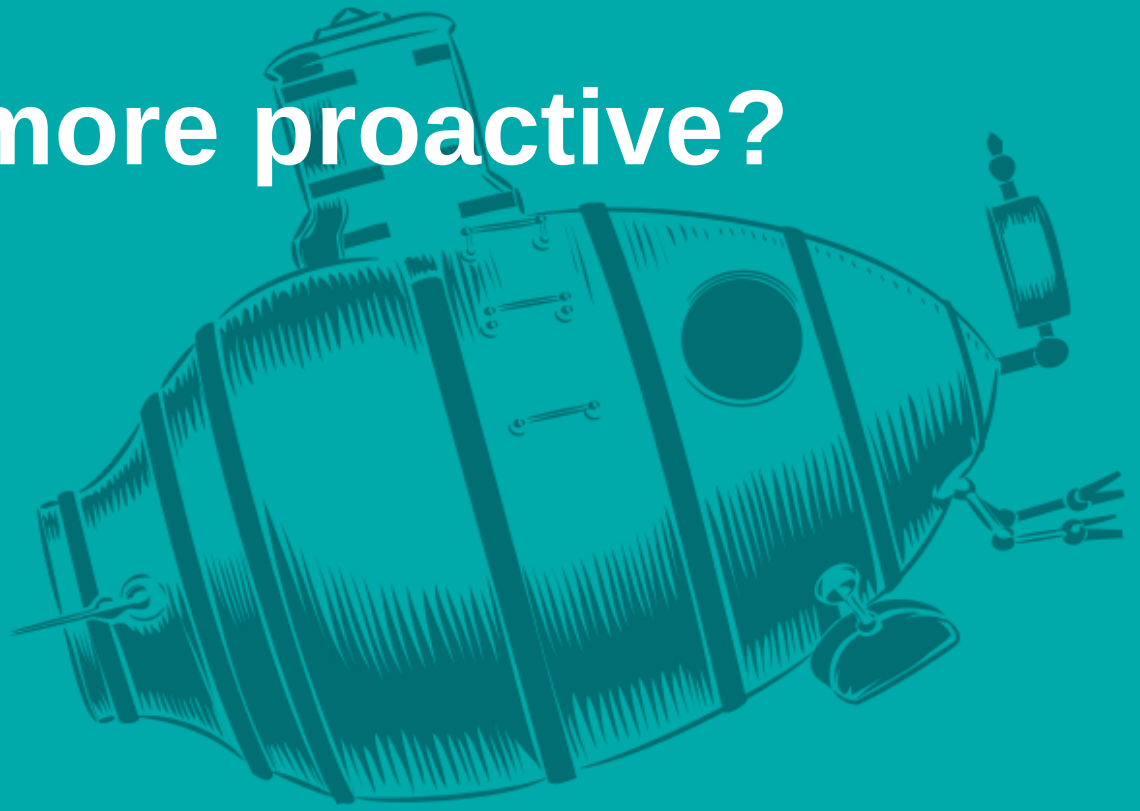
ALEF

Should we be (much) more proactive?



Jan Kopřiva

jan.kopriva@alef.com @jk0pr

ALEF CSIRT

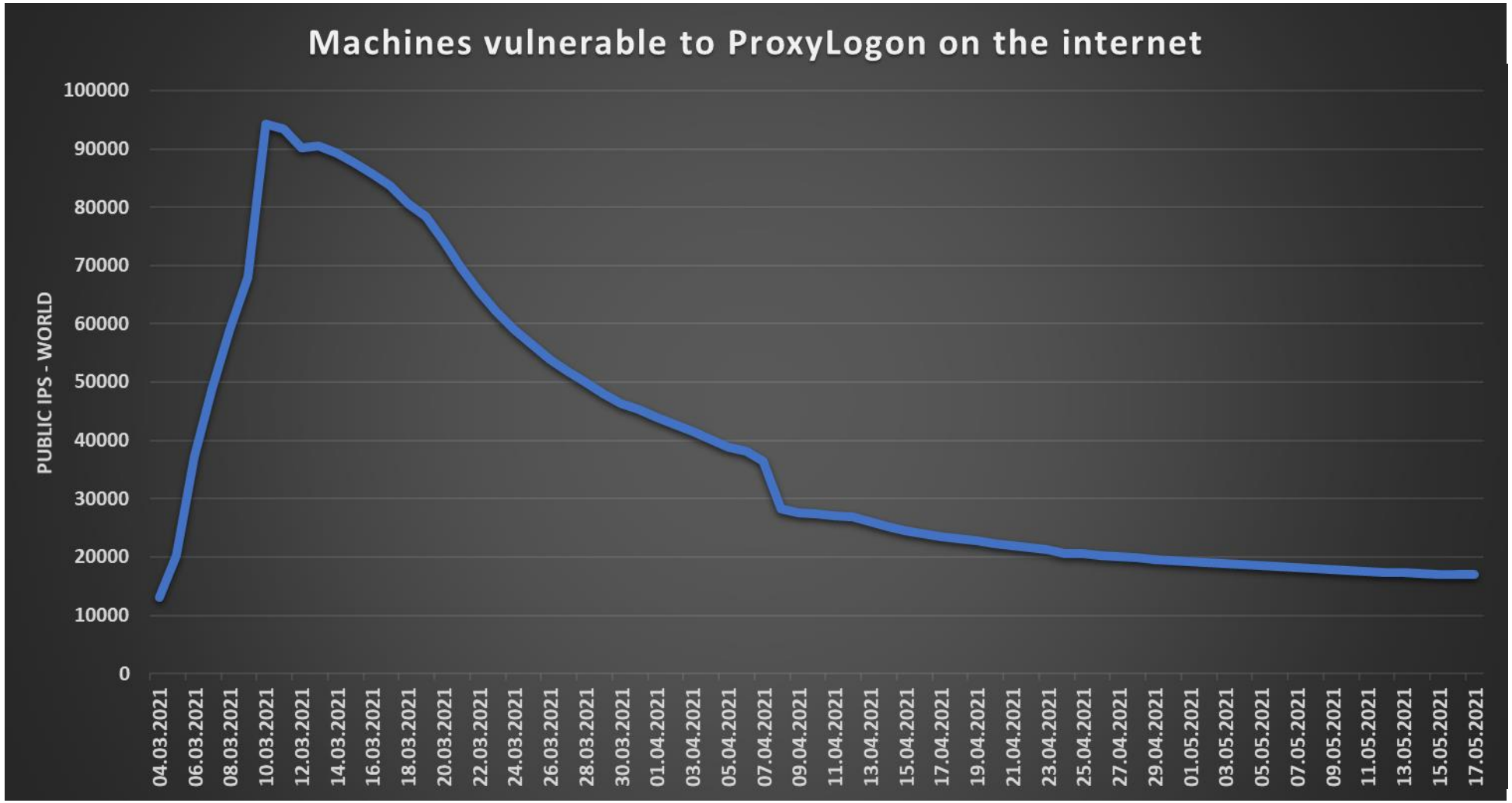
TLP: WHITE

How are we doing with managing vulnerabilities?

- Well, it‘s...complicated
  - As incident response specialists, we mostly respond to incidents after they occur
  - Many CSIRTs also proactively engage in improving security posture of their constituencies
  - In short, we‘re doing a lot

...is it enough, thought?

At first glance, it seems to be going well



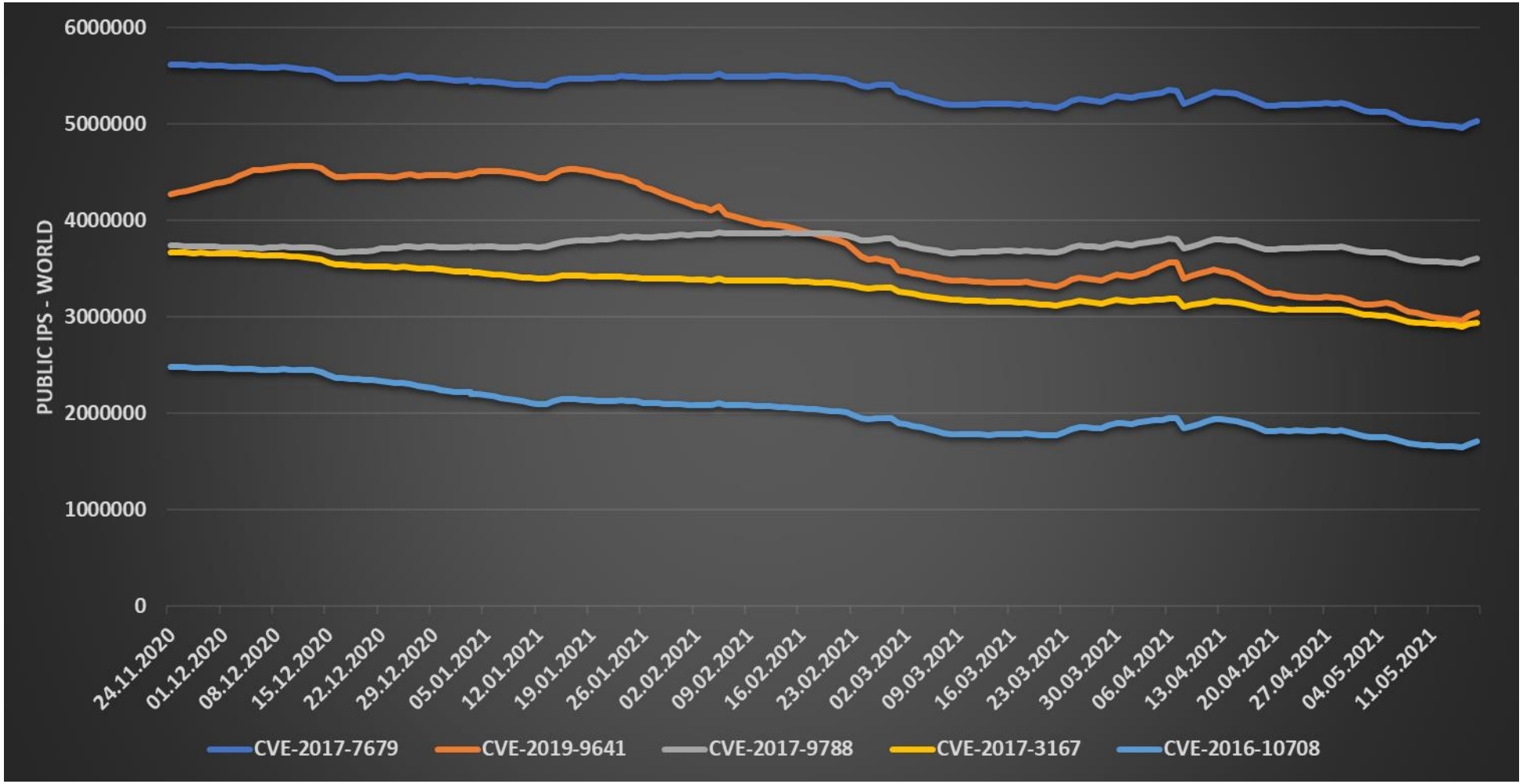
ALEF

Source: Shodan

What about not so well-known vulnerabilities?

- CVE-2017-7679 - Buffer Over-read in Apache - CVSSv3: 9.8
- CVE-2019-9641 - Uninitalized read in PHP - CVSSv3: 9.8
- CVE-2017-9788 - Information leak in Apache - CVSSv3: 9.1
- CVE-2017-3167 - Authentication bypass in Apache - CVSSv3: 9.8
- CVE-2016-10708 - Null Pointer Dereference in OpenSSH - CVSSv3: 7.5

What about not so well-known vulnerabilities?



Source: Shodan

What if a „really bad“ worm appears?

- Days of SQL Slammer and CodeRed are gone...
  - Significant move toward for-profit mentality among attackers made „destructive“ internet worms (mostly) obsolete
  - WannaCry and Mirai were still fairly „impactful“
    - What if the next one is worse?

Something needs to change

- The change won‘t come from the security industry
  - Not a technological issue
  - *<slightly_cynical_note>*

    The current „vulnerable“ landscape & associated FUD can be quite profitable...

    </slightly_cynical_note>

What about CSIRT communities?

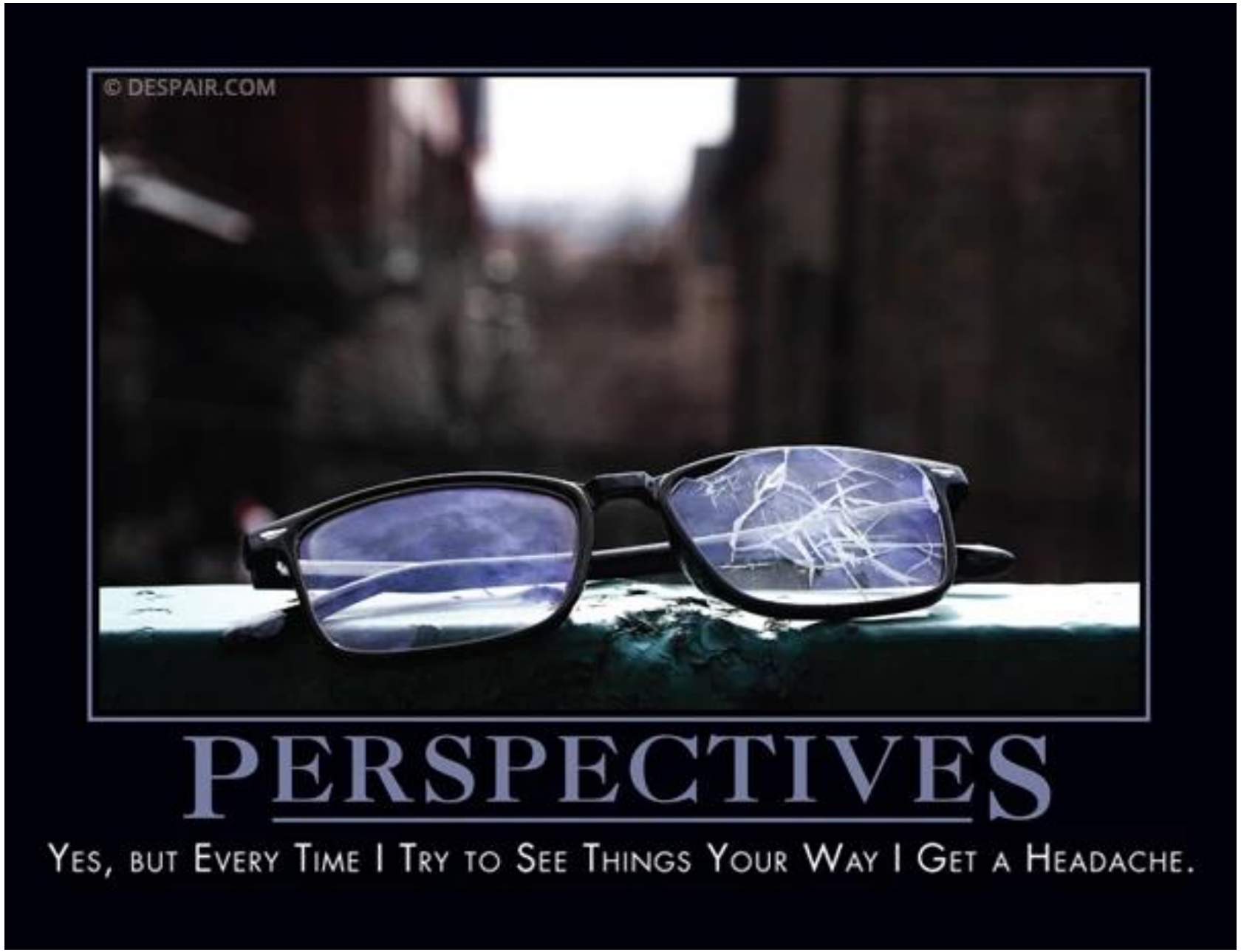
- We‘re organized
- We understand the issues
- We have links to governments, compliance organizations, large ISPs, hosting providers, cloud providers,...

What more can we do/recommend?

- This is not a question about technical capabilities but about ethics and current attitudes and paradigms
- We have (some) recent precedents for unusual actions
  - Distribution of „uninstall“ updates through Emotet C2 infrastructure
  - Hack-to-clean ProxyLogon-affected Exchange servers

Wild, unrealistic and ethically questionable ideas

- Legally forcing ISPs to inform subscribers about vulnerabilities affecting them? Potentially cutting service to those who don‘t patch?
- Moving to a „forced patching“ model for SW?
- Hack-to-clean as a standard approach?
- Hack-to-patch as a standard approach?
- Sanctioned creation of a nematode when new worm appears?

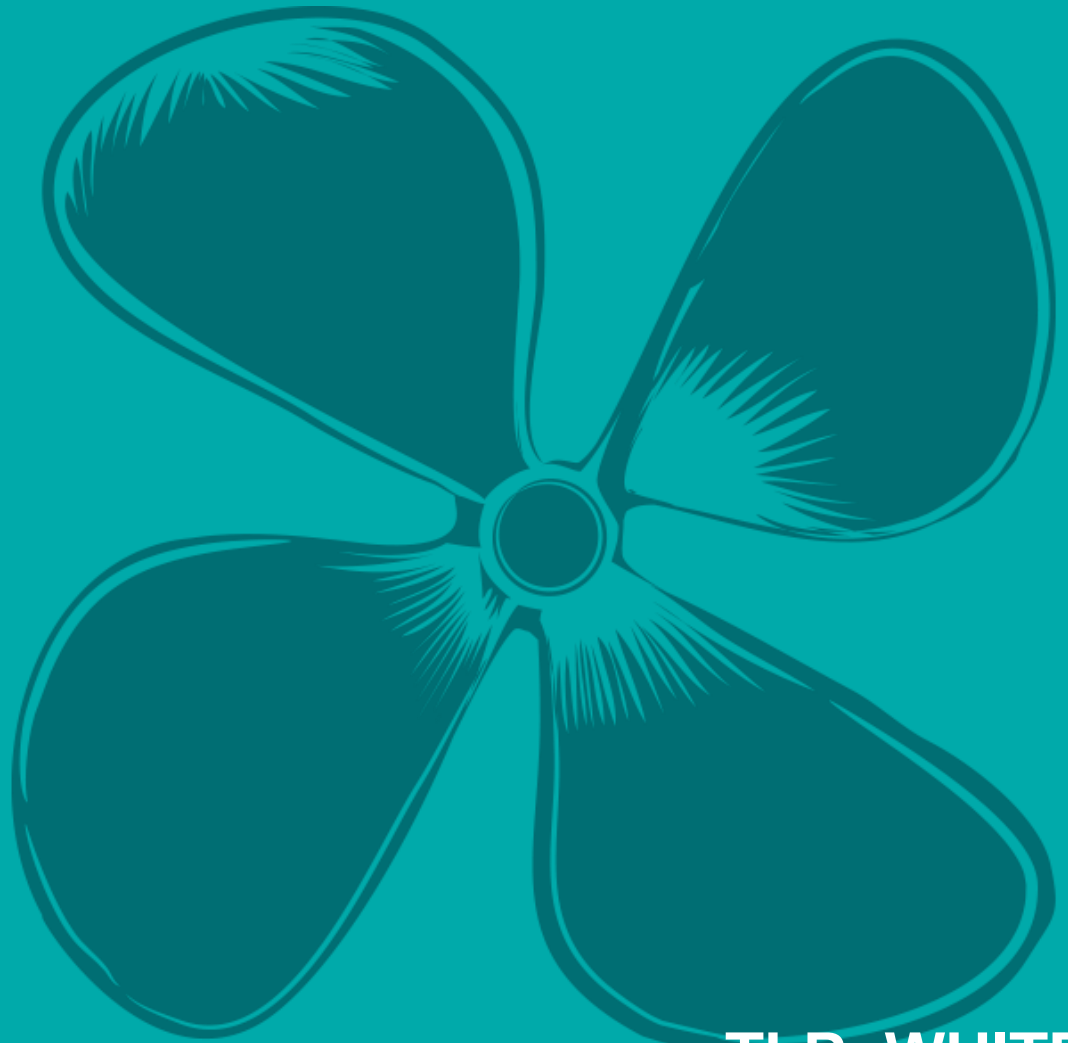


ALEF

Source: Despair.com

ALEF

Thank you for your attention



TLP: WHITE