REAGAN? NO, REGIN — YET ANOTHER [GCHQ] INTELLIGENCE MALWARE

Recently, computer security firm Symantec reported discovery of another intelligence-gathering malware, dubbing it "Regin."

What's particularly interesting about this malware is its targets:

- It infected computers in Afghanistan, Austria, Belgium, India, Iran, Ireland, Mexico, Pakistan, Russia, Saudia Arabia;
- At 48% of total infections, the largest group of targets were private individuals and small businesses.

Please do read Symantec's blog post and its technical paper on Regin to understand how it works as well as its targets. Many news outlets either do not understand malware and cybersecurity, or they get facts wrong whenever major malware attacks are reported. Symantec's revelation about Regin is no different in this respect.

Independent.ie offers a particularly exceptional example distorting Symantec's report, claiming "Ireland is one of the countries worst hit globally by a dangerous new computer virus that spies on governments and companies, according to a leading technology firm."

If by "worst hit," they mean among the top four countries targeted by this malware? Sure. But only 9% of the infections affected Irish-based computers, versus 28% of infections aimed at Russian machines, and 24% affecting Saudi

machines. The Independent.ie's piece reads like clickbait hyperbole, or fearmongering, take your pick.

What wasn't addressed by the Independent.ie and numerous other outlets, including those covering the tech sector are some fundamental questions:

- What assets or activities might the targeted countries have in common that would make them targets of a single intelligence operation organized by one or more nation-states?
- What are so many private individuals and small businesses targeted by this malware, in contrast to other malware-based intelligence-collection operations seen to date?

The Guardian came closest to examining these issues, having interviewed researchers at computer security firm F-Secure to ask the origins of the malware. As of 24-NOV-2014, the firm's Mikko Hypponen speculated that the US, UK, and/or Israel were behind Regin's development and deployment.

As of the video embedded above, Hypponen firmly says the UK's intelligence entity GCHQ is behind Regin, in particular the malware's invasion of a Belgian telecom network (see video at 07:20).

It's surprising how many international groups these ten Regin-targeted countries have been members of at the same time, including the IAEA, IBRD (World Bank), ICAO, IDA, IFRCS, IFC (except for Russia), IFAD (except for Russia), ILO, IMO (except Afghanistan), IMF, ISO (except Afghanistan), ICRM, ITU, INTELSAT, UNESCO, UPU, WHO, WMO. But membership in these entities

doesn’t seem to jibe with the malware’s concentration on private individuals and small business.

Or does it? Let’s not rule out the possibility that “small business” may refer to entities organized as intelligence fronts.

The international entities affiliated with business and finance are also of interest, given what we know about the TREASURE MAP program, and about the recent breach of JPMorgan Chase’s 76 million accounts which surely include overseas clients located in those ten Regin-targeted countries.

Given Hypponen’s statement about the UK’s role in Regin before a crowd in in Brussels, looking at ties between Belgium and Saudi Arabia are particularly interesting. Belgian royalty – specifically the recently deceased Queen Fabiola, of Spanish birth – had avoided trips to Saudi Arabia because of Salafism. But tax treaties regarding double taxation between the two countries have surely encouraged business ties through requirements of “bonafide business activity” in their states, further manifest in the Belgian trade mission documentation circa 2009 (PDF).

And Regin’s development and deployment also synced with the period of time during which Microsoft acquired Nokia mobile devices from its parent firm. Nokia provides network to Belgacom, one of the Regin-targeted businesses, as well as the GSM-Railway, within Belgium and without. Finding a backdoor into the devices during the acquisition process, along with Belgian network providers, would reach much, much farther than Belgium.

Of course a similar analysis of relationships between the remaining eight Regin-targeted countries is warranted. But a superficial glance at the origins of the malware, and two of the targets tells us a lot – the rationale behind Regin’s use likely has much more to do with asymmetric warfare than terrorism or traditional

warfare, as seen in previous revelations about NSA spying on Petrobras and other businesses, including France’s oil company Total SA.