TURNS OUT THEIR REASSURANCES WERE TOO SWIFT

When I first wrote about the $81 million bank heist of Bangladesh, I noted that the hack appeared to target SWIFT, the international payment transfer system, even while SWIFT itself was giving us reassurances that they had not been breached.

> While SWIFT insists it has not been breached, the hackers used a name making it clear they were targeting the SWIFT system.
>
> > On Jan. 29, attackers installed “SysMon in SWIFTLIVE” in what was interpreted as reconnaissance activity, and appeared to operate exclusively with “local administrator accounts.”
>
> SWIFT is sending out a security advisors to its members, advising them to shore up their local operating environments.

Three days ago, Reuters issued a report that seemed to reiterate the centrality of the negligence of Bangladesh bank for the hack, which was relying on a second-hand, $10 router for its SWIFT set-up.

> Bangladesh’s central bank was vulnerable to hackers because it did not have a firewall and used second-hand, $10 switches to network computers connected to the SWIFT global payment network, an investigator into one of the world’s biggest cyber heists said.
>
> The shortcomings made it easier for hackers to break into the Bangladesh Bank system earlier this year and

> attempt to siphon off nearly $1 billion using the bank's SWIFT credentials, said Mohammad Shah Alam, head of the Forensic Training Institute of the Bangladesh police's criminal investigation department.
>
> "It could be difficult to hack if there was a firewall," Alam said in an interview.
>
> The lack of sophisticated switches, which can cost several hundred dollars or more, also means it is difficult for investigators to figure out what the hackers did and where they might have been based, he added.

Though local cops cast some of the blame on SWIFT.

> The police believe that both the bank and SWIFT should take the blame for the oversight, Alam said in an interview.
>
> "It was their responsibility to point it out but we haven't found any evidence that they advised before the heist," he said, referring to SWIFT.
>
> A spokeswoman for Brussels-based SWIFT declined comment.

Which might have been the tip-off that this was coming…

> The attackers who stole $81 million from the Bangladesh central bank probably hacked into software from the SWIFT financial platform that is at the heart of the global financial system, said security researchers at British defense contractor BAE Systems.
>
> SWIFT, a cooperative owned by 3,000 financial institutions, confirmed to Reuters that it was aware of malware targeting its client software. Its

> spokeswoman Natasha Deteran said SWIFT would release on Monday a software update to thwart the malware, along with a special warning for financial institutions to scrutinize their security procedures.
>
> [snip]
>
> Deteran told Reuters on Sunday that it was issuing the software update "to assist customers in enhancing their security and to spot inconsistencies in their local database records." She said "the malware has no impact on SWIFT's network or core messaging services."
>
> The software update and warning from Brussels-based Swift, or the Society for Worldwide Interbank Financial Telecommunication, come after researchers at BAE (BAES.L), which has a large cyber-security business, told Reuters they believe they discovered malware that the Bangladesh Bank attackers used to manipulate SWIFT client software known as Alliance Access.

One wonders whether SWIFT would have released a public statement if not for BAE's imminent public report on this?

Again, NSA managed to hack into SWIFT (double-dipping on the sanctioned access they got through an agreement with the EU) via printer traffic at member banks.

> NSA's TAO hackers hacked into SWIFT (even though the US has access to SWIFT to obtain counterterrorism information via an intelligence agreement anyway), apparently by accessing printer traffic from what sounds like member banks.
>
> > The NSA's Tracfin data bank also contained data from the Brussels-based Society for

> Worldwide Interbank Financial Telecommunication (SWIFT), a network used by thousands of banks to send transaction information securely. SWIFT was named as a "target," according to the documents, which also show that the NSA spied on the organization on several levels, involving, among others, the agency's "tailored access operations" division. One of the ways the agency accessed the data included reading "SWIFT printer traffic from numerous banks," the documents show.

So SWIFT had warning there were vulnerabilities in its local printer system (though it's not clear this is the same vulnerability the Bangladesh thieves used).

You'd think SWIFT would have made some effort when that became public to shore up vulnerabilities in the global finance system. Instead, they left themselves vulnerable to a $10 router.