Narrative On Recent Supply Chain Cyber Attacks Already Wearing Thin

There is little consistency or credibility in the stories being reported about recent cyber attacks on Colonial Pipeline and JBS. These were attacks on critical parts of the global "supply chain" and great opportunities for fear mongering by the global elite. Meanwhile, calls for more control and surveillance are already on the table. TN Editor

There was a moment of sheer hilarity earlier today when, during a Congressional Hearing, the CEO of Colonial Pipeline Joseph Blount took the merely farcical episode of the Colonial Pipeline ransomware hack – *when, as a reminder, a ragtag band of elite "Russian" hackers somehow managed to penetrate the company's cyberdefenses but was so stupid it left most if not all of the $4.4 million bitcoins it demanded in ransom in an easily traceable address for the FBI to track down and magically confiscate (it is still unclear how the Feds got the private key to access the "hackers" digital wallet) in days if not hours* – and elevated it to a level of sheer ridiculous absurdity when he told Congress that **he didn't consult the FBI before paying the ransom.**

This, pardon the parlance of our times, is complete bullshit: either the

CEO is lying or, worse, he is telling the truth and as some have speculated, *he, the FBI and the "hackers" are all in on this so-called ransomware breach…*

… a scenario which for now is **yet another "conspiracy theory" and which we expect will become proven fact in the usual 6-9 months.**

Yet just a few hours later, the exact same ridiculous narrative meant to achieve just one thing – *tarnish the reputation of bitcoin further to the point where the US has to ban it* – has struck again, and according to the WSJ last week's big hack, that of food processing giant JBS, was also resolved when the company paid $11 million – *in bitcoin of course, because in this day and age one can't simply dump a suitcase full of cash or send a wire transfer to an incognito account* – as ransom to the criminals (*who will naturally soon be unveiled as Russians because of course*) responsible for the cyberattack that halted the company's operations.

Yes, if this story seems identical to that of Colonial Pipeline, up to and almost matching the demanded ransom amount, it's because it is: so barren is the imagination of the administration's narrative writers that they can only regurgitate the same old story over and over.

Naturally, and just like in the Colonial "hack", the ransom payment, in

bitcoin, was made to shield JBS meat plants from further disruption and to limit the potential impact on restaurants, grocery stores and farmers that rely on JBS, said Andre Nogueira, chief executive of Brazilian meat company JBS SA's U.S. division.

"It was very painful to pay the criminals, but we did the right thing for our customers," Nogueira said Wednesday. It remains to be seen if the JDS CEO, like his Colonial colleague, promptly transferred the bitcoin to the ~~FBI's~~ hackers' digital wallet without advising the FBI (first for the simple reason that the FBI already knew the crypto was inbound?)

The latest "shocking" attack on JBS has been part of a wave of bizarre incursions using ransomware, in which companies are hit with demands for multimillion-dollar payments to regain control of their operating systems. Some questions that remain unanswered is how the hell do these multi-billion dollar companies not have the most basic virus/malware protection to prevent some outsider – be it a 13 year old kid living in his mom's basement, some Ukrainian hacker, or the FBI – from getting access to the company's entire infrastructure **and locking out the company itself**. And then, this genius mastermind(s) is so stupid, they have no idea how to cover up their traces and promptly hand over the cash to the Feds.

Even more grotesque is that, as the WSJ notes, the attacks show how hackers have shifted from targeting data-rich companies such as retailers, banks and insurers to essential-service providers such as hospitals, transport operators and food companies. Because apparently instead of spending $29.95 on an anti-virus program, these various companies used the cash to buyback stonk.

According to the WSJ, the FBI last week attributed the JBS attack to REvil, a criminal ransomware gang, which of course comes from Russia, because – again – of course. Nogueira said that JBS and outside firms are conducting forensic analyses of its information-technology systems, and that it isn't yet clear how the attackers accessed JBS's systems.

What is clear is that in just a few days these crack Russian cybercommandos will have a few dozen bitcoins less when the FBI ~~which~~

~~organized the entire farcical affair~~ confiscates it all.

And speaking of farcical, it gets even worse, because unlike the Colonial "hack" where the company lost all control over its infrastructure, in the case of the JBS hack, Nogueira said that the company maintains secondary backups of all its data, which are encrypted. Here things get downright surreal: according to the official narrative, the company brought back operations at its plants using those backup systems, but "JBS's technology experts cautioned the company that there was no guarantee that the hackers wouldn't find another way to strike, and JBS's consultants continued negotiating with the attackers."

So even though the company had regained control, it decided to… pay the hackers?

Read full story here…