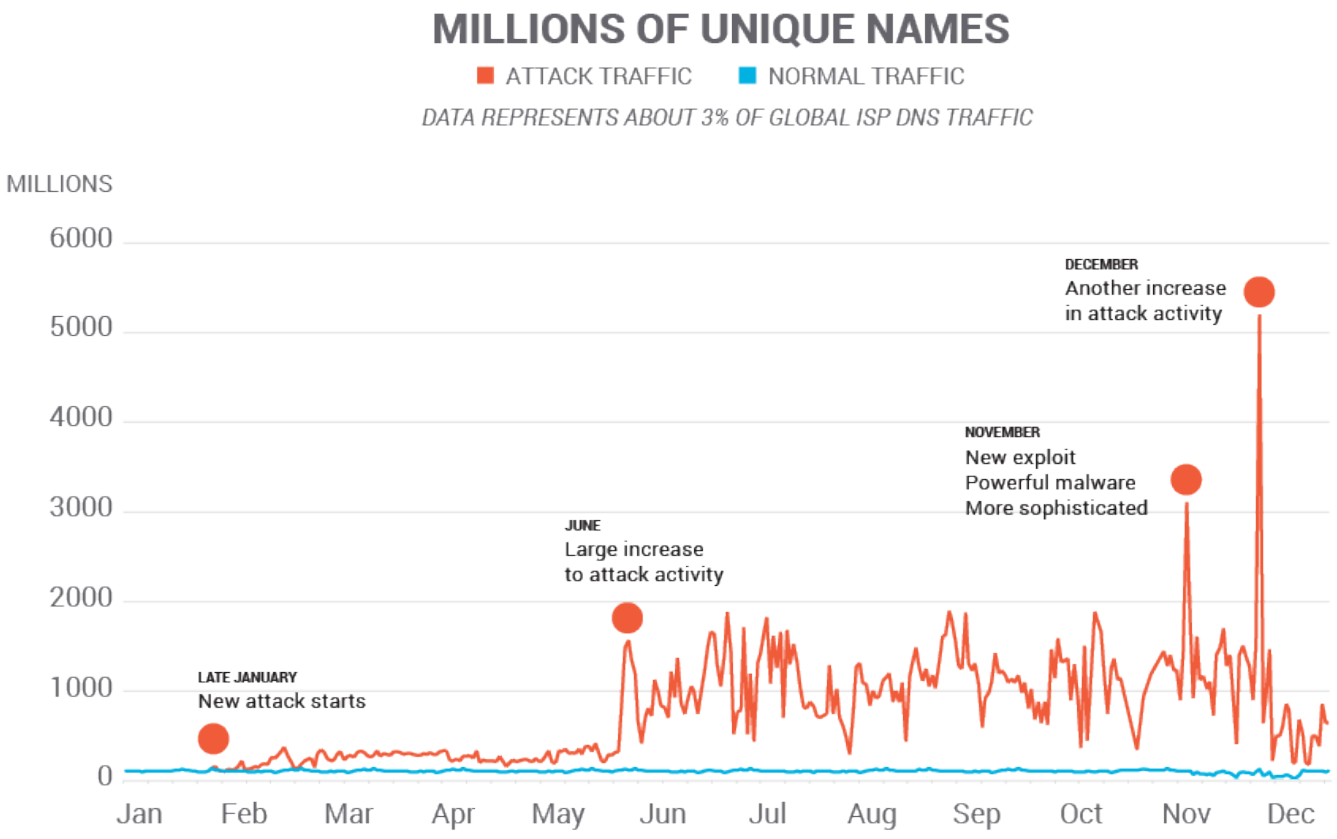
Solution Brief

Bot-based DNS DDoS Attacks

Introduction

DNS is now a mainstream DDoS vector because attackers have figured out how to use provider DNS resolvers to maximize the impact of their exploits. In November 2014 Nominum research uncovered a new kind of DDoS attack initiated by bots using queries with randomized subdomains. In December Attack activity *increased dramatically* to more than 5 B unique names/day. These attacks differ from earlier ones:

- They *don't* use open DNS proxies in home gateways like earlier amplification & random subdomain attacks. Instead malware running in home gateways and other devices source the traffic within provider networks.
- Far *fewer* devices participate in attacks; previously 1,000s of devices used, recently 100 devices had a devastating impact on a large provider network.
- Intensity has increased significantly, a single device was observed sending 8,000 queries, *far higher* than earlier attacks.
- *Popular web sites are becoming targets*, unlike earlier attacks which tended to focus on obscure sites.



Actual attack query volume across the Internet is *far* higher since Nominum data represents about 3% of ISP DNS traffic. The graph also only charts each appearance of a unique name, there are usually duplicate queries for each, doubling the volume of malicious queries again.

Nominum Research found evidence these attacks are generated by bots running in home gateways. Attackers scan the Internet for home gateways with weak passwords, login, and use load malware that enables DDoS attacks. There are direct links between strings discovered in the malware and attack activity. Additional research showed other kinds of devices like cameras can also be compromised and participate in DDoS.

Implications

Since attacks are driven by bots within provider networks many traditional protections won't work:

- ACLs to filter DNS traffic at borders are ineffective since queries are created *within* the network.
- Coarse grained filters in DNS firewalls and other products will cause substantial collateral damage.
- In-place DDoS equipment won't help since malicious traffic is created by distributed bots in the network.
- Load balancers can fail during random subdomain attacks due to resource exhaustion.
- Homegrown scripts require 24/7 manual intervention, detection can be slow, coverage can be inadequate.

Nominum Solution

ThreatAvert uses Precision Policies and Global Intelligence Xchange to block these new attacks. Nominum Research's "early warning system" detects these attacks in 10 minutes on average. Additional validation processing separates legitimate subdomains from those used in attacks before GIX lists are published:

- A block list blocks queries to malicious randomized subdomains
- A white list contains legitimate subdomains associated with target names
- A Precision Policy to tie the lists together is served along with the lists

Updates to GIX lists are distributed automatically where they protect Vantio ThreatAvert servers immediately. Blocking attack traffic using dynamic lists (GIX) is the best way to defend against these attacks:

- Stress on resolvers is eliminated since they don't have to recurse useless traffic
- Authoritative servers never see the queries at all, eliminating the attackers goal of taking down a web site

Fine-grained filters in Precision Policies ensure legitimate traffic for domains targeted in attacks is preserved.

Leadership and Innovation

DNS defenses belong in DNS servers. In order for any other equipment to defend against DNS DDoS it needs to look like a DNS server to properly filter traffic. This validates the premise protections should simply be implemented in DNS servers to begin with. Additional equipment to defend against DNS DDoS also adds cost and complexity and introduces the possibility conflicting configurations have unintended consequences. Finally, coordinating attack mitigation between two groups increases response time and stress on both organizations.

Attackers always adapt their exploits so they remain effective in the face of defenses. Recent examples where Nominum was at the forefront tracking DNS exposure and ensuring provider resolvers are protected include:

- April 2013 - Nominum discovered 10s of millions of home gateways with open DNS proxies that expose provider resolvers to DDoS even if they employ Best Practices like BCP 38 and "close" their resolvers.

Precision Policies deterred early amplification attacks while minimizing over-filtering that provokes subscriber support calls.

- June 2013 - Nominum research exposed new domains with very large Resource Records, created exclusively for DNS amplification. These "purpose built" domains make it easy to launch attacks, especially using the large population of open home gateways.
  Global Intelligence Xchange began targeting these domains when they first appeared, completely automating protection.

- January 2014 - Nominum uncovered a new kind of DDoS attack using open home gateways and queries with randomized subdomains prepended to target domains. Randomized queries are typically not in-cache and thus require computationally expensive recursion, which also stresses authorities at attack-scale.
  Global Intelligence Xchange and Precision Policies targeted these domains when they first appeared in January 2014, again with completely automated protection.

No other vendor has a similar track record consistently identifying new attacks based on in-house researchers evaluating 2 Terabytes of data per day, and leveraging foundational platform capabilities like GIX and fine grained Precision Policies to protect provider DNS.