LATEST STUXNET INCARNATION RESEMBLES ALLEGED PROJECT OF MURDERED GCHQ OFFICER

Kaspersky Labs has found a new incarnation of StuxNet malware, which they've called Gauss. As Wired summarizes, the malware is focused geographically on Lebanon and has targeted banks.

> A newly uncovered espionage tool, apparently designed by the same people behind the state-sponsored Flame malware that infiltrated machines in Iran, has been found infecting systems in other countries in the Middle East, according to researchers.
>
> The malware, which steals system information but also has a mysterious payload that could be destructive against critical infrastructure, has been found infecting at least 2,500 machines, most of them in Lebanon, according to Russia-based security firm Kaspersky Lab, which discovered the malware in June and published an extensive analysis of it on Thursday.
>
> The spyware, dubbed Gauss after a name found in one of its main files, also has a module that targets bank accounts in order to capture login credentials. The malware targets accounts at several banks in Lebanon, including the Bank of Beirut, EBLF, BlomBank, ByblosBank, FransaBank and Credit Libanais. It also targets customers of Citibank and PayPal.

I find that interesting for a number of reasons.

First, every time banks have squawked about our government's access of SWIFT to track terrorist financing, the spooks have said if they don't use SWIFT they'll access the information via other means; it appears this malware may be just that. And the focus on Lebanon fits, too, given the increasing US claims about Hezbollah money laundering in the time since Gauss was launched. I'm even struck by the coincidence of Gauss' creation last summer around the same time that John Ashcroft was going through the Lebanese Canadian Bank to find any evidence of money laundering rather than—as happens with US and European banks—crafting a settlement. I would imagine how that kind of access to a bank would give you some hints about how to build malware.

But the other thing the malware made me think of, almost immediately, was the (I thought) bogus excuse some British spooks offered last summer to explain the murder of Gareth Williams, the GCHQ officer—who had worked closely with NSA—who was found dead in a gym bag in his flat in August 2010. Williams was murdered, the Daily Mail claimed, because he was working on a way to track the money laundering of the Russian mob.

> The MI6 agent found dead in a holdall at his London flat was working on secret technology to target Russian criminal gangs who launder stolen money through Britain.
>
> [snip]
>
> But now security sources say Williams, who was on secondment to MI6 from the Government's eavesdropping centre GCHQ, was working on equipment that tracked the flow of money from Russia to Europe.
>
> The technology enabled MI6 agents to follow the money trails from bank accounts in Russia to criminal European gangs via internet and wire transfers, said the source.
>
> 'He was involved in a very sensitive project with the highest security

> clearance. He was not an agent doing surveillance, but was very much part of the team, working on the technology side, devising stuff like software,' said the source.
>
> He added: 'A knock-on effect of this technology would be that a number of criminal groups in Russia would be disrupted.
>
> 'Some of these powerful criminal networks have links with, and employ, former KGB agents who can track down people like Williams.'

Frankly, I always thought that explanation was bogus—I suggested that the Brits could just partner with the US to access such data via SWIFT. And whatever it means, I haven't seen such an explanation since.

But I do find it rather interesting that one of the most prominent unsolved murders of a spook was blamed—at around the time the StuxNet people were working on Gauss—on a plan to track money laundering.