Twitter Thread by Vess

Vess
@VessOnSecurity

I kinda disagree with this.

Not disagree as in "He's wrong, this is complete bollocks" but as in "He's right about some things, wrong bout others, missing yet others and the things are much more nuanced and discretion must be applied".

> Never upload #ransomware samples to the Internet. Let me explain what information such a sample contains, why you shouldn't upload them, and what happens if you upload them after all. #SysAdmin #DFIR #malwarehttps://t.co/M4S3ET5Eqc
>
> — Thomas Barabosch (@tbarabosch) December 28, 2020

I was asked to elaborate, so here it is.

The whole article is based on the premise "ransomware contains data that's private for you, once you upload it, everyone can get it from VirusTotal". This is wrong and incomplete in several ways.

To begin with, by far not all ransomware is hand-crafted for the victim and even when it is, by far not all of it contains personal information.

Furthermore, the author is confusing the ransomware executable (which is what you normally upload to VirusTotal, so that the scanners there can tell you what it is) with the ransom note. The note contains victim-specific data much more often than the executable.

Next, VirusTotal, while hugely popular, is not the only such service. I very much like id-ransomware for ransomware identification - and you never upload the executable there anyway; only encrypted files (and ransom note, if available; often it's not).

id-ransomware does not make the uploads available to the public.

There are also services like hybrid-analysis where you can specify that a sample should not be shared publicly.

Next, many ransomwares delete the executable once it has finished encrypting, so you don't have an executable to upload anyway.

In fact, by the article's logic, you shouldn't upload *any* malware you come across to any place on the Internet, on the off-chance that it might contain information specific to you - and this is plain ridiculous.

Furthermore, your response to the incident (even if it consists of just consulting nomoreransom for the availability of a decryptor) depends very much on identifying the ransomware that has hit you. How are you going to do this?

Scanners like those that VT uses are pretty much useless, because they rarely bother with exact identification these days and often disagree in their naming. You need something better and more accurate, like id-ransomware.

Finally, don't forget that these days many ransomware gangs leak the information they have stolen before encrypting it, so your info is likely to become public anyway.

And at least if you are in Europe, when you discover a likely data breach, you have 72 hours to notify. If you try to hide that fact instead, you're likely to be slapped with fines far exceeding the ransom demands.

Basically, "never upload ransomware to the internet" is wrong. The correct position is "be aware of the possible pros and cons and exercise proper discretion".

/end