WHY DID TOM BOSSERT CLAIM WANNACRY WAS SPREAD VIA PHISHING?

Writing this post made me look more closely at what Trump's Homeland Security Czar Tom Bossert said in a briefing on WannaCry on Monday, May 15.

He claimed, having just gotten off the phone with his British counterpart and in spite of evidence to the contrary, that there had been minimal disruption to care in Britain's DHS.

> The UK National Health Care Service announced 48 of its organizations were affected, and that resulted in inaccessible computers and telephone service, but an extremely minimal effect on disruption to patient care.
>
> [snip]
>
> And from the British perspective, I thought it was important to pass along from them two points – one, that they thought it was an extremely small number of patients that might have been inconvenienced and not necessarily a disruption to their clinical care, as opposed to their administrative processes. And two, that they felt that some of those reports might have been misstated or overblown given how they had gotten themselves into a position of patching.

Of course, this may be an issue in the upcoming election, so I can see why Theresa May's government might want to downplay any impact on patient care, especially since the Tories have long been ignoring IT problems at DHS.

He dodged a follow-up question about whether

there might be more tools in the Shadow Brokers haul that would lead to similar attacks in the future, by pointing to our Vulnerabilities Equities Process.

> Q I guess a shorter way to put it would be is there more out there that you're worried about that would lead to more attacks in the future?
>
> MR. BOSSERT: I actually think that the United States, more than probably any other country, is extremely careful with their processes about how they handle any vulnerabilities that they're aware of. That's something that we do when we know of the vulnerability, not when we know we lost a vulnerability. I think that's a key distinction between us and other countries — and other adversaries that don't provide any such consideration to their people, customers, or industry.

Obviously, the VEP did not prevent this attack. More importantly, someone in government really needs to start answering what the NSA and CIA (and FBI, if it ever happens) do when their hacking tools get stolen, an issue which Bossert totally ignored.

But I'm most interested in something Bossert said during the original exchange on NSA's role in all this.

> Q So this is one episode of malware or ransomware. Do you know from the documents and the cyber hacking tools that were stolen from NSA if there are potentially more out there?
>
> MR. BOSSERT: So there's a little bit of a double question there. Part of that has to do with the underlying vulnerability exploit here used. I think if I could, I'd rather, instead of directly answering that, and can't speak to how we do or don't do our business as

> a government in that regard, I'd like to instead point out that this was a vulnerability exploit as one part of a much larger tool that was put together by the culpable parties and not by the U.S. government.
>
> So this was not a tool developed by the NSA to hold ransom data. This was a tool developed by culpable parties, potentially criminals of foreign nation states, **that was put together in such a way so to deliver it with phishing emails**, put it into embedded documents, and cause an infection in encryption and locking. [my emphasis]

Three days into the WannaCry attack, having spent the weekend consulting with DHS and NSA, Bossert asserted that WannaCry was spread via phishing.

That is a claim that was reported in the press. But even by Monday, I was seeing security researchers persistently question the claim. Over and over they kept looking and failing to find any infections via phishing. And I had already seen several demonstrations showing it didn't spread via phishing.

Now, Bossert is one of the grown-ups in the Trump Administration. His appointment – and the cybersecurity policy continuity with Obama's policy – was regarded with relief when it was made, as laid out in this Wired profile.

> "People that follow cybersecurity issues will be happy that Tom is involved in those discussions as one of the reasoned voices," Healey says.
>
> "Frankly, he's an unusual figure in this White House. He's not a Bannon. He's not even a Priebus," says one former senior Obama administration official who asked to remain unnamed, contrasting Bossert with Trump's top advisers Stephen Bannon and Reince Priebus. "He has a lot of

> credibility. He's very straightforward and level-headed."

And (as the rest of the profile makes clear) he does know cybersecurity.

So I'm wondering why Bossert was stating that this attack spread by phishing at a time when open source investigation had already largely undermined that hasty claim.

There are at least three possibilities. Perhaps Bossert simply mistated here, accidentally blaming the vector we've grown used to blaming. Possibly (though this would be shocking) the best SIGINT agency in the world still hadn't figured out what a bunch of people on Twitter already had.

Or, perhaps there were some phished infections, which quickly got flooded as the infection spread via SMB. Though that's unlikely, because the certainty that it didn't spread via email has only grown since Monday.

So assuming Bossert was, in fact, incorrect when he made this claim, why did have this faulty information?