NonPetya: no evidence it was a "smokescreen"

blog.erratasec.com/2017/06/nonpetya-no-evidence-it-was-smokescreen.html

Many well-regarded experts claim that the not-Petya ransomware wasn't "ransomware" at all, but a "wiper" whose goal was to destroy files, without any intent at letting victims recover their files. I want to point out that there is no real evidence of this.

Certainly, things look suspicious. For one thing, it certainly targeted the Ukraine. For another thing, it made several mistakes that prevent them from ever decrypting drives. Their email account was shutdown, and it corrupts the boot sector.

But these things aren't evidence, they are problems. They are things needing explanation, not things that support our preferred conspiracy theory.

The simplest, Occam's Razor explanation explanation is that they were simple mistakes. Such mistakes are common among ransomware. We think of virus writers as professional software developers who thoroughly test their code. Decades of evidence show the opposite, that such software is of poor quality with shockingly bad bugs.

It's true that effectively, nPetya is a wiper. Matthieu Suiche does a great job describing one flaw that prevents it working. @hasherezade does a great job explaining another flaw. But best explanation isn't that this is intentional. Even if these bugs didn't exist, it'd still be a wiper if the perpetrators simply ignored the decryption requests. They need not intentionally make the decryption fail.

Thus, the simpler explanation is that it's simply a bug. Ransomware authors test the bits they care about, and test less well the bits they don't. It's quite plausible to believe that just before shipping the code, they'd add a few extra features, and forget to regression test the entire suite. I mean, I do that all the time with my code.

Some have pointed to the sophistication of the code as proof that such simple errors are unlikely. This isn't true. While it's more sophisticated than WannaCry, it's about average for the current state-of-the-art for ransomware in general. What people think of, such the Petya base, or using PsExec to spread throughout a Windows domain, is already at least a year old.

Indeed, the use of PsExec itself is a bit clumsy, when the code for doing the same thing is already public. It's just a few calls to basic Windows networking APIs. A sophisticated virus would do this itself, rather than clumsily use PsExec.

Infamy doesn't mean skill. People keep making the mistake that the more widespread something is in the news, the more skill, the more of a "conspiracy" there must be behind it. This is not true. Virus/worm writers often do newsworthy things by accident. Indeed, the history of worms, starting with the Morris Worm, has been things running out of control more than the author's expectations.

What makes nPetya newsworthy isn't the EternalBlue exploit or the wiper feature. Instead, the creators got lucky with MeDoc. The software is used by every major organization in the Ukraine, and at the same time, their website was horribly insecure -- laughably insecure. Furthermore, it's autoupdate feature didn't check cryptographic signatures. No hacker can plan for this level of widespread incompetence -- it's just extreme luck.

Thus, the effect of bumbling around is something that hit the Ukraine pretty hard, but it's not necessarily the intent of the creators. It's like how the Slammer worm hit South Korea pretty hard, or how the Witty worm hit the DoD pretty hard. These things look "targeted", especially to the victims, but it was by pure chance (provably so, in the case of Witty).

Certainly, MeDoc was targeted. But then, targeting a single organization is the norm for ransomware. They have to do it that way, giving each target a different Bitcoin address for payment. That it then spread to the entire Ukraine, and further, is the sort of thing that typically surprises worm writers.

Finally, there's little reason to believe that there needs to be a "smokescreen". Russian hackers are targeting the Ukraine all the time. Whether Russian hackers are to blame for "ransomware" vs. "wiper" makes little difference.

Conclusion

We know that Russian hackers are constantly targeting the Ukraine. Therefore, the theory that this was nPetya's goal all along, to destroy Ukraines computers, is a good one.

Yet, there's no actual "evidence" of this. nPetya's issues are just as easily explained by normal software bugs. The smokescreen isn't needed. The boot record bug isn't needed. The single email address that was shutdown isn't significant, since half of all ransomware uses the same technique.

The experts who disagree with me are really smart/experienced people who you should generally trust. It's just that I can't see their evidence.

Update: I wrote another blogpost about "survivorship bias", refuting the claim by many experts talking about the sophistication of the spreading feature.

Update: comment asks "why is there no Internet spreading code?". The answer is "I don't know", but unanswerable questions aren't evidence of a conspiracy. "What aren't there any stars in the background?" isn't proof the moon landings are fake, such because you can't answer the question. One guess is that you never want ransomware to spread that far, until you've figured out how to get payment from so many people.