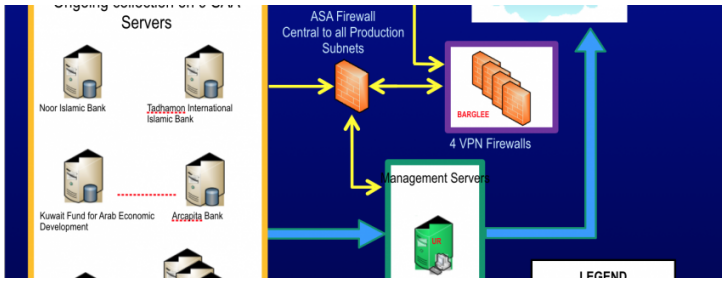
NSA CONTINUED DOUBLE DIPPING AT SWIFT EVEN AFTER IT WAS EXPOSED



One of the most contentious Snowden revelations — first reported on September 8, 2013 by Globo and then repeated a week later by Der Spiegel — was that NSA's Tailored Operations group was hacking SWIFT, the international financial transfer messaging system. It was contentious because when the servers moved to Europe, the US and EU negotiated access for the US, access with protections for Europeans that happened to be oversold.

Shadowbrokers just released its second set of NSA files in a week. This set includes far more interesting documents than the batch released last week. Most significantly, it includes details on NSA's thorough pawning of SWIFT. Whereas the SWIFT files from Snowden, which were never released publicly, seemed to date from 2011, the most recent files released today, including one dated October 17, 2013, appear to date to a month *after* the first public Snowden reports that NSA had targeted SWIFT. In addition, it includes files showing NSA targeting a ~~SWIFT~~ EastNets engineer in Belgium.

A number of people have been arguing that the mostly Middle Eastern financial institutions that seem to be the focus here — things like the Al Quds Bank for Development and Investment — are legitimate intelligence targets. And they are, within the framework of NSA's spying in the US. But that ignores that the US had an

agreement in place about what legitimate targets were (which, according to MEPs who tried to oversee the agreement, were violated anyway). Also, a number of our Arab allies may not be too happy to see their own banks targeted.

Both last week's release and this week's cite Trump's suddenly volatile foreign policy. "Maybe if all suviving WWIII theshadowbrokers be seeing you next week." By releasing files that remind Europe that the US continued to flout multilateral negotiations, SB may be trying to make continued adventures more difficult for Trump.

Update: Security researcher Matt Suiche did a more detailed post on how much this release endangers SWIFT.

Update: Shadow Brokers has long made a show of asking for Bitcoin for all this. But these SWIFT files alone (to say nothing of what appear to be multiple Windows 0days in this release) would have been at least as valuable.

Even more interesting, remember that the US threatened to kick Russia out of SWIFT in 2014, which led Russia to build a redundant system in case it were ejected from the cooperative. Even the Trump Administration has floated making sanctions more stringent. If Russia ever were targeted in such a way, it seems these files would be invaluable. And yet they got leaked, for free. To my mind that's one of the best pieces of evidence yet that Shadow Brokers is not Russian.

Update: EastNets, the primary target in the SWIFT files, issued this statement:

> ***No credibility to the online claim of a compromise of EastNets customer information on its SWIFT service***

> ***bureau***
>
> *The reports of an alleged hacker-compromised EastNets Service Bureau (ENSB) network is totally false and unfounded. The EastNets Network internal Security Unit has run a complete check of its servers and found no hacker compromise or any vulnerabilities.*
> *The EastNets Service Bureau runs on a separate secure network that cannot be accessed over the public networks. The photos shown on twitter, claiming compromised information, is about pages that are outdated and obsolete, generated on a low-level internal server that is retired since 2013.*
> *“While we cannot ascertain the information that has been published, we can confirm that no EastNets customer data has been compromised in any way, EastNets continues to guarantee the complete safety and security of its customer’s data with the highest levels of protection from its SWIFT certified Service bureau”*
> *Hazem Mulhim, CEO and founder EastNets.*

Note what the statement is, however: a denial of *current* compromise. It says it retired the server in question down in 2013, which is the date of these files. But that might also mean they reviewed their files after the Snowden-related disclosures and responded by revamping their security.