THE BANKRUPT ATTRIBUTION OF WANNACRY

THE HOUSE
NGTON
Japan
Honda plant halted car production for a day
WANNACRY RANSOMWARE ATTACK

I've been puzzling through this briefing, purportedly attributing the WannaCry hack to North Korea, which followed last night's Axis of CyberEvil op-ed (here's the text). The presser was … perhaps even more puzzling than the Axis of CyberEvil op-ed.

Unlike the op-ed, Homeland Security Czar Tom Bossert provided hints about how the government came to attribute this attack.

Bossert makes much of the fact that the Five Eyes plus Japan all agree on this.

> We do so with evidence, and we do so with partners.
>
> Other governments and private companies agree. The United Kingdom, Australia, Canada, New Zealand, and Japan have seen our analysis, and they join us in denouncing North Korea for WannaCry.

He also points to the Microsoft and (unnamed — because it'd be downright awkward to name Kaspersky in the same briefing where you attack them as a cybersecurity target) security consultant attributions from months ago.

> Commercial partners have also acted. Microsoft traced the attack to cyber affiliates of the North Korean government, and others in the security community have contributed their

> analysis.

Here are the specific things he says about how the US, independent of Microsoft and villains like Kaspersky, made an attribution.

> What we did was, rely on — and some of it I can’t share, unfortunately — technical links to previously identified North Korean cyber tools, tradecraft, operational infrastructure. We had to examine a lot. And we had to put it together in a way that allowed us to make a confident attribution.
>
> [snip]
>
> [I]t’s a little tradecraft, to get to your second question. It’s hard to find that smoking gun, but what we’ve done here is combined a series of behaviors. We’ve got analysts all over the world, but also deep and experienced analysts within our intelligence community that looked at not only the operational infrastructure, but also the tradecraft and the routine and the behaviors that we’ve seen demonstrated in past attacks. And so you have to apply some gumshoe work here, not just some code analysis.

Nevertheless, Bossert alludes to people launching this attack from “keyboards all over the world,” but says because these “intermediaries … had carried out those types of attacks on behalf of the North Korean government in the past,” they were confident in the attribution.

> People operating keyboards all over the world on behalf of a North Korean actor can be launching from places that are not in North Korea. And so that’s one of the challenges behind cyber attribution.

> [snip]
>
> [T]here were actors on their behalf, intermediaries, carrying out this attack, and that they had carried out those types of attacks on behalf of the North Korean government in the past. And that was one of the tradecraft routines that allowed us to reach that conclusion.

Taking credit for stuff the private sector did

In his prewritten statement, Bossert provides on explanation for the timing of all this. One of the reasons the US is attributing the WannaCry attack now — aside from the need to gin up war with North Korea — is that Facebook and Microsoft, “acting on their own initiative last week,” took action last week against North Korean targets.

> We applaud our corporate partners, Microsoft and Facebook especially, for acting on their own initiative last week without any direction by the U.S. government or coordination to disrupt the activities of North Korean hackers. Microsoft acted before the attack in ways that spared many U.S. targets.
>
> Last week, Microsoft and Facebook and other major tech companies acted to disable a number of North Korean cyber exploits and disrupt their operations as the North Koreans were still infecting computers across the globe. They shut down accounts the North Korean regime hackers used to launch attacks and patched systems.

Yet even while acknowledging that Microsoft and Facebook are busy keeping the US safe, he demands that the private sector … keep us safe.

> We call today — I call today, and the President calls today, on the private sector to increase its accountability in the cyber realm by taking actions that deny North Korea and the bad actors the ability to launch reckless and disruptive cyber acts.

Golly how do you think the US avoided damage from the attack based on US tools so well?

Then Bossert invites Assistant Secretary for Cybersecurity and Communications at DHS Jeanette Manfra to explain *not* how the US attributed this attack (the ostensible point of this presser), but how the US magically avoided getting slammed — by an attack based on US tools — as badly as other countries did.

> By midafternoon, I had all of the major Internet service providers either on the phone or on our watch floor sharing information with us about what they were seeing globally and in the United States. We partnered with the Department of Health and Human Services to reach out to hospitals across the country to offer assistance. We engaged with federal CIOs across our government to ensure that our systems were not vulnerable. I asked for assistance from our partners in the IT and cybersecurity industry. And by 9:00 p.m. that night, I had over 30 companies represented on calls, many of whom offered us analytical assistance throughout the weekend.
>
> By working closely with these companies and the FBI throughout that night, we were able to issue a technical alert, publicly, that would assist defenders

> with defeating this malware. We stayed on alert all weekend but were largely able to escape the impacts here in this country that other countries experienced.

Managing to avoid getting slammed by an attack that the US had far more warning of (because it would have recognized and had 96 days to prepare) is proof, Manfra argues, of our preparation to respond to attacks we didn't write the exploit for.

> [T]he WannaCry attack demonstrated our national capability to effectively operate and respond.

Ix-Nay on the AdowBrokers-Shay

Which brings us to the dramatic climax of this entire presser, where Tom Bossert plays dumb about the fact that his this attack exploited an NSA exploit. In his first attempt to deflect this question, Bossert tried to distinguish between vulnerabilities and the exploits NSA wrote for them.

> Q Had they not been able to take advantage of the vulnerabilities that got published in the Shadow Brokers website, do you think that would have made a significant difference in their ability to carry out the attack?
>
> MR. BOSSERT: Yeah. So I think what Dave is alluding to here is that vulnerabilities exist in software. They're not — almost never designed on purpose. Software producers are making a product, and they're selling it for a purpose.

Pretending a vulnerability is the same thing as an exploit, Bossert pointed to the (more visible but still largely the same) Vulnerabilities Exploit Process Trump has instituted.

> When we find vulnerabilities, the United States government, we generally identify them and tell the companies so they can patch them.
>
> In this particular case, I'm fairly proud of that process, so I'd like to elaborate. Under this President's leadership and under the leadership of Rob Joyce, who's serving as my deputy now and the cybersecurity coordinator, we have led the most transparent Vulnerabilities Equities Process in the world.

Hey, by the way, why isn't Rob Joyce at this presser so the person in government best able to protect against cyber attacks can answer questions?

Oh, never mind—let's continue with this VEP thing.

> And what that means is the United States government finds vulnerabilities in software, routinely, and then, at a rate of almost 90 percent, reveals those. They could be useful tools for us to then exploit for our own national security benefit. But instead, what we choose to do is share those back with the companies so that they can patch and increase the collective defense of the country. It's not fair for us to keep those exploits while people sit vulnerable to those totalitarian regimes that are going to bring harm to them.
>
> So, in this particular case, I'm proud of the VEP program. And I'd go one step deeper for you: Those vulnerabilities that we do keep, we keep for very specific purposes so that we can increase our national security. And we use them for very specific purposes only

> tailored to our perceived threats. I think that they're used very carefully. They need to be protected in such a way that we don't leak them out and so that bad people can get them. That has happened, unfortunately, in the past.

Hell! Let's go for broke. Let's turn the risk that someone can steal our toys and set off a global worm into the promise that we'll warn people they've been hacked.

> But one level even deeper. When we do use those vulnerabilities to develop exploits for the purpose of national security for the classified work that we do, we sometimes find evidence of bad behavior. Sometimes it allows us to attribute bad actions. Other times it allows us to privately call — and we're doing this on a regular basis, and we're doing it better and in a more routine fashion as this administration advances — we're able to call targets that aren't subject to big rollouts. We're able to call companies, and we're able to say to them, "We believe that you've been hacked. You need to take immediate action." It works well; we need to get better at doing that. And I think that allows us to save a lot of time and money.

We're not yet broke yet, though! When Bossert again gets asked whether WannaCry was based off a US tool, he tried to argue the only tool involved was the final WannaCry one, not than the underlying NSA exploit.

> Q So you talked about the 90 percent of times when you guys share information back with companies rather than exploit those vulnerabilities. Was this one of the 10 percent that you guys had held onto?

> MR. BOSSERT: So I think there’s a case to be made for the tool that was used here being cobbled together from a number of different sources. But the vulnerability that was exploited — the exploit developed by the culpable party here — is the tool, the bad tool.

This soon descends into full-on Sergeant Schultz.

> I don’t know what they got and where they got it, but they certainly had a number of things cobbled together in a pretty complicated, intentional tool meant to cause harm that they didn’t entirely create themselves.

MalwareTech took a risk doing what he always does [er, did, before the US government kidnapped him] with malware?

Then there’s weird bit — one of those Bossert moments (like when he said WannaCry was spread by phishing) that makes me think he doesn’t know what he’s talking about. When asked if this North Korean attribution changed the government’s intent to prosecute MalwareTech (Marcus Hutchins), Bossert dodged that tricksy question (the answer is, yes, the prosecution is still on track to go to trial next year) but then claimed that Hutchins “took a risk” doing something he has repeatedly said he always does when responding to malware.

> I can’t comment on the ongoing criminal prosecution or judicial proceedings there. But I will note that, to some

> degree, we got lucky. In a lot of ways, in the United States we were well-prepared. So it wasn't luck — it was preparation, it was partnership with private companies, and so forth. But we also had a programmer that was sophisticated, that noticed a glitch in the malware, a kill-switch, and then acted to kill it. He took a risk, it worked, and it caused a lot of benefit. So we'll give him that. Next time, we're not going to get so lucky.

After dodging the issue of why the government is prosecuting the guy whose "luck" Bossert acknowledges saved the world, he has the gall to say — in the very next breath!! — we need to do the kind of information sharing that Hutchins' prosecution disincents.

> So what we're calling on here today is an increased partnership, an increased rapidity in routine speed of sharing information so that we can prevent patient zero from being patient 150.

Whatever you do, don't follow the lack of money

All that was bad enough. But then things really went off the rail when a journalist asked about what one of the poorest countries on earth — a country with a severe exchangeable currency shortage — did with the money obtained in this ransomware attack.

> Q   Tom, the purpose of ransomware is to raise money. So do you have a sense now of exactly how much money the North Koreans raised as a result of this? And do you have any idea what they did with the money? Did it go to fund the nuclear program? Did it go just to the

> regime for its own benefit? Or where did that money go?
>
> MR. BOSSERT: Yeah, it's interesting. There's two conundrums here. First, we don't really know how much money they raised, but they didn't seem to architect it in the way that a smart ransomware architect would do. They didn't want to get a lot of money out of this. If they did, they would have opened computers if you paid. Once word got out that paying didn't unlock your computer, the payment stopped.
>
> And so I think that, in this case, this was a reckless attack and it was meant to cause havoc and destruction. The money was an ancillary side benefit. I don't think they got a lot of it.

Wow. A couple things here. First, of one of the poorest countries in the world, Bossert said with a straight face: "They didn't want to get a lot of money out of this."

He has to do that, because he has just said that, "They've got some smart programmers." So he has to treat the attack, as implemented, as the attack that the perpetrators wanted. That apparently doesn't mean he feels bound to offer some explanation for *why* North Korea would forgo the money that their smart programmers could have earned. Because he never offers that, without which you have zero credible attribution.

Still nuttier, at one level it cannot be true that "we don't know how much money they raised." Later in his presser he claims, "cryptocurrency might be difficult to track" and suggests the government only learned about how little they were making because, "targets seem to have reported to us, by and large, that they mostly didn't pay. … So we were able to track the behavior of the targets in that case."

Um. No. It was very public! We watched

WannaCry’s perps collect $144,000 via the @Actual_ransom account, and we watched the account be cashed out in the immediate wake of the aforementioned MalwareTech arrest (as Hutchins noted, making it look like he had absconded with his Bitcoin rather than gotten arrested by the FBI). That, too, is a detail that Bossert would have needed to address for this to be a marginally credible press conference.

But wait! There’s more! We also know that as soon as WannaCry’s perps publicly cashed out, Shapeshift blacklisted all its known accounts, making it impossible for WannaCry to launder the money, and adding still more transparency to the process. Which means Bossert should know well the answer to the question “how much did North Korea (or whatever perp) make off this?” is, zero. None. Because their money got cut off in the laundering process. (For some reason, Bossert gave Shapeshift zero credit here, which raises further questions I might return to at a later date.) Either attribution includes details about this process or … it’s not credible.

Bossert’s backflips to pretend Trump isn’t treating North Korea differently than Russia

Now, all this is before you get into the gymnastics Bossert performed to pretend that Trump isn’t treating North Korea — against whom this attribution will serve as justification for war — differently than Russia. After being asked about it, Bossert claimed,

> President Trump not only continued the national emergency for cybersecurity, but he did so himself and sanctioned the Russians involved in the hacks of last year.

His effort to conflate last year’s hack-related sanctions with the sanctions imposed by Congress but not fully implemented looked really pathetic.

> Q   Have all the sanctions been implemented?
>
> MR. BOSSERT: This was — yeah, this was the Continuation of the National Emergency with Respect to Significant Malicious Cyber-Enabled Activities. President Trump continued that national emergency, pursuant to the International Emergency Economic Powers Act, to deal with the “unusual and extraordinary threat to the national security, foreign policy, and economy of the United States.”

Pivoting to one of the most important private companies

Immediately after which, perhaps in an act of desperation, Bossert pivoted to Kaspersky, one of the most important security firms in unpacking WannaCry and therefore utterly central to any claim the answer to cyberattacks is to share between the private and public sector. Bossert said *this* to defend the claim that the Trump administration is taking Russian threats seriously.

> Now, look, in addition, if that’s not making people comfortable, this year we acted to remove Kaspersky from all of our federal networks. We did so because having a company that can report back information to the Russian government constituted a risk unacceptable to our federal networks.

And then — in the same press conference where Bossert hailed cooperation, including with private security firms like Kaspersky, he boasted about how “in the spirit of cooperation” the US has gotten “providers, sellers, retail stores” to ban one of the firms that was critical in analyzing and minimizing the WannaCry impact.

> In the spirit of cooperation, which is the second pillar of our strategy — accountability being one, cooperation being the second — we’ve had providers, sellers, retail stores follow suit. And we’ve had other private companies and other foreign governments also follow suit with that action.

In case you’re counting, he has boasted about cooperation in the same breath as speaking of *both* MalwareTech *and* Kaspersky.

Whatever. From this we’re supposed to conclude we should go to war against North Korea and their non-NK keyboarders the world over *and* that the way to defend ourselves against them is to simultaneously demand “cooperation” even while treating two of the most important entities who minimized the threat of WannaCry as outlaws.