TLP:CLEAR

NETTLES CONSULTING

Patching on a global scale: how fast do we really apply patches?

Jan Kopřiva

jan.kopriva@nettles.cz

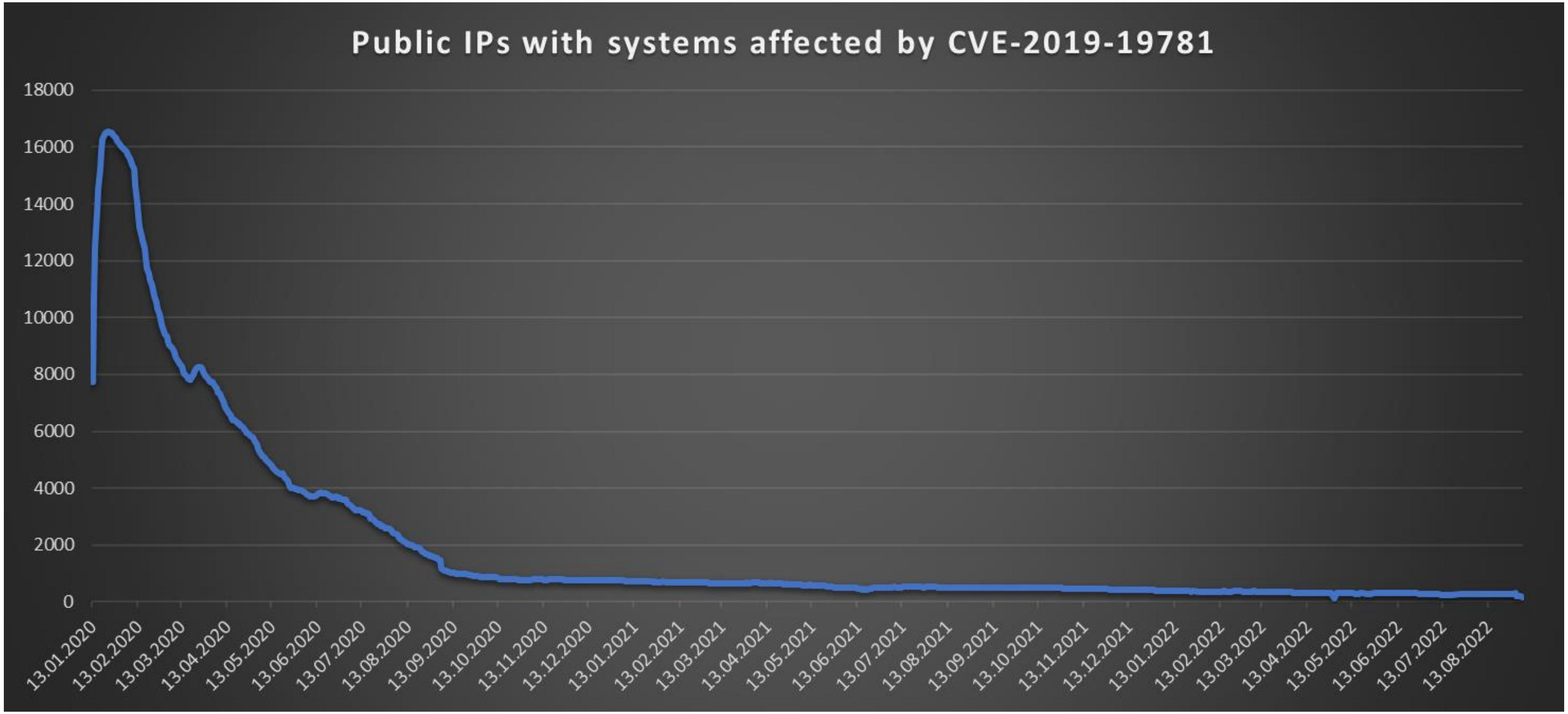
@jk0pr

67th TF-CSIRT Meeting - Vilnius

Do we really „manage“ vulnerabilities?

- Technical debt is continually increasing
  - The number of old / obsolete systems on the internal networks as well as on the internet keeps rising
- Historically, we used to “manage” mostly vulnerabilities affecting OS and SW directly used to provide services
- Log4shell was the first massive, global example of the need to go more in-depth when it comes to applications and (multi-level) dependencies on libraries, plugins and “external” code

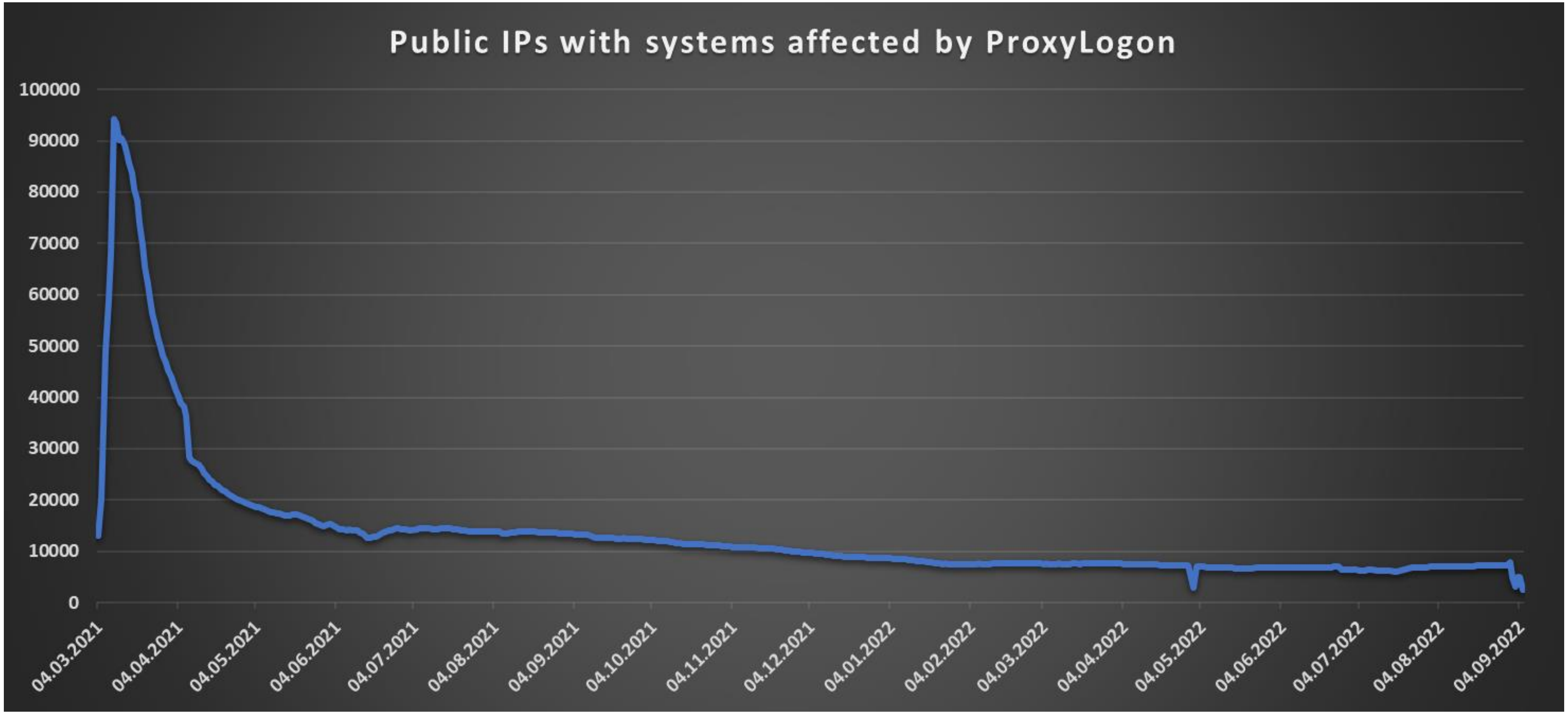
Quick reaction to vulnerabilities on a global scale is optimal…



Zdroj: Shodan

NETTLES CONSULTING

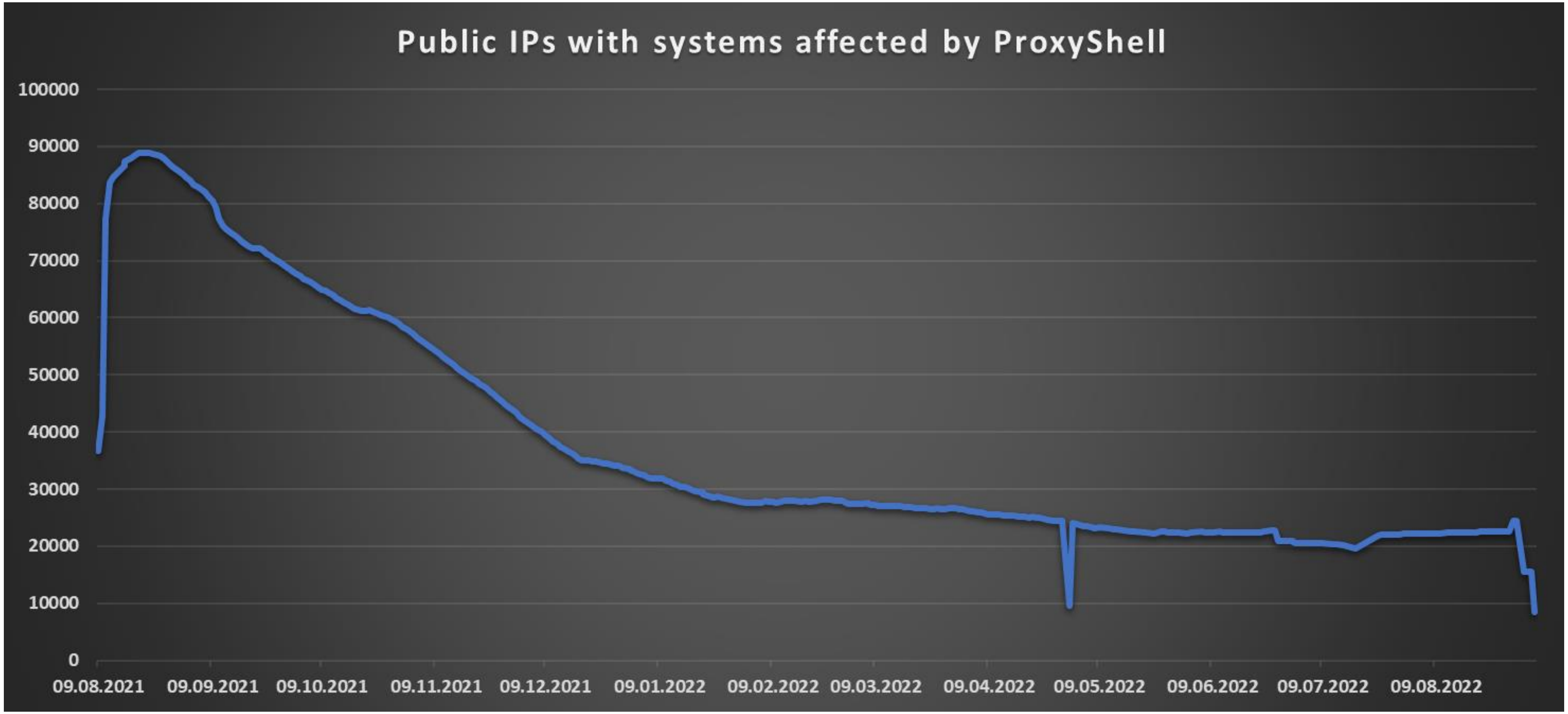
Quick reaction to vulnerabilities on a global scale is optimal…



Zdroj: Shodan

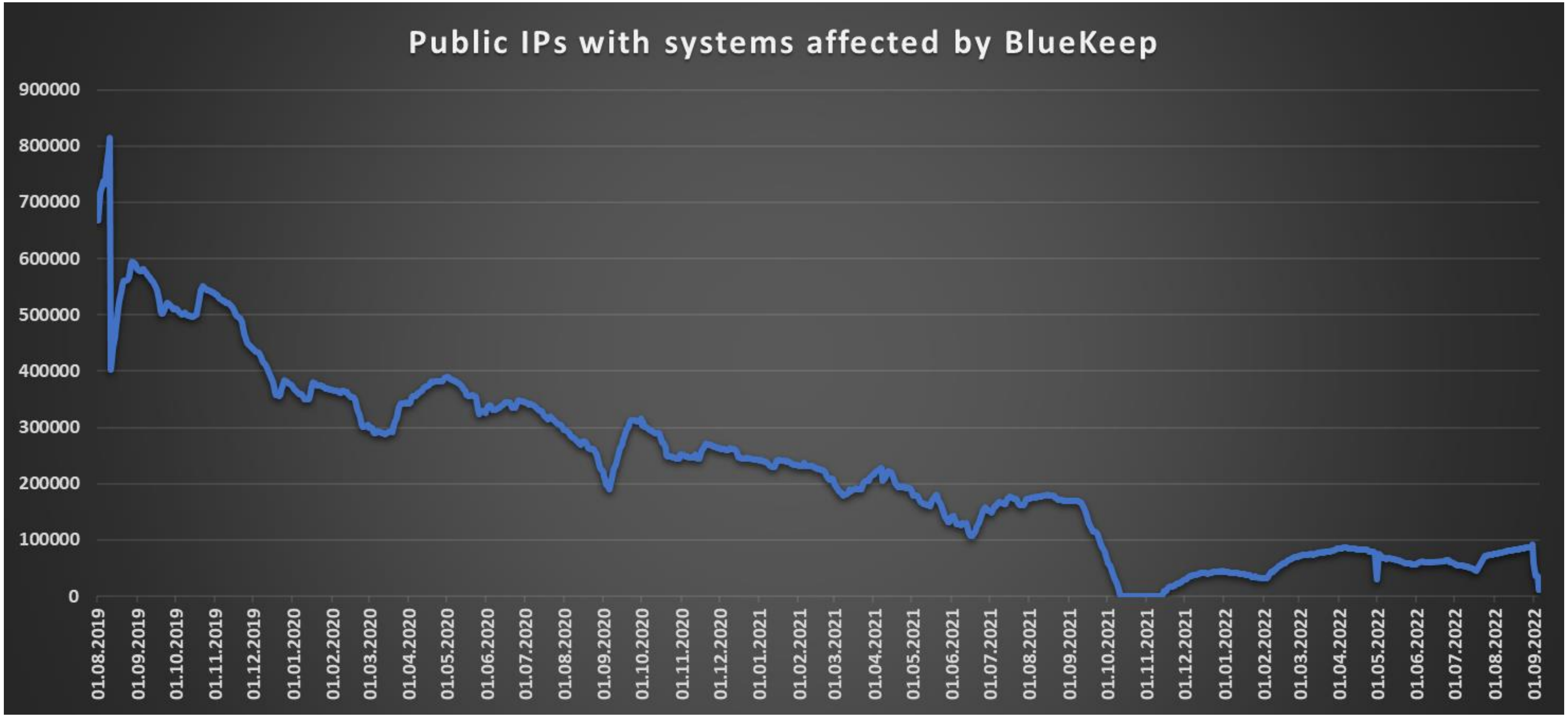
NETTLES
CONSULTING

…even slower reaction isn‘t necessarily the worse thing that could happen…



Zdroj: Shodan

…even slower reaction isn‘t necessarily the worse thing that could happen…



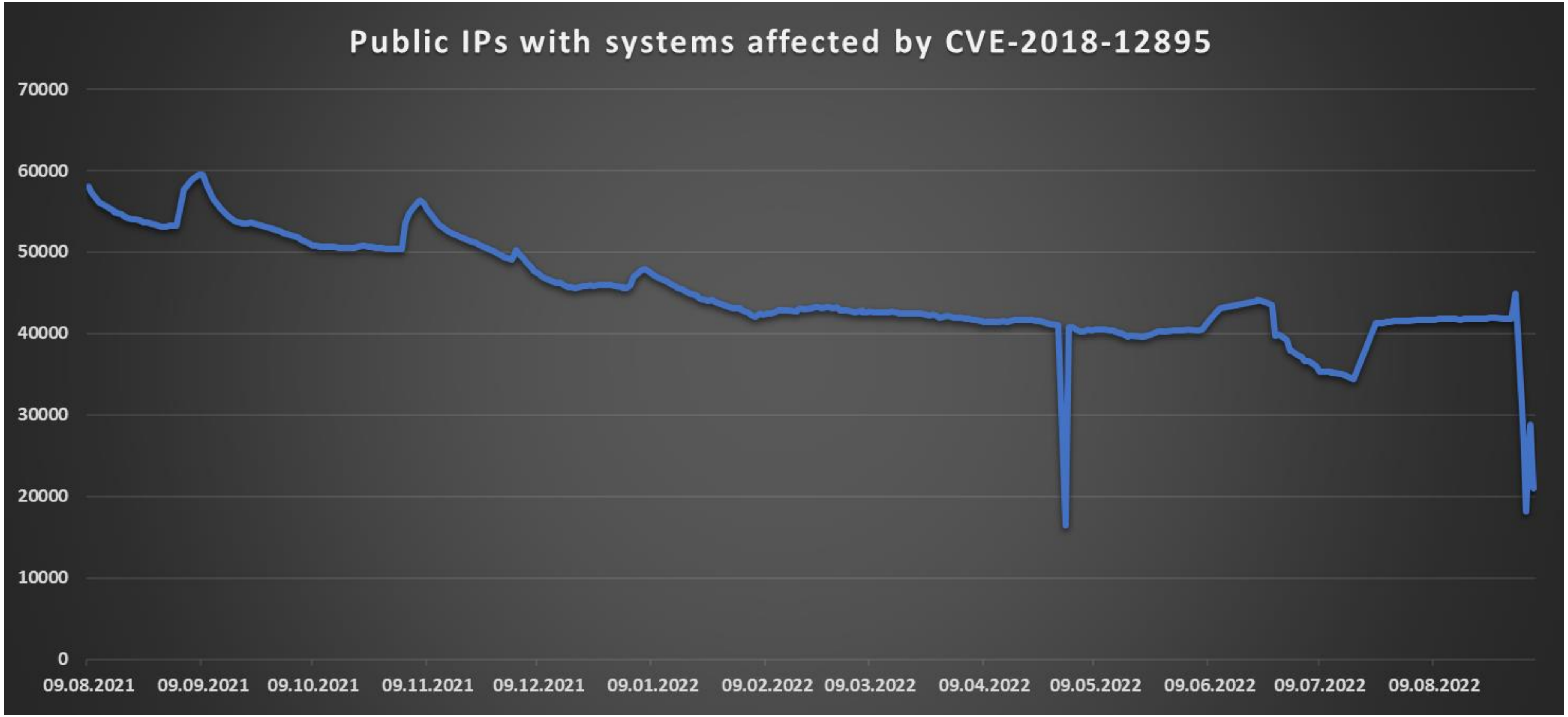
Zdroj: Shodan

NETTLES CONSULTING

Doesn‘t that mean that we know how to patch?

- 50% of affected internet-exposed systems patched in ~3 months
    - It is better than nothing, but is this enough?
- This is not all…
    - CVE-2019-19781 („Shitrix“) is an RCE vulnerability affecting a critical system, which was heavily covered by (not just) professional media, and for which an exploit has been published
    - CVE-2019-0708 („BlueKeep“) is an RCE vulnerability affecting a remote-access solution, which was heavily covered by (not just) professional media, and for which an exploit has been published
    - ...what about less critical vulnerabilities?

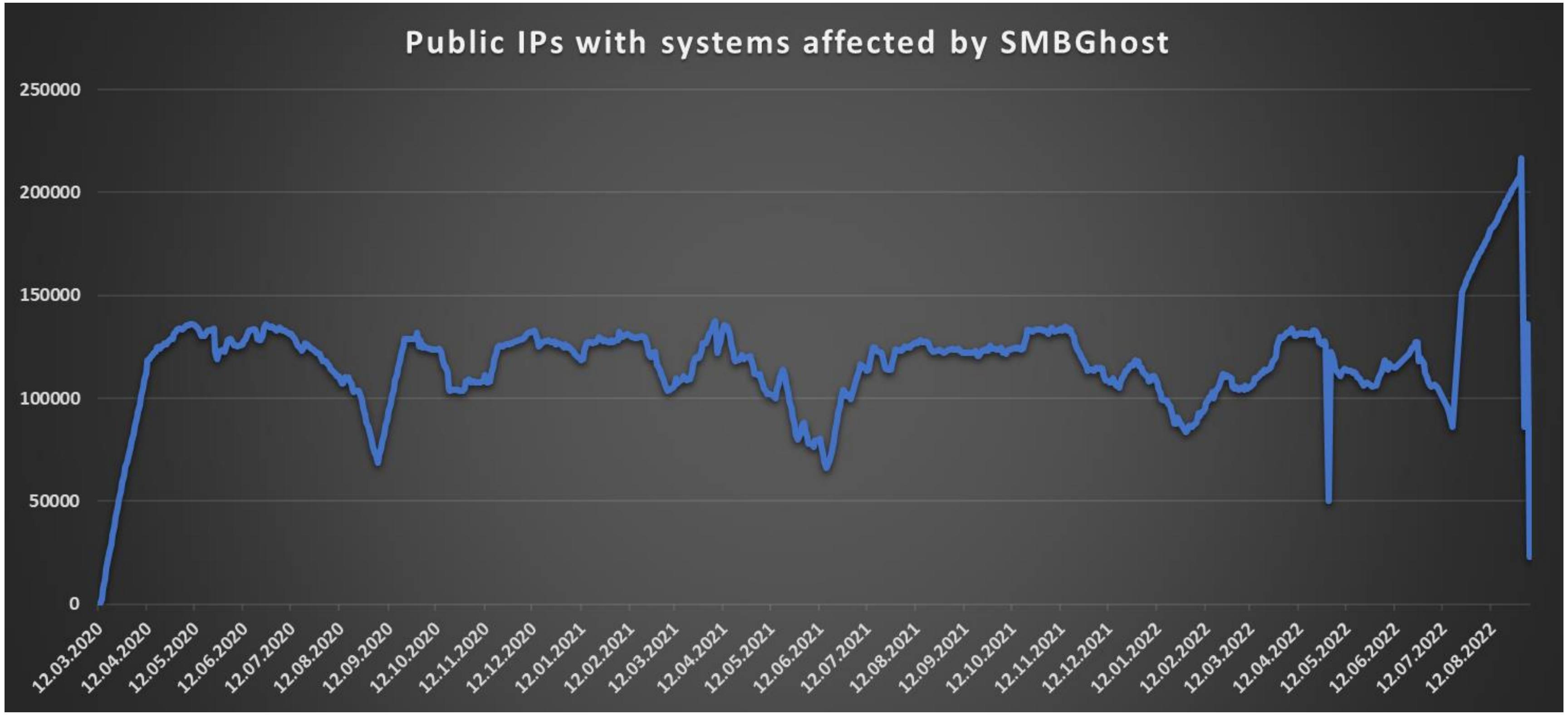
Less critical vulnerabilities



Zdroj: Shodan

Doesn‘t that mean that we at least know how to patch critical and famous vulnerabilities?

- Case study: SMBGhost (CVE-2020-0796)
  - Vulnerability in SMBv3, CVSS 10.0



Zdroj: Shodan

NETTLES
CONSULTING

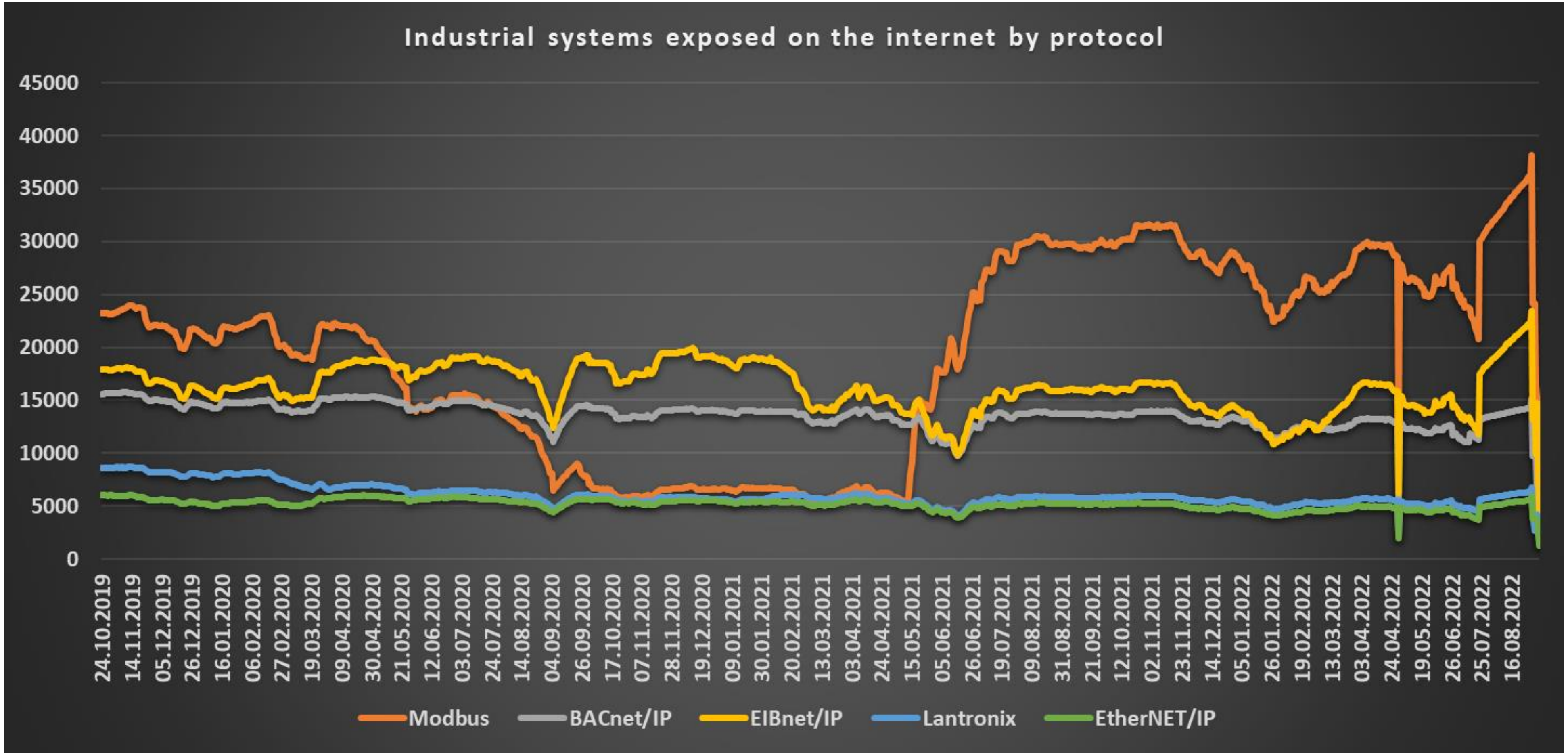
What is the current state of affairs?

- We can relatively quickly patch (most) critical vulnerabilities that are highly covered by media, affect critical systems and for which exploits have been published
- Everything else is a little „problematic“…

So, what don‘t we cover?

- It is possible that BlueKeep and SMBGhost might show us the reasons why reaction to even critical vulnerabilities differ
- Both are similar – critical, heavily covered by media, (PoC) exploit available
- BlueKeep affects RDP
- SMBGhost (as the name suggests) affects SMB
  - ⇒It is possible that the difference is due to (lack of) knowledge that about the relevant service being accessible on the side of the system owner..?

Who would expose an ICS protocol to the internet on purpose?



Zdroj: Shodan

NETTLES
CONSULTING

It seems that we can‘t patch almost anything reasonably fast quite yet…

- …though, it appears that high numbers of vulnerable systems exposed to the internet might be (at least in the long term) mostly connected with lack of attack surface management.
- At least some critical vulnerabilities seem to be patched on 50% of exposed systems within ~3 months

Q&A

NETTLES CONSULTING

Thank you for your attention

NETTLES CONSULTING