GhostDNSbusters (Part 3)

team-cymru.com/blog/2021/01/26/illuminating-ghostdns-infrastructure-part-3/

S2 Research Team View all posts by S2 Research Team January 26, 2021

This research was undertaken in collaboration with Manabu Niseki (@ninoseki on Twitter) and CERT.br (https://cert.br).

Last year we posted two blogs detailing our methodology for tracking GhostDNS infrastructure:

- GhostDNSbusters Part 1
- GhostDNSbusters Part 2

In summary, Part 1 focused primarily on the identification of Rogue DNS servers and Part 2 on the discovery and assessment of HTTP phishing infrastructure. This blog provides an update on all infrastructure we have observed since that time – focusing on the period 1st November 2020 to 15th January 2021. As previously, we continue to share details of our investigations, including victim details, with CERT.br.

In December 2020, we posted details of four GhostDNS Rogue DNS servers on our twitter page.

These four servers were identified using queries for the string **dnscfg.cgi?dnsPrimary=** before being cross-referenced against other datasets – confirming them as GhostDNS infrastructure:

149.56.152.185 (OVH, FR)

167.114.138.250 (OVH, FR)

192.95.59.130 (OVH, FR)

51.81.27.247 (OVH, FR)

Note: All four IP addresses are assigned to OVH, FR – however, the first three geolocate to Brazil and the remaining IP address (51.81.27.247) geolocates to the United States.

In identifying these Rogue DNS servers, we also observed 55 IP addresses being used by threat actors to update the DNS settings of vulnerable routers. We previously defined these IP addresses as **Changer** IP addresses – a full list of all identified infrastructure is provided at the end of this blog.

Returning to the four previously referenced Rogue DNS servers and repeating the methodology outlined in our previous blogs, we pivoted on potential victim IP addresses (specifically looking at UDP/53 traffic) in order to identify additional candidate Rogue DNS servers.

In total 14 Rogue DNS servers were identified being queried by potential victims during our period of interest (1st November 2020 to 15th January 2021), of which nine did not appear in our previous blogs.

The below timeline provides an overview of when these Rogue DNS servers were 'active' – based on first and last seen timestamps.

HTTP Phishing Infrastructure

In our second GhostDNS blog, we examined the HTTP phishing infrastructure element of the attack cycle, providing an x.509 certificate being used by one distinct GhostDNS threat group (CDD):

SHA1 – 8D9B394BA67D1913566115094C1AD0257FEFF26E

During our period of interest, we observed two IP addresses hosting this certificate:

45.62.198.176 (most recently 24th December 2020)

45.62.198.69 (most recently 2nd November 2020)

In addition to the IP addresses hosting the x.509 certificate, a further HTTP phishing server (68.183.245.48) was identified based on passive DNS data for Rogue DNS server 192.95.59.130.

In this image, some of the sites/brands targeted by GhostDNS are evident – including Facebook and Netflix.

Three further HTTP phishing servers were identified based on DNS queries performed during the course of writing this blog – and therefore represent the most recent infrastructure:

144.217.105.149

47.88.76.58

18.197.159.147

```
; <<>> DiG 9.10.6 <<>> bb.com.br @192.95.59.130
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 53911
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 1, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 1280
;; QUESTION SECTION:
;bb.com.br.                     IN      A

;; ANSWER SECTION:
bb.com.br.              10800   IN      A       144.217.105.149
```

Indicators of Compromise

Note: The below IOCs were all observed during the period 1st November 2020 – 15th January 2021 and include some IOCs which were shared in our previous blogs.

HTTP Phishing servers [6]

144.217.105.149

18.197.159.147

45.62.198.176

45.62.198.69

47.88.76.58

68.183.245.48

Rogue DNS servers [18]

107.155.152.20

149.56.152.185

158.69.37.88

167.114.138.250

192.95.42.19

192.95.59.130

192.95.63.156

3.131.142.96

45.62.198.242

45.62.198.243

45.62.198.50

45.62.198.54

45.62.198.73

45.62.198.74

45.62.198.89

51.81.101.114

51.81.27.247

51.81.28.240

Changer IP addresses [55]

104.248.84.36

134.122.17.197

134.122.20.72

134.209.114.117

134.209.119.201

134.209.119.215

134.209.194.227

134.209.208.12

134.209.208.32

134.209.208.34

134.209.208.60

134.209.208.89

134.209.208.90

134.209.208.91

142.93.7.241

157.245.240.62

157.245.253.224

157.245.80.115

157.245.87.63

157.245.95.131

157.245.95.198

159.65.197.126

159.65.197.220

159.65.197.67

159.65.197.70

159.65.202.16

159.65.228.195

159.65.228.2

159.65.228.60

159.65.228.79

159.65.236.178

159.89.84.50

161.35.113.178

161.35.113.198

162.243.14.132

165.22.199.47

167.172.39.220

167.71.73.30

168.61.52.32

178.62.254.221

188.166.104.122

188.166.104.148

188.166.105.104

188.166.31.41

188.166.38.126

188.166.90.70

191.252.178.203

192.241.150.141

192.241.165.214

192.81.214.228

198.211.110.224

51.81.53.144

51.81.53.171

64.227.10.49

64.227.22.224