HOW MUCH DOES KEITH ALEXANDER'S PATENTED SOLUTION FOR CREATING FEAR DEPEND ON CISA?

Keith Alexander has attempted to explain his million dollar salary demands for cyber consulting to Shane Harris. This story doesn't necessary hang together any better than his claims about NSA's spying.

Alexander is worth a million a month, he says (though he already dropped his price to $600K) because he has a unique approach to detecting persistent threats that he plans to patent.

> The answer, Alexander said in an interview Monday, is a new technology, based on a patented and "unique" approach to detecting malicious hackers and cyber-intruders that the retired Army general said he has invented, along with his business partners at IronNet Cybersecurity Inc., the company he co-founded after leaving the government and retiring from military service in March.

Alexander developed the technologies behind these patents — which Alexander says would address precisely the kind of attacks he facetiously argues have carried out the greatest transfer of wealth in history, the ones attacking the US — in his spare time.

> A source familiarly [sic] with Alexander's situation, who asked not to be identified, said that the former director developed this new technology on his private time, and that he addressed any potential infractions before deciding to seek his patents.

To which Harris asked the obvious question: if this solution is so great, then why not implement it while he was still in government? Why not save America from that greatest transfer of wealth in history?

Alexander then added that his solution relies on behavioral analysis one of his partners contributed.

> Alexander said that his new approach is different than anything that's been done before because it uses "behavioral models" to help predict what a hacker is likely to do.
>
> [snip]
>
> Alexander said the key insight about using behavior models came from one of his business partners, whom he also declined to name, and that it takes an approach that the government hadn't considered. It's these methods that Alexander said he will seek to patent.

Perhaps the best (anonymous) quote Harris includes in his story is a "former national security official with decades of experience in security technology" who says such behavioral models are highly speculative and have never before worked.

So it's possible that Keith Alexander is simply going to sell his new approach to a bunch of chumps who have gotten rich trading off of algorithms — proof behavioral models "work" even if they don't work! — and therefore believe they will work to find persistent threats.

The guy who couldn't find Edward Snowden absconding with thousands of files and his friends the big banks are going to start policing their networks by using algos to find suspicious behavior.

Harris sort of alludes to one problem with this scheme. Alexander used his perch at DIRNSA to create this market. As Harris points out, that's

in part because Wiper — a variant of the StuxNet attack developed under Alexander's tenure — is what the banks are so afraid of.

> That will come as a supreme irony to many computer security experts, who say that Wiper is a cousin of the notorious Stuxnet virus, which was built by the NSA — while Alexander was in charge — in cooperation with Israeli intelligence.

That is, Alexander will get rich helping banks defeat the weapons he released in the first place.

More generally, too, this fear exists because Alexander sowed it. The banks are responding to the intelligence claims Alexander has been making for years, whether or not a real threat exists behind it (and whether not resilience would be a better defense than Alexander's algos).

One more thing: as far as we know, in addition to inventing this purportedly new technology in his free time, Alexander was consulting with his partners — which as far as we know include Promontory Financial Group and Chertoff — while he was DIRNSA. So it's not just the underlying technology, but the discussions of partnership, that likely derive from Alexander's time at DIRNSA.

And that seems to be the fourth part of Alexander's magic sauce (in addition to the tech developed on the government dime, his ability to sow fear, and partnerships laid out while still in the private sector). After all, with Alexander out of his NSA, where will he and his profitable partners get the data they need to model threats? How much of this model will depend on the Cyber Information sharing plan that Alexander has demanded for years? How much will Alexander's privatized solutions to the problem he couldn't solve at NSA depend on access to all the information the government

has, along with immunity?

To what degree is CISA about making Keith Alexander rich?