COMPANIES VICTIMIZED BY REPURPOSED NSA TOOLS DON'T SHARE THOSE DETAILS WITH GOVERNMENT

Reporting on an appearance by acting DHS undersecretary for the National Protection and Programs Directorate Christopher Krebs, CyberScoop explains that the government only heard from six victims of the WannaCry and NotPetya ransomware outbreaks (two known major victims are Maersk shipping, which had to shut down multiple terminals in the US, and the US law firm DLA Piper).

> Christopher Krebs, acting undersecretary for the National Protection and Programs Directorate, told an audience of cybersecurity professionals Wednesday that the biggest issue with both incidents came from an absence of reports from businesses who were affected. While experts say that WannaCry and NotPetya disrupted business operations at American companies, it's not clear how many enterprises were damaged or to what degree.
>
> The government wanted to collect more information from affected companies in order to better assess the initial infection vector, track the spread of the virus and develop ways to deter similar future attacks.
>
> Collecting data from victim organizations was important, a senior U.S. official who spoke on condition of anonymity told CyberScoop, because the information could have been used to inform policymakers about the perpetrator of the attack and potential

> responses

The rest of the story explains that private companies are generally reluctant to share details of being a ransomware victim (particularly if a company pays the ransom, there are even legal reasons for that).

But it doesn't consider another factor. If a cop left his gun lying around and some nutjob stole the gun and killed a kid with it, how likely is that family going to trust the cop in question, who indirectly enabled the murder?

The same problem exists here. Having proven unable to protect its own powerful tools (this is more a factor in WannaCry than NotPetya, though it took some time before people understood that the latter didn't rely primarily on the NSA's exploit), the government as a whole may be deemed less trustworthy on efforts to respond to the attack.

Whether that was the intent or just a handy side benefit for the perpetrators of WannaCry (and of Shadow Brokers, who released the exploit) remains unclear. But the effect is clear: attacking people with NSA tools may undermine the credibility of the government, and in the process, its ability to respond to attacks.