RICK LEDGETT'S STRAW MALWARE

For some reason, over a month after NotPetya and almost two months after WannaCry, former Deputy DIRNSA Rick Ledgett has decided now's the time to respond to them by inventing a straw man argument denying the need for vulnerabilities disclosure. In the same (opening) paragraph where he claims the malware attacks have revived calls for the government to release all vulnerabilities, he accuses his opponents of oversimplification.

> The WannaCry and Petya malware, both of which are partially based on hacking tools allegedly developed by the National Security Agency, have revived calls for the U.S. government to release all vulnerabilities that it holds. Proponents argue this will allow for the development of patches, which will in turn ensure networks are secure. On the face of it, this argument might seem to make sense, but it is actually a gross oversimplification of the problem, would not have the desired effect, and would in fact be dangerous.

Yet it's Ledgett who is oversimplifying. What most people engaging in the VEP debate — even before two worms based, in part, on tools stolen from NSA — have asked for is for some kind of sense and transparency on the process by which NSA reviews vulnerabilities for disclosure. Ledgett instead poses his opponents as absolutists, asking for everything to be disclosed.

Ledgett then spends part of his column claiming that WannaCry targeted XP.

> Users agree to buy the software "as is" and most software companies will attempt to patch vulnerabilities as they are discovered, unless the software has been

> made obsolete by the company, as was the case with Windows XP that WannaCry exploited.
>
> [snip]
>
> Customers who buy software should expect to have to patch it and update it to new versions periodically.

Except multiple reports said that XP wasn't the problem, Windows 7 was. Ledgett's mistake is all the more curious given reports that EternalBlue was blue screening at NSA when — while he was still at the agency — it was primarily focused on XP. That is, Ledgett is one of the people who might have expected WannaCry to crash XP; that he doesn't even when I do doesn't say a lot for NSA's oversight of its exploits.

Ledgett then goes on to claim that WannaCry was a failed ransomware attack, even though that's not entirely clear.

At least he understands NotPetya better, noting that the NSA component of that worm was largely a shiny object.

> In fact, the primary damage caused by Petya resulted from credential theft, not an exploit.

The most disturbing part of Ledgett's column, however, is that it takes him a good eight (of nine total) paragraphs to get around to addressing what really has been the specific response to WannaCry and NotPetya, a response shared by people on both sides of the VEP debate: NSA needs to secure its shit.

> Some have made the analogy that the alleged U.S. government loss of control of their software tools is tantamount to losing control of Tomahawk missile systems, with the systems in the hands of criminal groups threatening to use them. While the analogy is vivid, it incorrectly places all the fault on the

> government. A more accurate rendering would be a missile in which the software industry built the warhead (vulnerabilities in their products), their customers built the rocket motor (failing to upgrade and patch), and the ransomware is the guidance system.

We are almost a full year past the day ShadowBrokers first came on the scene, threatening to leak NSA's tools. A recent CyberScoop article suggests that, while government investigators now have a profile they believe ShadowBrokers matches, they're not even entirely sure whether they're looking for a disgruntled former IC insider, a current employee, or a contractor.

> The U.S. government's counterintelligence investigation into the so-called Shadow Brokers group is currently focused on identifying a disgruntled, former U.S. intelligence community insider, multiple people familiar with the matter told CyberScoop.
>
> [snip]
>
> While investigators believe that a former insider is involved, the expansive probe also spans other possibilities, including the threat of a current intelligence community employee being connected to the mysterious group.
>
> [snip]
>
> It's not clear if the former insider was once a contractor or in-house employee of the secretive agency. Two people familiar with the matter said the investigation "goes beyond" Harold Martin, the former Booz Allen Hamilton contractor who is currently facing charges for taking troves of classified material outside a secure environment.

At least some of Shadow Brokers' tools were stolen after Edward Snowden walked out of NSA Hawaii with the crown jewels, at a time when Rick Ledgett, personally, was leading a leak investigation into NSA's vulnerabilities. And yet, over three years after Snowden stole his documents, the Rick Ledgett-led NSA still had servers sitting unlocked in their racks, still hadn't addressed its privileged user issues.

Rick Ledgett, the guy inventing straw man arguments about absolutist VEP demands is a guy who'd do the country far more good if he talked about what NSA can do to lock down its shit — and explained why that shit didn't get locked down when Ledgett was working on those issues specifically.

But he barely mentions that part of the response to WannaCry and NotPetya.