FAKE RUSSIAN METADATA THAT WILL DO NOTHING TO PREVENT NUCLEAR WAR

Apparently I'm not the only one troubled by Tom Bossert's attribution of WannaCry to North Korea the other day.

In this post, Jack Goldsmith suggests the attribution will do nothing for deterrence.

> He said that he thought the public attribution alone, without more, accomplished something important in holding North Korea accountable. As he put it, somewhat confusingly, later:
>
> > It's about simple culpability. We've determined who was behind the attack and we're saying it. It's pretty straightforward. All I learned about cybersecurity I learned in kindergarten. We're going to hold them accountable and we're going to say it. And we're going to shame them for it.
>
> There you have it: The U.S. government thinks that naming and shaming by itself is a useful response to a cyberattack that caused billions of dollars of damage (though relatively little in the United States) and targeted precisely the types of critical infrastructure officials have long warned was a red line.
>
> [snip]
>
> it's not just that name and shame is ineffective. For at least two reasons, it is counterproductive for the United States to take evident pride in an

> attribution of a major cyberattack that it at the same time concedes it lacks the tools to retaliate against or deter. First, the consequence of the attribution, and the emphasis on the damage caused by WannaCry, is to raise expectations, at least domestically, about a response. Second, the effect of such a drum-beating attribution and statement of damage, combined with a weak response, is to reveal what has been apparent for a while: "We currently cannot put a lot of stock … in cyber deterrence," as former DNI Clapper said last year. "It is … very hard to create the substance and psychology of deterrence." When we overtly signal to North Korea that we have no tools to counteract their cyberattacks, we invite more attacks by North Korea and others—though to be fair, for the reasons Inglis stated, North Korea already has plenty of incentive, since cyber is a relatively inexpensive but very consequential tool for it, and since the United States has already imposed such extensive sanctions and seems out of tools.
>
> I must be missing something here. Probably what I am missing is that the public attribution sends an important signal to the North Koreans about the extent to which we have penetrated their cyber operations and are watching their current cyber activities. But that message could have been delivered privately, and it does not explain why the United States delayed public attribution at least six months after its internal attribution, and two months after the U.K. had done so publicly.

In this thread, Emily Maxima notes that not everyone in the Infosec community agrees with this attribution (here's an old piece I did on

some oddities with it) and worries that the attribution might be used to justify war with North Korea.

> So in the context of a potential hot-war with DPRK, the attribution chain from Wannacry to DPRK is *really* fucking important.

She then goes on to explain one of her concerns about the attribution to Lazarus group.

> A few months back, I was doing some research into malware that used obfuscation mechanisms in their campaigns and code that could be used to misattribute them to other actors/nations.
>
> It turns out, Lazarus group was one of these actors that had examples of misleading operation that made it seem like it was made in Russia, but was likely built to act as a false flag deus ex machina to lead researchers away from the true actors.
>
> [snip]
>
> [W]e're talking about an increasingly tense situation where the largest attack on networked computer infrastructure in probably the last 5 years may be pinned on a group known for running false flag operations.

She points to this article that shows that some 2016 watering hole attacks that had targeted Polish and Mexican bank supervisor sites, which might be associated with Lazarus, used Russian words as a false flag to hide their origin.

> In spite of some 'Russian' words being used, it is evident that the malware author is not a native Russian speaker.
>
> Of our previous examples, five of the commands were likely produced by an

online translation. Below we provide the examples and the correct analogues for reference:

Word	Type of error	Correct analogue
“ustanavlivat”	omitted sign at the end, verb tense error	*“ustanovit'”* or *“ustanoviti”*
“poluchit”	omitted sign at the end	*“poluchit'”* or *“poluchiti”*
“pereslat”	omitted sign at the end	*“pereslat'”* or *“pereslati”*
“derzhat”	omitted sign at the end	*“derzhat'”* or *“derzhati”*
“vykhodit”	omitted sign at the end, verb tense error	*“vyiti”*

Another example is *“kliyent2podklyuchit”*. This is most likely a result of an online translation of *“client2connect”* (which means *‘client-to-connect’*). In this case, the two words *“client”* and *“connect”*were translated separately, then transliterated from the Russian pronunciation form into the Latin alphabet and finally joined to produce *“kliyent2podklyuchit”*.

[snip]

Internally, the ActionScript also uses transliterated Russian words, similar to the tactic seen in the bot code:

Transliterated Russian words used in AS	Translated from Russian

Podgotovkaskotiny	Preparation of farm animals
geigeigei3raza	Hey, hey, hey 3 times
chainik	Dummy (a stupid person)
chainikaddress	Dummy’s address
poishemdatu	Let’s search for data
poiskvpro	Searching in ‘pro’
vyzov_chainika	Calling the dummy (a stupid person)
daiadreschainika	Get address of the dummy
runskotina	Execute farm animals
babaLEna	Old woman Lena

As seen in the table, while the words are technically Russian, their usage is out-of-context.

In one code fragment, the ActionScript contains both “chainik” and “dummy”:

```
01  private function put_dummy_args(param1:*) : *
02  {
03  return chainik.call.apply(null,param1);
```

```
04                  }
05  private function vyzov_chainika() : *
06                  {
07      return chainik.call(null);
08                  }
```

> As such, it is obvious that the word “dummy” has been translated into “chainik”. However, the word “chainik” in Russian slang (with the literal meaning of “a kettle”) is used to describe an unsophisticated person, a newbie; while, the word “dummy” in the exploit code is used to mean a “placeholder” or an “empty” data structure/argument.

The BAE analysis suggests that this incorrect usage is evidence proving the attackers are not native Russian speakers (leaving open the possibility they’re North Korean, though the report doesn’t attribute that aggressively).

I point to all this because of my continuing obsession with attacks featuring Russian metadata — starting from the first stolen Democratic files released by Guccifer 2.0 in June 2016 to faked Macron leak documents and extending to metadata ShadowBrokers left in some SWIFT files released in April — that served to deflect blame.

Perhaps it’s just fashionable to blame Russians these days.

Mind you, that other Russian metadata is for a totally unrelated watering hole attack, not for WannaCry. It’s worth remembering, however, that in addition to using Lazarus code, WannaCry also appears to have used code from Metasploit.

Ah well. I guess none of this will matter when North Korea nukes Seoul.