The DNS of Things

Peter Silva, 2014-09-04

Hey DNS - Find Me that Thing!

There's a new craze occurring in homes, highways, workplaces and everywhere imaginable - the Internet of Things or as I like to call it, The Internet of Nouns. Sensors, thermostats, kitchen appliances, toilets and almost every person, place or thing will have a chip capable of connecting to the internet. And if you want to identify and find those things with recognizable words instead of a 128-bit IP address, you're going to need DNS.

DNS translates the names we type into browser or mobile app into an IP address so the services can be found on the internet. It is one of the most important components of the internet, especially for human interaction. With the explosion of mobile devices and the millions of apps deployed to support those devices, DNS growth has doubled in recent years. It is also a vulnerable target.

While the ability to adjust the temperature of your house or remotely flush your toilet from around the globe is cool, I think one of the biggest challenges of the Internet of Nouns will be the strain on DNS. Not only having to resolve the millions of additional 'things' getting connected but also the potential vulnerabilities and risks introduced when your washing machine connects to the internet to find the optimal temperature and detergent mix to remove those grass, wine and blood stains.

Recent research suggests that the bad guys are already taking advantage of these easy targets. Arstechnica reports that the malware that has been targeting routers has now spread to DVRs. Not my precious digital video reorder!! Last week, Sans found a Bitcoin mining trojan that can infect security camera DVRs. As they were watching a script that hunted the internet for data storage devices, they learned that the bot was coming from a DVR. Most likely, they say, it was compromised through the telnet defaults.

In another report, ESET said it found 11 year old malware that had been updated with the ability to compromise a residential broadband router's DNS settings. The malware finds a vulnerable router and changes the default DNS entries to either send the person to a rogue site to install more malware (join the bot, why don't ya) or to just redirect them to annoying sites. Imagine if the 50+ connected things we will soon have in our homes also joined the bot? Forget about needing compute and bandwidth from machines around the globe, you can zero in on a neighborhood to launch an attack.

Nominum research shows that DNS-based DDoS amplification attacks have significantly increased in the recent months, targeting vulnerable home routers all over. A simple attack can create tens-of-gigs of traffic to disrupt networks, businesses, websites, and regular folks anywhere in the world. More than 24 million home routers on the Internet have open DNS proxies which expose ISPs to DNS-based DDoS attacks and in February 2014 alone, more than 5.3 million of these routers were used to generate attack traffic. These are especially hard to track since it is difficult to determine both the origination and target of the attack.

Lastly, Ultra Electronics AEP says 47% of the internet remains insecure since many top level domains (TLDs) have failed to sign up to use domain name system security extensions (DNSSEC). These include heavy internet using countries like Italy (.it), Spain (.es) and South Africa (.za), leaving millions of internetizens open to malicious redirects to fake websites. Unless the top level domain is signed, every single website operating under a national domain can have its DNS spoofed and that's bad for the good guys.

We often don't think about the Wizard behind the curtain until we are unable resolve an internet resource. DNS will become even more critical as additional nouns are connected and we want to find them by name. F5 DNS Solutions can help you manage this rapid growth with complete solutions that increase the speed, availability, scalability, and security of your DNS infrastructure.

And I do imagine a time when our current commands could also work on, for instance, the connected toilet: /flushdns.

Just couldn't let that one go.

ps

Related:

- “Internet of Things” is the new Windows XP—malware’s favorite target
- Win32/Sality newest component: a router’s primary DNS changer named Win32/RBrute
- 24 million home routers expose ISPs to massive DNS-based DDoS attacks
- 24 million reasons to lock down DNS amplification attacks
- Half the internet lacks DNS security extensions
- F5 Intelligent DNS Scale

Technorati Tags: f5,dns,dnssec,ddos,security,iot,things,big-ip,malware,silva,trojan

Connect with Peter:

Connect with F5:

F5 Networks, Inc. | 401 Elliot Avenue West, Seattle, WA 98119 | 888-882-4447 | f5.com

F5 Networks, Inc.
Corporate Headquarters
info@f5.com

F5 Networks
Asia-Pacific
apacinfo@f5.com

F5 Networks Ltd.
Europe/Middle-East/Africa
emeainfo@f5.com

F5 Networks
Japan K.K.
f5j-info@f5.com