THE LEGITIMACY PROBLEM WITH NSA’S SILENCE ON WANNACRY

Over at Matt Suiche’s website, he chronicles the discovery of a way to work around WannaCry’s ransomware. First a guy named Adrien Guinet figured out how the find the prime numbers that had computed the key locking a computer’s files. Then a guy named Benjamin Delpy recreated the effort and tested it against versions up to Windows 7. This is not a cure-all, but it may be a way to restore files encrypted by the attackers.

This of course comes after Suiche and before him Malware Tech set up sinkholes to divert the malware attack. Other security researchers have released tools to prevent the encryption of files after infection.

And all the while, NSA — which made the exploit that made this worm so damaging, EternalBlue — has remained utterly silent. At this point, Lauri Love, who faces 99 years of prison time for alleged hacking in the US, has done more *in public* to respond to this global ransomware attack than the NSA has.

The most public comment from NSA has come in the form of this WaPo article, which describes “current and former” officials defending the use of EternalBlue and sort of confirming that NSA told Microsoft of the vulnerability. It also revealed the White House called an emergency cabinet meeting to deal with the attack. Department of Homeland Security released a pretty useless statement last Friday. On Monday, Homeland Security Czar Tom Bossert answered questions at the press briefing (sometimes inaccurately, I think), emphasizing that the US is not responsible for the attack.

> I’d like to instead point out that this was a vulnerability exploit as one part of a much larger tool that was put

> together by the culpable parties and not by the U.S. government.
>
> So this was not a tool developed by the NSA to hold ransom data.

That's it. That's what we've seen of our government's response to a malware attack that it had a role in creating.

(For what it's worth, people in the UK have said their cybersecurity organization, the National Cyber Security Centre, has been very helpful.)

Don't get me wrong. I'm sure folks at NSA have been working frantically to understand and undercut this attack. Surely they've been coordinating with the private sector, including Microsoft and more visible victims like FedEx. NSA intervention may even explain why there have been fewer infections in the US than in Europe. There may even be some cooperation between the security people who've offered public solutions and the NSA. But if those things have happened, it remains totally secret.

And I understand why NSA would want to remain silent. After all, companies and countries are going to want some accountability for this, and while the hackers deserve the primary blame, NSA's own practices have already come in for criticism in Europe.

Plus, I'm sure whatever NSA is doing to counter this attack is even more interesting — and therefore more important to keep secret from the attackers — than the really awesome sinkholes and prime number workarounds the security researchers have come up with. It's worth noting that the attackers and aspiring copy-catters are undoubtedly watching the public discussions in the security community to figure out how to improve the attack (though the WannaCry attackers didn't seem to want or be able to use the information on sinkholes to their advantage, as the release that fixed that problem is corrupted).

But, in my opinion, NSA’s silence creates a legitimacy problem. This is the premier SIGINT agency in the world, tasked to keep the US (and more directly, DOD networks) safe from such attacks. And it has remained silent while a bunch of researchers and consultants collaborating together have *appeared* to be the primary defense against the weaponization of an NSA tool.

If 22 year olds fueled by pizza are the best line of defense against global attacks, then it suggests (I’m not endorsing this view, mind you) that we don’t need the NSA.

Update: On Twitter, Jake Williams asked whether NSA would have had a better response if the defensive Information Assurance Directorate hadn’t been disbanded last year by Mike Rogers. I hadn’t thought of that, but it’s a good question.