NSA, LAZARUS, AND ODINAFF

Reuters has a report that SWIFT — the international financial transfer messaging system — has been hacked again, what it describes as the second effort to steal big money by hacking the system.

> Cyber-security firm Symantec Corp said on Tuesday that a second hacking group has sought to rob banks using fraudulent SWIFT messages, the same approach that yielded $81 million in the high-profile February attack on Bangladesh's central bank.
>
> Symantec said that a group dubbed Odinaff has infected 10 to 20 organizations with malware that can be used to hide fraudulent transfer requests made over SWIFT, the messaging system that is a lynchpin of the global financial system.

But it should say the *third* hack. As the Snowden documents revealed, NSA was double dipping at SWIFT in the 2010 to 2011 timeframe, though to steal information, not money.

What's interesting about this latest hack, though, is it targets the US and countries closely aligned with it, though it appears to be a criminal organization not a state.

> Symantec said that most Odinaff attacks occurred in the United States, Hong Kong, Australia, the United Kingdom and Ukraine.

The Reuters report also notes that Symantec thinks the Sony hack was done by a group it calls Lazarus, which may not be the same as North Korea.

As with the Yahoo scan ordered last year — which

effectively appears to have hacked all Yahoo’s users — it makes sense to think of US nation-state hacks and criminal or foreign adversary ones in the same breath. Not only might an NSA hack expose methods others might use, but with an entity like SWIFT, there’s no reason to privilege US hacking over others.