WANNACRY ATTRIBUTION: MISSING THE SARCASM TAG

Parts of the security community have decided that Lazarus, a hacking group associated with North Korea, is behind WannaCry, including the global ransomware attack from a few weeks back. That's based on significant reuse of code from earlier Lazarus activities.

But to explain certain aspects of the attack — notably, why Lazarus would become incompetent at ransomware after having been perfectly competent at it in the past — proponents of this theory are adopting some curious theories. For example, this — in Symantec's report on the code reuse — doesn't make any sense at all.

> The small number of Bitcoin wallets used by first version of WannaCry, and its limited spread, indicates that this was not a tool that was shared across cyber crime groups. This provides further evidence that both versions of WannaCry were operated by a single group.

It's effectively the equivalent of saying, "using just three bitcoin wallets doesn't make sense [it doesn't, if your goal is actual ransomware], so we'll just claim that's further proof that there must be few people involved." In interviews, Symantec's technical director has explained away other inconsistencies in this story by hackers working for a brutal dictator with a penchant for executing those who cross them by suggesting they were moonlighting when they blew up Lazarus' ransomware by misdeploying it with Eternal Blue.

> At the same time, flaws in the WannaCry code, its wide spread, and its demands for payment in the electronic bitcoin before files are decrypted suggest that the hackers were not working for North

> Korean government objectives in this case, said Vikram Thakur, Symantec's security response technical director.
>
> "Our confidence is very high that this is the work of people associated with the Lazarus Group, because they had to have source code access," Thakur said in an interview.
>
> But he added: "We don't think that this is an operation run by a nation-state."
>
> With WannaCry, Thakur said, Lazarus Group members could have been moonlighting to make extra money, or they could have left government service, or they could have been contractors without direct obligations to serve only the government.

Krypt3ia has a post making fun of the nonsense theories out there.

> - *LAZARUS code snippets found in WANNACRY samples*
> - *LAZARUS has been active in stealing large sums of money from banks, as this attack was about ransom and money… well… UNDERPANTS GNOMES AND PROFIT!*
> - *LAZARUS aka Un, would likely love to sow terror by unleashing the digital hounds with malware attacks like this to prove a point, that they are out there and to be afraid.*

> - *LAZARUS aka Un, might have done this not only to sow fear but also to say to President CRAZYPANTS (Official USSS code name btw) "FEAR US AND OUR CYBER PROWESS"*
> - *LAZARUS aka Un, is poor and needs funds so ransoming hospitals and in the end gathering about $100k is so gonna fill the coffers!*
> - *LAZARUS aka UNIT 108 players are "Freelancing" and using TTP's from work to make MO' MONEY MO' MONEY MO' MONEY (No! Someone actually really floated that idea!)*
> - *LAZARUS is a top flight spooky as shit hacking group that needed to STEAL code from RiskSense (lookit that IPC$ from the pcap yo) to make their shit work.. Huh?*

Note the last bullet is a reference to another post he did, where he showed another piece of code in WannaCry was taken from folks working to reverse engineer Eternal Blue for Metasploit. That piece of borrowed code doesn't permit you to blame the Evil Hermit Kingdom, though, so no one is talking about it.

Perhaps the oddest piece of evidence presented relating the claim North Korea did WannaCry comes from CNBC.

> Analysts have been weighing in with various theories on the identity of those behind WannaCry, and some early evidence had pointed to North Korea. The Shadow Brokers endorsed that theory, perhaps to take heat off their own government backers for the disaster.

CNBC must be referring to this passage from Shadow Brokers' latest screed.

> In May, No dumps, theshadowbrokers is eating popcorn and watching "Your Fired" and WannaCry. Is being very strange behavior for crimeware? Killswitch? Crimeware is caring about target country? The oracle is telling theshadowbrokers North Korea is being responsible for the global cyber attack Wanna Cry. Nukes and cyber attacks, America has to go to war, no other choices! (Sarcasm) No new ZeroDays.

As part of a narrative of how reasonable it was to release all these files after they've been patched (all the while threatening far more damaging leaks), Shadow Brokers comments on WannaCry. Importantly, it lays out one detail — the kill switches — that doesn't make sense if the goal was true ransomware, as well as another detail — "caring about target country"? — that I don't understand. (Russia was hit badly in the attack, the US very lightly, and there were reports that Arabic speaking countries weren't hard hit, which I find interesting since it is the one Microsoft supported language that for which a ransomware note was not included.)

But the part that CNBC has read to mean Shadow Brokers *endorsed* this theory instead does nothing of the sort; if anything, it does the opposite. I read it as a comment about how

quickly we go from dodgy attribution to calling for war. And it comes with a sarcasm tag!

Moreover, why would you take Shadow Brokers' endorsement for anything? Either they did WannaCry (which actually seems to be what CNBC suggests; Krypt3ia makes fun of that possibility, too), in which case any endorsement might be disinformation, or they didn't do it, and they'd have no more clue who did than the rest of us.

The entire exercise in attribution with WannaCry is particularly odd given the assumptions that it is what it looks like, traditional ransomware, in spite of all the evidence to suggest it is not. And so we'll just ignore obvious tags, like a "sarcasm" tag, because accounting for such details gets very confusing.