TREASURE MAP: IT'S ABOUT LOCATION, NOT GOLD

Der Spiegel and The Intercept published collaborative reporting this weekend on another Snowden document – this one referring to a National Security Agency program named TREASURE MAP.

The most chilling part of this reporting is a network engineer's reaction (see here on video) when he realizes he is marked or targeted as a subject of observation. He's assured it's not personal, it's about the work he does – but his reaction still telegraphs stress. An intelligence agency can get to him, has gotten to him; he's touchable.

The truth is that almost any of us who follow national security, cyber warfare, or information technology are potential subjects depending on our work or play.

The metadata we generate is only part of the observation process; it provides information about our individual patterns of behavior, but may not actually disclose where we are.

TREASURE MAP goes further, by providing the layout of the network on which any of us are generating metadata. But there is some other component either within TREASURE MAP, or within a complementary tool, that provides the physical address of any networked electronic device.

The NSA has the ability to track individuals not only by Internet Protocol addresses (IP addresses), but by media access control addresses (MAC addresses), according a recent interview with Snowden by James Bamford in Wired. This little nugget was a throwaway; perhaps readers already assumed this capability has existed, or didn't understand the implications:

> …But Snowden's disenchantment would only grow. It was bad enough when spies were getting bankers drunk to recruit them; now he was learning about targeted killings and mass surveillance, all piped into monitors at the NSA facilities around the world. Snowden would watch as military and CIA drones silently turned people into body parts. And he would also begin to appreciate the enormous scope of the NSA's surveillance capabilities, an ability to map the movement of everyone in a city by **monitoring their MAC address**, a unique identifier emitted by every cell phone, computer, and other electronic device.

[*emphasis added*]

In simple terms, IP addresses are like phone numbers – they are assigned. They can be static; a printer on a business network, for example, may be assigned a static address to assure it is always available to accept print orders at a stationary location. IP addresses may also be dynamic; if there's an ongoing change in users on a network, allowing them to use a temporary address works best. Think of visits to your local coffee shop where customers use WiFi as an example. When they leave the premise, their IP address will soon revert to the pool available on the WiFi router.

But MAC addresses are physical attributes, like a house number and street name. They are assigned to the network interface card (NIC) inside electronic devices by their manufacturer. The range of addresses used indicate the maker and are registered to that firm. Any device that attaches to a network, from server at one end to cellphones at the other, has a MAC address. Devices with more than one NIC will have a MAC address for each NIC.

(Note that some cellphones may have an International Mobile Station Equipment

Identity (IMEI number) or Mobile Equipment Identifier (MEID) as well as a MAC address if they attach to both wireless and WiFi networks. IMEI/MEID works much like a MAC address, assigned by the manufacturer to a handset, but not to a subscriber identity module (SIM card) which can be swapped out in a handset.)

MAC addresses and IP addresses do not always coincide, the first being physical and the later being virtual. They cannot be used reliably to identify an individual all the time and can be foiled as a tracking tool. Users can swap phone network cards and still grab the same IP address they had been using. Spoofing – substituting a fake alternative address – is possible, to subvert tracking users. In the case of cellphones, "burner" disposable phones tossed after limited use detach both addresses from the user.

In spite of the ability to thwart tracking, the implementation of applications like TREASURE MAP ahead of the public's awareness suggests the entire network, physical and virtual, has been laid out. The NSA can find an overwhelming majority of users' physical location, and gradually fill in the rest with a systematic match of behavior patterns culled from metadata, matched against MAC addresses.

We know there have been other attempts to gather information about the internet. Malware created by nation-state entities like Duqu and Flame, relatives of cyber weapon Stuxnet, have intelligence gathering components "phoning home" information about a wide swath of infected devices.

But TREASURE MAP and its affiliated mapping application(s) may be far more effective and informative. The application only needs to target key nodes like ISPs on the internet, as well as those persons most likely to control those nodes. Once a particular IP address' behavior pattern attributed to a specific individual or group has been associated with a particular MAC address, it is relatively easy to

identify that individual or groups physical location. The potential applications are alarming.

Imagine a tiny processor chip equipped with both WiFi network capability and a MAC address, attached to an oblivious target. Imagine the chip transmitting the target's every word and move to a remote observer, without ever giving away its presence.

Imagine a drone targeting that same chip when it pings a network – or perhaps pings from two different chips over a distance, allowing an accurate calculation about the length of time required to transmit volatile information.

No need for Star Wars when the same capabilities can be achieved closer to the earth's surface.

There are links to space, however; the reach of the map to satellites from ISPs to end users is worth additional consideration. The recent failure rate across satellite launches and operations gives pause, in particular among Russian communications and navigation satellites. These malfunctions and breakdowns range from launch setbacks to GLONASS' 12-hour outage. Given the frequency of failures, one might wonder whether network-related systems affiliated with these Russian programs been affected by malware or other interference intended to obstruct similar network mapping capability.

Conflicting information regarding disposition of satellites does not help. Source in the US reported a Russian imaging reconnaissance satellite burned up over North America 03-SEP, while Russia maintains the same satellite is still in orbit. GLONASS' outage in particular has been attributed to a software bug, but outage beginning at the top of the hour on 01-APR looks less like a bug than not. When added to a growing body of failures, one can't help but wonder if this is all purely coincidental, or if much less benign forces are at work to prevent satellite connections to networks.

We'll likely never know if there are links between the implementation of NSA's network mapping tools and specific satellite failures. But we do know based on Der Spiegel's and The Intercept's reporting that identifying and targeting users through a satellite-relayed network by way of TREASURE MAP is possible.

Perhaps there really is gold where TREASURE MAP marks the spot. It might inform its users the fastest route to send trading information ahead of the rest of the market. It might point to the right subject of obstruction to prevent or launch economic havoc.

Imagine executing an "immaculate" trade in one country's market, milliseconds before a key victim hits the ground in another.