TO TALK OF MANY THINGS: OF VANDALS, AND CUTS, AND CABLES, AND PINGS

The time has come,' the Walrus said,
To talk of many things:
Of shoes — and ships — and sealing-wax —
Of cabbages — and kings —
And why the sea is boiling hot —
And whether pigs have wings.'

(Excerpt, Lewis Carroll's The Walrus and the Carpenter)

Here's an open information security topic worth examining more closely: the recent *vandalization* of yet another fiber optic cable on the west coast.

A total of eleven cuts have been made since last July on fiber optic cables in the greater San Francisco/Oakland area. The most recent cut occurred on June 30th. The FBI had already asked the public for help with information about the first ten cuts, made in these general locations at the time and date indicated here:

> 1) July 6, 2014, 9:44 p.m. near 7th St. and Grayson St. in Berkeley
> 2) July 6, 2014, 11:39 p.m. near Niles Canyon Blvd. and Mission Blvd. in Fremont
> 3) July 7, 2014, 12:24 a.m. near Jones Road and Iron Horse Trail in Walnut Creek
> 4) July 7, 2014, 12:51 a.m. near Niles Canyon Blvd. and Alameda Creek in Fremont
> 5) July 7, 2014, 2:13 a.m. near Stockton Ave. and University Ave. in San Jose
>
> _____
>
> 6) February 24, 2015, 11:30 p.m. near Niles Canyon Blvd. and Mission Blvd. in Fremont
> 7) February 24, 2015 11:30 p.m. near Niles Canyon Blvd. and Alameda Creek in Fremont
>
> _____
>
> 8) June 8, 2015, 11:00 p.m. near Danville

Blvd. and Rudgear Road in Alamo
9) June 8, 2015, 11:40 p.m. near Overacker Ave and Mowry Ave in Fremont

_____

10) June 9, 2015, 1:38 p.m. near Jones Road and Parkside Dr. in Walnut Creek

The FBI presented these first ten cuts as a single, undivided list. After looking at the dates and times, one can see these cuts may have occurred not as discrete events, but as three separate clusters of cuts. The first cluster occurred within a five-hour span; the second occurred nearly simultaneously at two points; and the third cluster occurred within three hours. The three clusters took place after dark, during the same evening. The tenth cut may be a one-off, or it may be connected to the third cluster as it took place within 14 hours of the eighth and ninth cuts.

The most recent cable cut, occurring this week, did not fit a pattern like the previous ten cuts. Reports indicate the cut was near Livemore – a new location much farther to the south and east in comparison, and only one cut reported rather than two or more.

Is this latest cut an outlier, or
were perpetrators interrupted before they could cut again?

Taking a closer look at the previous cut events, we can see there must have been more than one individual involved in the cuts, and they may have been coordinated.

Cluster 1: The first cluster from one year ago, the evening of July 6-7, took place over a distance of roughly 34 miles. Cuts 1 and 2 are nearly 30 miles apart; by private car they are more than 40 minutes drive or more than an hour and a half apart by public transportation. At two hours between events it's possible the same single perpetrator made these cuts, but only if they traveled by private car and if they knew exactly where to go and what to cut.

Cuts 2 and 3 are also about 30 miles apart, in

the opposite direction. It would be nearly impossible for the same single perpetrator to make these two cuts back-to-back since the time window between the cuts is only 55 minutes. Could a single person make it up out of a manhole from one cut, into a vehicle, drive nearly 40 minutes, park, open and climb into another manhole, then cut a fiber optic cable?

Cuts 3 and 4 were not made by the same single perpetrator. They are roughly 34 miles apart, and the time window between the cuts is less than 30 minutes. To cut-exit-manhole-drive-park-enter-manhole-cut would require traveling at speed that would surely draw attention, even at 12:30-ish in the morning.

Cuts 4 and 5 were made one hour and 24 minutes apart, and the sites are about 20 miles apart. This last cut was the farthest south of the first cluster.

Cluster 2: The second cluster from February this year, consisting of only two cuts happening at what appears to be the same time, suggests there was more than one perpetrator involved. The two cuts occurred at the same time, but within 0.2 miles apart – as if two persons within line of sight cut at the same time. The cuts also occurred near or at two of the previous locations from the first cluster.

Cluster 3: Cuts 8 and 9 occurred 40 minutes apart, yet the sites are roughly 30 miles apart – too far once again for a single perpetrator. Both happened within the hour before midnight local time.

The tenth cut may have been related to third cluster, as noted previously – but it broke from the established pattern. The first nine cuts all occurred after 9:00 p.m. but before 3:00 a.m. local time. The tenth occurred at 1:38 p.m., in broad daylight.

Cut 11, the most recent on June 30th shared this same attribute. It happened some time between 4:20 a.m. and 7:45 a.m. local time (14:45 UTC), near Livermore, CA, to the east of the previous

ten cuts.

Were the same so-called vandals at work for all eleven cuts? If so, were they getting cocky, having not been caught on nine earlier occasions?

Or were they getting desperate?

The implication, assuming desperation, is that these were not the acts of vandals, but a focused effort dedicated to network disruption?

Or perhaps not disruption with intent to halt or disturb, but disruption to map network response and content movement?

What might these vandals have been looking for, as they cut at one end of an area across the bay from Palo Alto and Mountainview across to an area east of Silicon Valley?

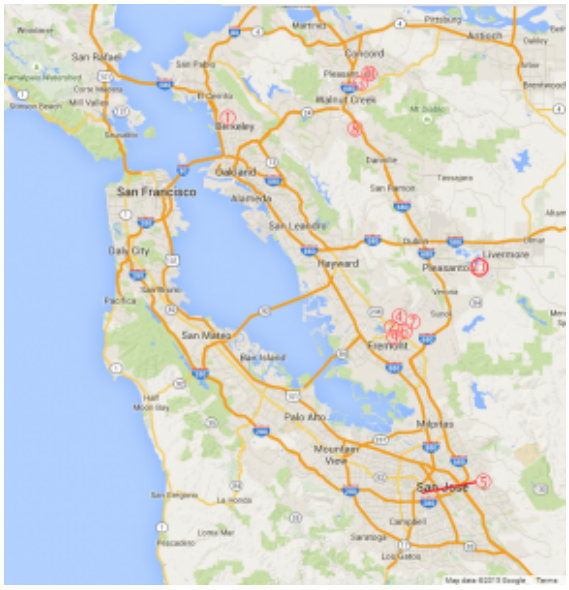
Did they finally learn something when Microsoft issued a formal status notice regarding disruption of its Azure cloud services – perhaps which fiber served the Azure data farm?

> *6/30*
> *Network Infrastructure – West US, South Central US – Advisory*
>
> *From approximately 14:45 UTC to 21:45 on 30 Jun, 2015 UTC customers may have experienced intermittent connectivity issues to Azure services deployed in West US and South Central US. Root cause for this issue is attributed to a fiber cuts in the Western US Region. This incident has now been mitigated.*

Or were they looking for fiber optics serving the Lawrence Livermore National Laboratory, home to other data farms and a number of sensitive research projects?

Or were they looking for the fiber running out of San Francisco, serving headquarters of businesses headquartered in the city like Wells Fargo?

UPDATE — 5:10 PM EDT — Here's the graphic as promised, mapping the approximate location of cuts per the FBI's list. The 11th cut is arbitrarily parked near Livermore as more specific site information was not provided. Cuts are labeled in chronological order.



[graphic: via Google Maps]