INSIDE RECENT FQDN (FULLY QUALIFIED DOMAIN NAME) SURGES ON THE INTERNET

Erik Wu
Nominum, USA

Email ewu@nominum.com

ABSTRACT

Recently, we have observed unprecedented increases in the number of unique Fully Qualified Domain Names (FQDN) on the Internet. The average daily number of new unique FQDNs increased from about 300 million a year ago to over 2 billion, with spikes of up to 5 billion. Such massive surges of unique domain names have serious consequences and a great impact on the availability and stability of the Internet.

In this talk, we'll provide an in-depth analysis of some recent surges and possible root causes. The analysis work is based on a large collection of DNS data from major ISPs around the world, 3TB per day, representing about 3% of total global DNS traffic. We will discuss some novel methods including multiple level random subdomains used to generate the huge volumes of unique domain names, infection vectors, and other attributions associated with the attacks. We will also present and compare a set of viable technical solutions that can detect and protect against the emerging threat in real-time.

Figure 1 depicts the unique FQDN volumes on the Internet measured in 2014. The level of normal FQDNs marked in blue

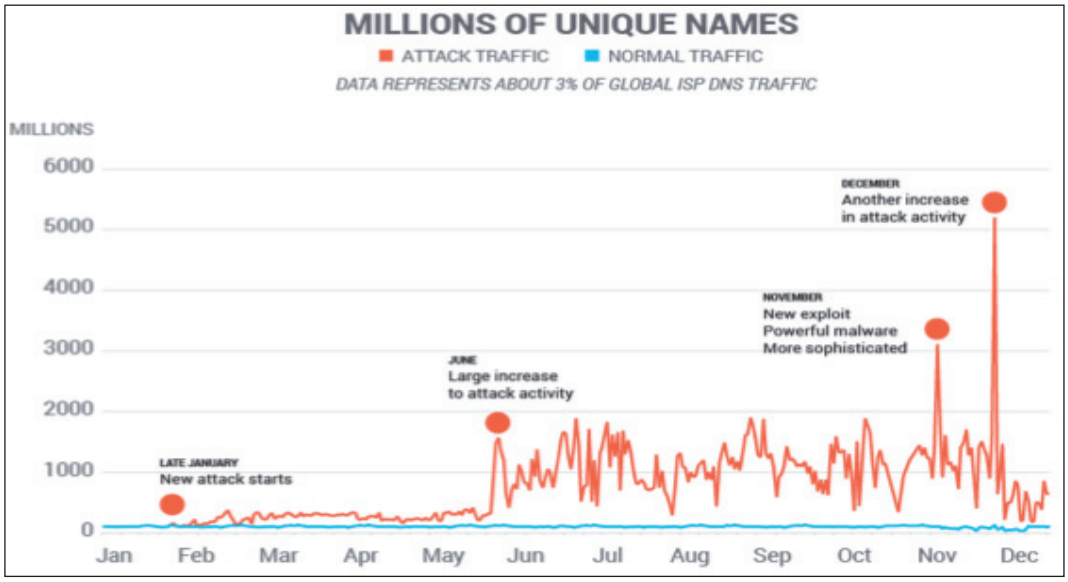

Figure1: Unique FQDN volumes.

```
aopdestuljxym.www.ghjy99.com.
v.www.ghjy99.com.
dsczh.www.ghjy99.com.
cpikeittdnl.www.ghjy99.com.
rzcymzyddkdvowl.www.ghjy99.com.
n.www.ghjy99.com.
dnm.www.ghjy99.com.
rpe.www.ghjy99.com.
bimvzbp.www.ghjy99.com.
nsiemlzmgorcutw.www.ghjy99.com.
kiuyi.www.ghjy99.com.
gthjczbmpxxcidv.www.ghjy99.com.
kgyecokww.www.ghjy99.com.
aopdesthijklz.www.ghjy99.com.
jyy.www.ghjy99.com.
jcxxk.www.ghjy99.com.
airugepbisc.www.ghjy99.com.
vjpealbqguqsunj.www.ghjy99.com.
ktergdolwxuncrqt.www.ghjy99.com.
ctafahkvyrav.www.ghjy99.com.
gxwpojwtmlwz.www.ghjy99.com.
mvsxcfsparot.www.ghjy99.com.
utghitsbwpkvgl.www.ghjy99.com.
kxydkfenkngjatwd.www.ghjy99.com.
szipwvenqjanofct.www.ghjy99.com.
szkbmnutonwbubwf.www.ghjy99.com.
otsngxcvqrcnuz.www.ghjy99.com.
dsiji.www.ghjy99.com.
gkpukoqyp.www.ghjy99.com.
nocdrfghiwxym.www.ghjy99.com.
wytoomrndiqehtc.www.ghjy99.com.
v.www.ghjy99.com.
feeksiuqu.www.ghjy99.com.
xshgrqjsxpt.www.ghjy99.com.
```

Figure 2(a): Online Gaming Subdomains.

```
01jfgq7d.mc.arkhamnetwork.org.
01jo9y9m.arkhamnetwork.org.
01k5jj4u.mc.arkhamnetwork.org.
01kcmfax.arkhamnetwork.org.
01m3t3hd.arkhamnetwork.org.
01mmei6l.mc.arkhamnetwork.org.
01mp5u89.mc.arkhamnetwork.org.
01n002t9.arkhamnetwork.org.
01s8ju2w.arkhamnetwork.org.
01tq7rx6.mc.arkhamnetwork.org.
01tqmsa4.arkhamnetwork.org.
01vaejfk.mc.arkhamnetwork.org.
01vptuga.arkhamnetwork.org.
01xd6ryr.arkhamnetwork.org.
01yc3wss.arkhamnetwork.org.
01yu5f65.mc.arkhamnetwork.org.
01zecuzp.mc.arkhamnetwork.org.
01zl8hx1.mc.arkhamnetwork.org.
01zlz0jj.arkhamnetwork.org.
020w4d2u.arkhamnetwork.org.
021ceyq1.arkhamnetwork.org.
021u7747.arkhamnetwork.org.
022hod0y.arkhamnetwork.org.
024ngogz.mc.arkhamnetwork.org.
025z3goz.arkhamnetwork.org.
0261qw3x.mc.arkhamnetwork.org.
027gfqre.arkhamnetwork.org.
028yi0ur.arkhamnetwork.org.
029zt2pt.arkhamnetwork.org.
02a8x02q.arkhamnetwork.org.
02amyfmj.mc.arkhamnetwork.org.
02btb1bd.mc.arkhamnetwork.org.
02e6ct6l.mc.arkhamnetwork.org.
02f6jro4.mc.arkhamnetwork.org.
```

Figure 2(b): MineCraft Subdomains.

remained relatively low and constant for the entire year, while the red coloured attacking domain name volumes were much higher. The spikes occurred in June, November and December, contributing to several serious outages among major ISPs in different countries.

One reason for the sudden surges was due to the use of random subdomain names, created by adding a random string prefix to an existing domain name (called core- or parent-domain), as follows.

Random subdomain:	wxctkzubkb.temp.proxypipe.net.
Prefix string:	wxctkzubkb
Core- or parent-domain:	temp.proxypipe.net

Initially, the random subdomain technique was used as a simple attacking tool to take down competitors' sites and gain more user traffic among some local online gaming sites, as shown in Figure 2(a). Later, the same approach was widely adopted to attack many other sites including highly ranked ones. Figure 2(b) illustrates some sample subdomain names related to one of the *MineCraft* servers.

We cannot simply block all queries to the subdomains of a highly ranked domain name such as MineCraft without disruption to legitimate traffic. We'll discuss a fine-grained approach that can distinguish legitimate queries from attacking traffic, and accurately stop such attacks.