Network Analysis of Yota-Related Resolution Events

1 Introduction

Network traffic analysis strongly suggests communications between Russian networks and Trump Tower, associated Trump properties, with artifacts also present at EOP. Spectrum Health resolver IP `167.73.110.8` in Grand Rapids MI is also observed making similar queries.

The traffic data indicates: (a) There are Russian-made cellular devices on these networks, seldom seen elsewhere in the US; and (b) these networks appear to be attempting SIP-connections to Russian networks which very few IPs globally are seen trying to resolve.

It is possible that one or more devices is at times travelling between locations as there are sometimes gaps possibly correlated to newsworthy events such as New York NY to Grand Rapids MI, lifting of some sanctions on Russia, and the disappearance of the queries from New York in mid December and from Grand Rapids MI in mid January 2017.

This document summarizes factual observations, so that others may infer activities associated with these Russian phones on Trump's networks.

2 YotaPhone Background

Yota is a Russian mobile broadband services provider, owned by Skartel LLC, which operates mobile 4G and microwave access (WiMAX) networks in Russia. Yota sells a line of smartphone devices called the YotaPhone, noted for its "dual screen" form factor (an AMOLED display, and always-on e-ink display on the reverse).

YotaPhones include custom software that periodically connects to Russian networks, e.g., to look for updates or conduct API queries. Thus, YotaPhone owners often resolve domains such as `webapi.yota.ru, asrv.yota.ru, login.yota.ru`, `hello.yota.ru`, and `check.yota.ru` , and `my.yota.ru`. These domains are used by the Yotaphone APIs to display tariff rates, check data usage, and manage online accounts. While spam, misc email, and global passive DNS systems may resolve domains such as `ns[2-3].yota.ru`, the application-layer domains are often only resolved by YotaPhone owners.

The Wall Street Journal reports that Russian president Vladimir Putin gave a Yotaphone as a gift to another world leader:

```
http://blogs.wsj.com/chinarealtime/2014/11/10/\
  vladimir-putin-gives-xi-jinping-a-russian-yotaphone-2-as-gift/
```

```
https://www.youtube.com/watch?v=z4PwsniY-EY
```

Speculation: Russian patriots and Kremlin inner circle might prefer the high end version of the Yotaphone apparently preferred by Putin as well as having the advantage of being ”made in Russia”.

The domain `wimax-client.yota.ru` is listed in the Grizzly Steppe Jar attack and has been discussed on cyber security news websites such as SC Magazine. More information is found at

```
https://www.us-cert.gov/security-publications/\
   GRIZZLY-STEPPE-Russian-Malicious-Cyber-Activity
```

2.1 Rarity of Yota in US

Industry reports note that Yota sales are about 80% in Russia, with only a few hundreds of thousands of units sold. The phone is only available in Russia, Germany, Austria, France and Spain [2]. A stock YotaPhone will work poorly on US networks, because of LTE band differences. [1]. As a result many US YotaPhone users would employ wifi where available. After a failed attempt to bring a version of the phone to the US networks [1], Yota shifted its focus to Asian markets. For US customers, the phone is only available through online retail or travel.

YotaPhones are therefore rarely seen on US networks. Table 1 summarizes the numbers of Yota-related domains resolved globally, for a three week sample period (Sept 28, 2016 to Oct 10, 2016).

2.2 Trump Resolutions of Yota Domains

Although YotaPhones are rare in the US, the Trump Tower network resolved Yota-related related domains at least as early as 2016-09-05:

```
{ "date": "2016-09-05T00:59:14.000Z",
  "qtype": [ "1" ],
  "qname": "ns4.yota.ru",
  "ttl": [ 600 ],
  "ip": [ "94.25.208.69" ],
  ....
}
```

The last resolution took place on December 15, 2016:

```
{ "date": "2016-12-15T09:46:49.000Z",
  "qtype": [ "1" ],
```

[1] AT&T/Verizon use LTE bands 1-5, 8, 13, 17, 19-20 and 25, and T-Mobile uses LTE bands 1-5, 8, 13, 17-20, 25 and 26. The YotaPhone uses LTE bands: 3, 7 and 20

Table 1: Sample of **Global** Yota-related Lookups

counts	**qname**
449225	yota.ru.
105540	ns3.yota.ru.
105506	ns2.yota.ru.
45203	webapi.yota.ru.
43374	asrv.yota.ru.
11814	topology4.dyndns.atlas.ripe.net.
5141	www.yota.ru.
4040	yota-ru.mail.protection.outlook.com.
2370	hello.yota.ru.
2342	my.yota.ru.
1995	forbidden.yota.ru.
1259	login.yota.ru.
1063	client.yota.ru.
1045	welcome.yota.ru.
552	static.yota.ru.
452	wa.yota.ru.
340	widgets.yota.ru.
283	cp2dp.ip-list.emileaben.com.
273	wimax-client.yota.ru.
132	check.yota.ru.
72	cim.yota.ru.
43	corp.yota.ru.
13	b2b.yota.ru.
2	roaming.yota.ru.

Table 2: Trump Network Yota-Related Lookups

counts	qname
250	client.yota.ru
22	ns1.yota.ru
38	ns2.yota.ru
39	ns3.yota.ru
27	ns4.yota.ru
41	wimax-client.yota.ru
6	www.yota.ru
19	yota.ru
3	yota-ru.mail.protection.outlook.com

Table 3: Spectrum Network Yota-Related Lookups

counts	qname
2311	wimax-client.yota.ru
960	client.yota.ru
353	yota.ru

```
  "qname": "ns2.yota.ru",
  "ttl": [ 600 ],
  "ip": [ "94.25.208.69" ],
  ....
}
```

This is a strong indication there was a YotaPhone inside Trump Tower periodically, from at least July 23, and up until December 15.

There are numerous other lookups for yota-related domains from the Trump network. In aggregate, these include:

Other related network lookups from Spectrum and Central Park West networks are listed in Tables 3 and 4.

Speculation: Given the other connections between Spectrum, Trump's networks, and Alfa Bank, it may be that these lookups come from a common set of devices.

Table 4: Central Park West Network Yota-Related Lookups

counts	qname
2	www.yota.ru
1	yota.ru
1	51b2963ac72449e5966c6ec740974328.yota.ru

Table 5: Trump Network Resolutions

counts	qname
6321	sipper.ru
3926	havermarkt.nl
2563	lolopros.com
1916	mx5.cdcservices.com
1248	conferencehiit.com
1026	contact-client2.com
901	mx2.cdcservices.com
881	mx6.cdcservices.com
749	service.govdelivery.com
749	flooringsolutionsinc.com
581	docusign.net

3 Other Russian-Related Resolutions

Traffic from the Trump networks also show large numbers of resolutions of sipper.ru, an opaque site that appears to be a VoIP-related site. The domain does not appear to resolve, yet a small number of hosts globally continue to be seen requesting it. Trump Tower is among the few hosts in the world where frequent and repetitive requests for sipper.ru were observed. It is possible that with the right VPN connection, a particular piece of equipment is able to reach the sipper.ru resource which could be private.

So far as public records of the old sipper.ru site, webarchive.org shows 6 minimalist captures between 21 May 2013 - Aug 1 2015. Passive DNS indications suggest expiration in 2014.

The site was one of the most actively queried hosts on the Trump Tower network - for a short time including November 2016. For comparison against other non-Russian traffuc, Table 5 shows counts of the top hosts resolved by Trump networks. Most are related to real-estate and marketing. The domain sipper.ru tops the list.

Speculation: The sipper.ru domain could be related to the voice operation of a Yota device.

4 Conclusions

There are Russian-related aspects to the network traffic observed from Trump Tower. First, hostnames resolved by the organization strongly suggest the presence of a YotaPhone or similar Yota-created network device. Such devices are very rare on the US networks and are more commonly found in Russia. Second, some hostnames resolved by the Trump network appear to be SIP/VoIP-related, and located in Russia. These lookups are large, relative even to the real-estate and marketing related domains one normally expects to see from the Trump network.

References

[1] Steve Costello. Us yotaphone 2 debut dropped. https://www.mobileworldlive.com/devices/news-devices/us-yotaphone-2-debut-dropped/, August 2015.

[2] Jennifer Lynn. Yota's latest sales numbers. http://www.droidreport.com/yotas-latest-sales-numbers-7890, March 2014.