RICK LEDGETT CLAIMS NSA'S MALWARE ISN'T MALWARE

I was beginning to be persuaded by all the coverage of Kaspersky Labs that they did something unethical with their virus scans.

Until I read this piece from former NSA Deputy Director Rick Ledgett. In it, he defines the current scandal as Kaspersky being accused of obtaining NSA hacking tools via its anti-virus.

> Kaspersky Lab has been under intense fire recently for allegedly using, or allowing Russian government agents to use, its signature anti-virus software to retrieve supposed National Security Agency tools from the home computer of an NSA employee.

He then describes both Jeanne Shaheen's efforts to prohibit KAV use on government computers, and Eugene Kaspersky's efforts to defend his company. Ledgett than describes how anti-virus works, ending with the possibility that an AV company can use its filters to search on words like "secret" or "confidential" or "proprietary" (as if NSA's hacking tools were only classified proprietary).

> This all makes perfect sense for legitimate anti-virus companies, but it's also a potential gold mine if misused. Instead of looking for signatures of malware, the software can be instructed to look for things like "secret" or "confidential" or "proprietary"—literally anything the vendor desires. Any files of interest can be pulled back to headquarters under the pretext of analyzing potential malware.

He then claims that's what Kaspersky is accused of doing.

> So that is what Kaspersky has been accused of doing: using (or allowing to be used) its legitimate, privileged access to a customer's computer to identify and retrieve files that were not malware.

Except, no, it's not.

The only things Kaspersky is accused of having retrieved are actual hacking tools. Which, if anyone besides the NSA were to use them, would obviously be called malware. As Kim Zetter explains KAV and other AV firms use silent signatures to search for malware.

> Silent signatures can lead to the discovery of new attack operations and have been used by Kaspersky to great success to hunt state-sponsored threats, sometimes referred to as advanced persistent threats, or APTs. If a Kaspersky analyst suspects a file is just one component in a suite of attack tools created by a hacking group, they will create silent signatures to see if they can find other components related to it. It's believed to be the method Kaspersky used to discover the Equation Group — a complex and sophisticated NSA spy kit that Kaspersky first discovered on a machine in the Middle East in 2014.

It's unclear whether Kaspersky found the malware by searching on "TS/SCI," actual tool names (which NSA stupidly uses in its code), or code strings that NSA reuses from one program to another.

> "[D]ocuments can contain malware — when you have things like macros and zero-days inside documents, that is relevant to a cybersecurity firm," said Tait, who is currently a cybersecurity fellow at

> the Robert S. Strauss Center for International Security and Law at the University of Texas at Austin. “What’s not clear from these stories is what precisely it was that they were looking for. Are they looking for a thing that is tied to NSA malware, or something that clearly has no security relevance, but intelligence relevance?”
>
> If Kaspersky was searching for “top secret” documents that contained no malicious code, then Tait said the company’s actions become indefensible.
>
> “In the event they’re looking for names of individuals or classification markings, that’s not them hunting malware but conducting foreign intelligence. In the event that the U.S. intelligence community has reason to believe that is going on, then they should … make a statement to that effect,” he said, not leak anonymously to reporters information that is confusing to readers.
>
> Kaspersky said in a statement to The Intercept that it “has never created any detection in its products based on keywords like ‘top secret’, or ‘classified.’”

One thing no one has discussed is whether Kaspersky could have searched on NSA’s encryption, because that’s how Kaspersky has always characterized NSA’s tools, by their developers’ enthusiasm for encryption.

In any case, what’s clear is no one would ever find a piece of NSA malware by searching on the word “proprietary,” so we can be sure that’s a bogus accusation.

I asked Susan Hennessey on Twitter, and she confirms that NSA did a prepublication review of this, so any “new” news in this is either bullshit (as the claim Kaspersky searched on the

word “proprietary” surely is) or “no[t] inadvertent declassification,” meaning NSA wanted Ledgett to break new news.

Which I take to mean that Ledgett is pretending that NSA’s malware is not malware but … Democracy Ponies or something like that. American exceptionalism, operating at the level of code.

Anyway, Ledgett goes on to suggest that Kaspersky can get beyond this taint by agreeing to let others spy on their malware detection to make sure it’s all legit. Except that is *precisely what we’re all worried Russia did against Kaspersky*, find malware as it transited from the TAO guy back to Kaspersky’s servers!

> If Eugene Kaspersky really wanted to assuage the fears of customers and potential customers, he would instead have all communications between the company’s servers and the 400 million or so installations on client machines go through an independent monitoring center. That way evaluators could see what commands and software updates were going from Kaspersky headquarters to those clients and what was being sent back in response. Of course, the evaluators would need to sign non-disclosure agreements to protect Kaspersky’s intellectual property, but they would be expected to reveal any actual misuse of the software. It’s a bold idea, but it’s the only way anyone can be sure of what the company is actually doing, and the only real way to regain trust in the marketplace. Let’s see if he does it.

What are the chances that NSA would have this “independent monitoring center” pwned within 6 hours, if it really even operated independently of NSA?

Like I said, I was beginning to be persuaded

that Kaspersky did something wrong. But this Ledgett piece leads me to believe this is just about American exceptionalism, just an attempt to protect NSA's spying from one of the few AV companies that will dare to spy on it.