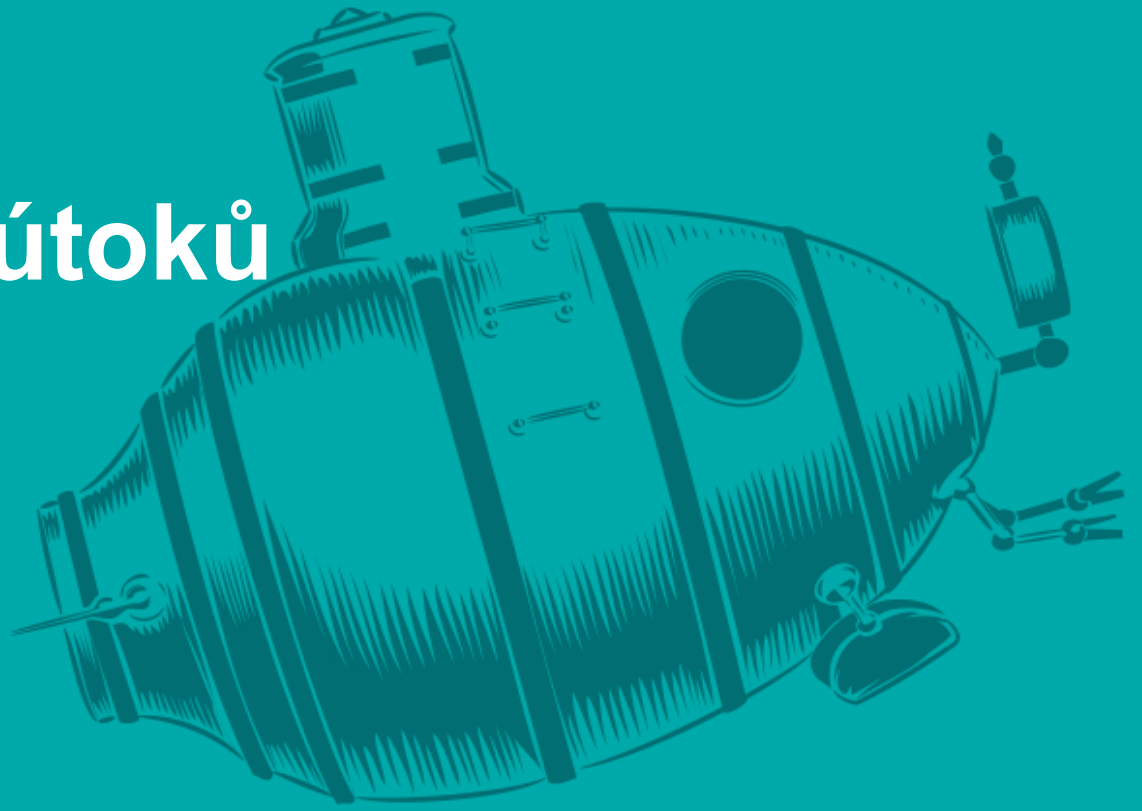
ALEF

2020:
Rok (ne)očekávaných útoků



Jan Kopřiva

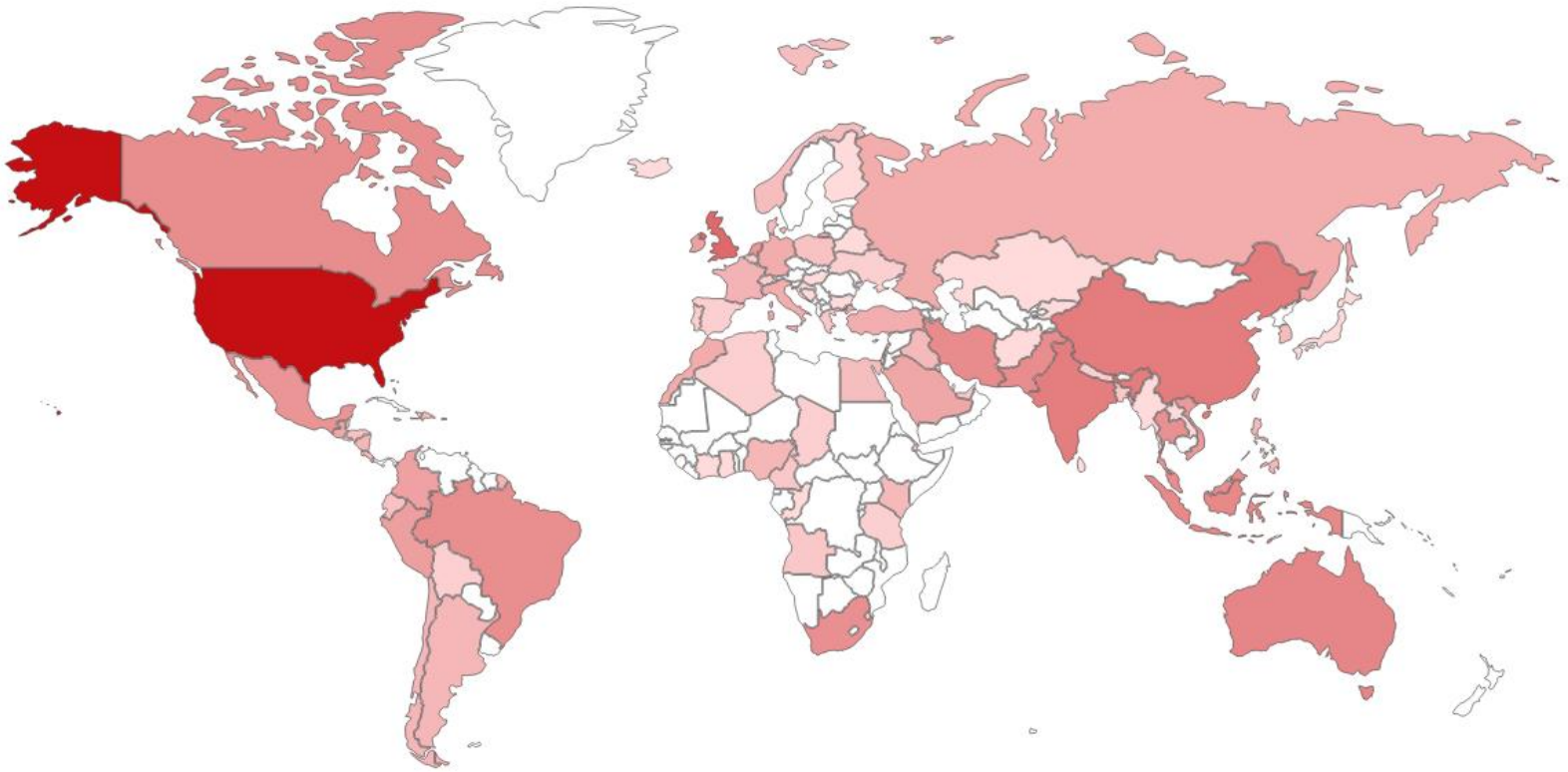
jan.kopriva@alef.com @jk0pr

ALEF CSIRT

TLP: WHITE

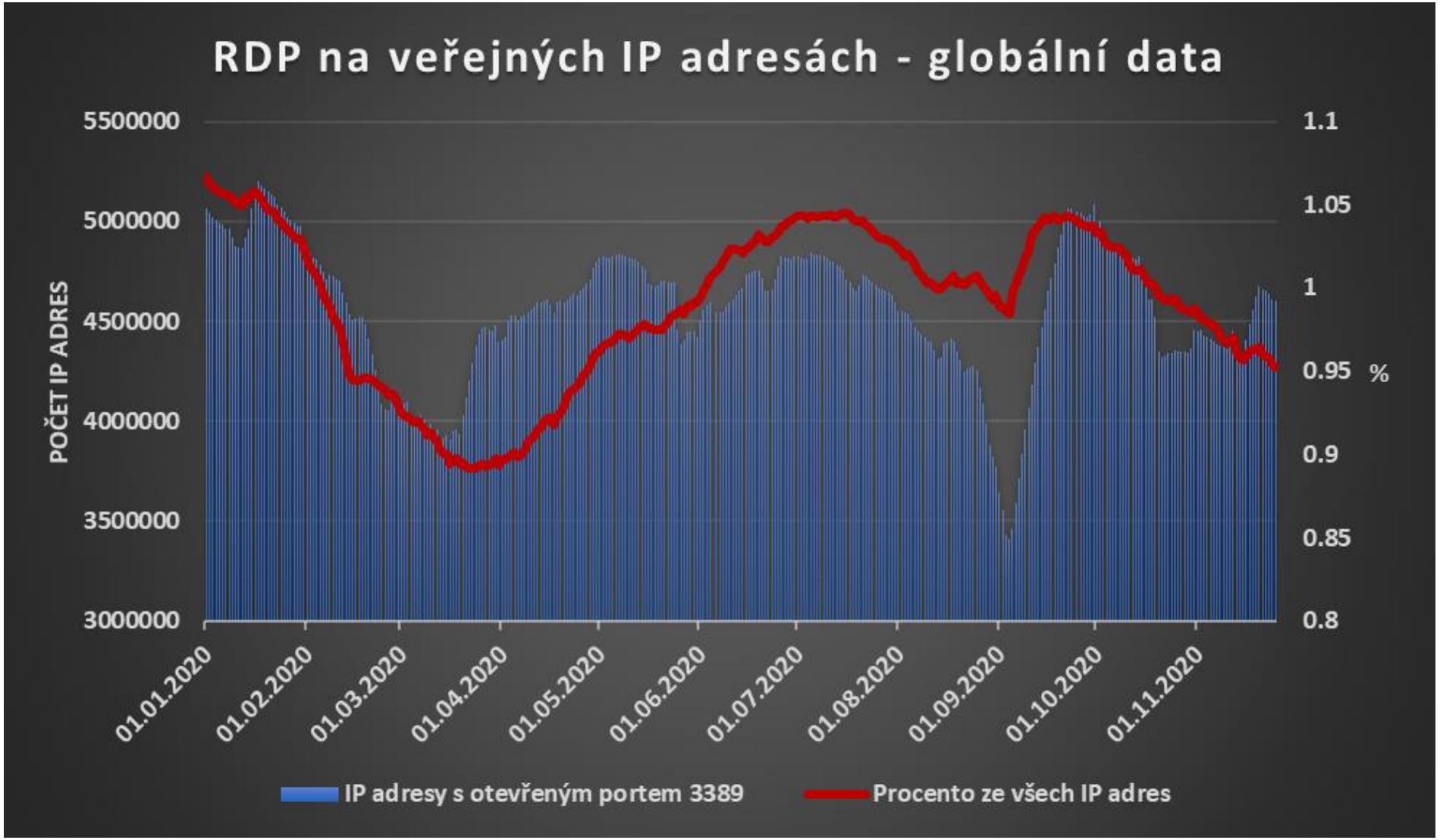
Útoky skrz dodavatelský řetězec

- SolarWinds (2020)
- M.E.Doc (2017)
- CCleaner (2017)

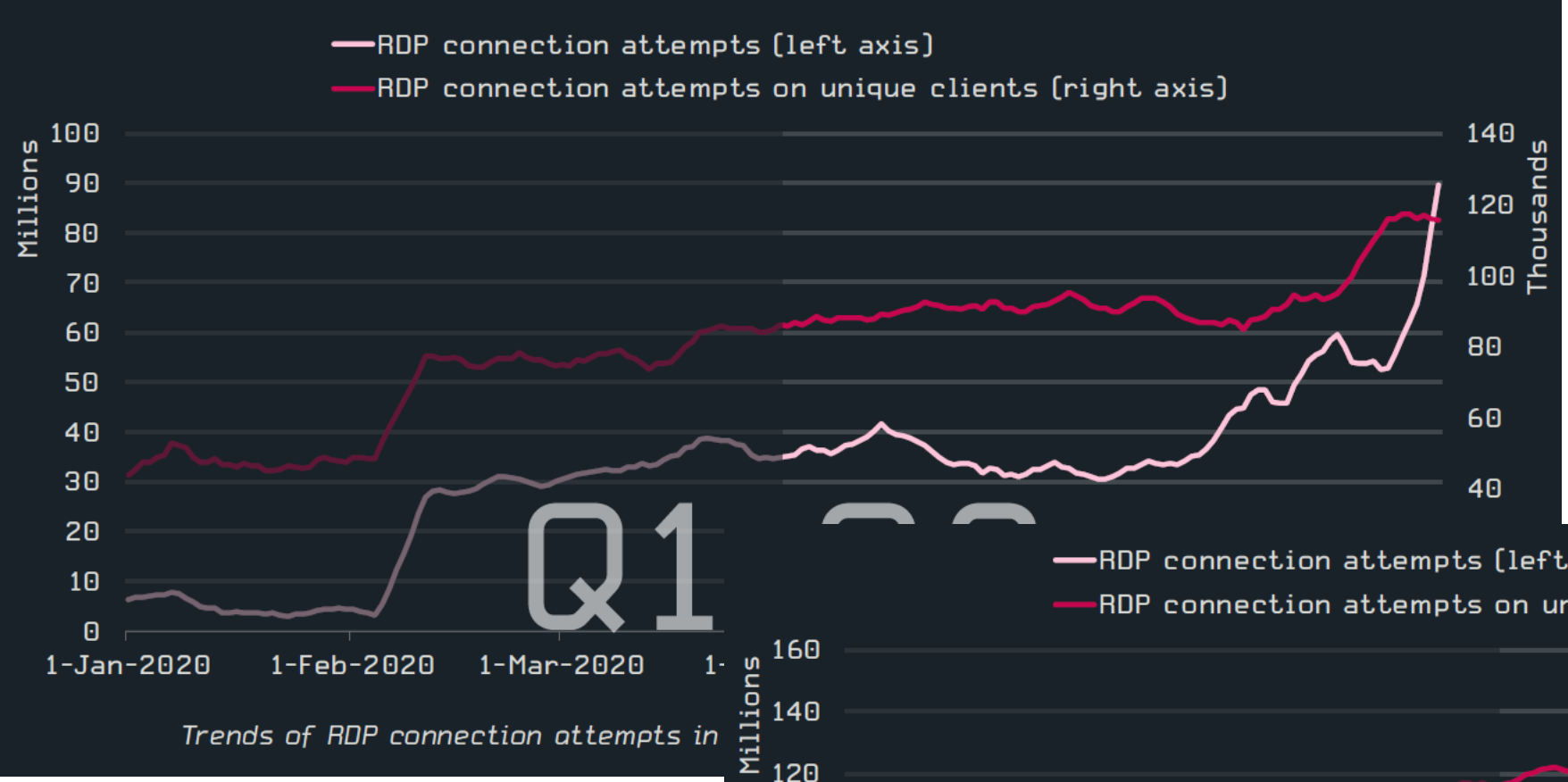


Zdroj:Shodan

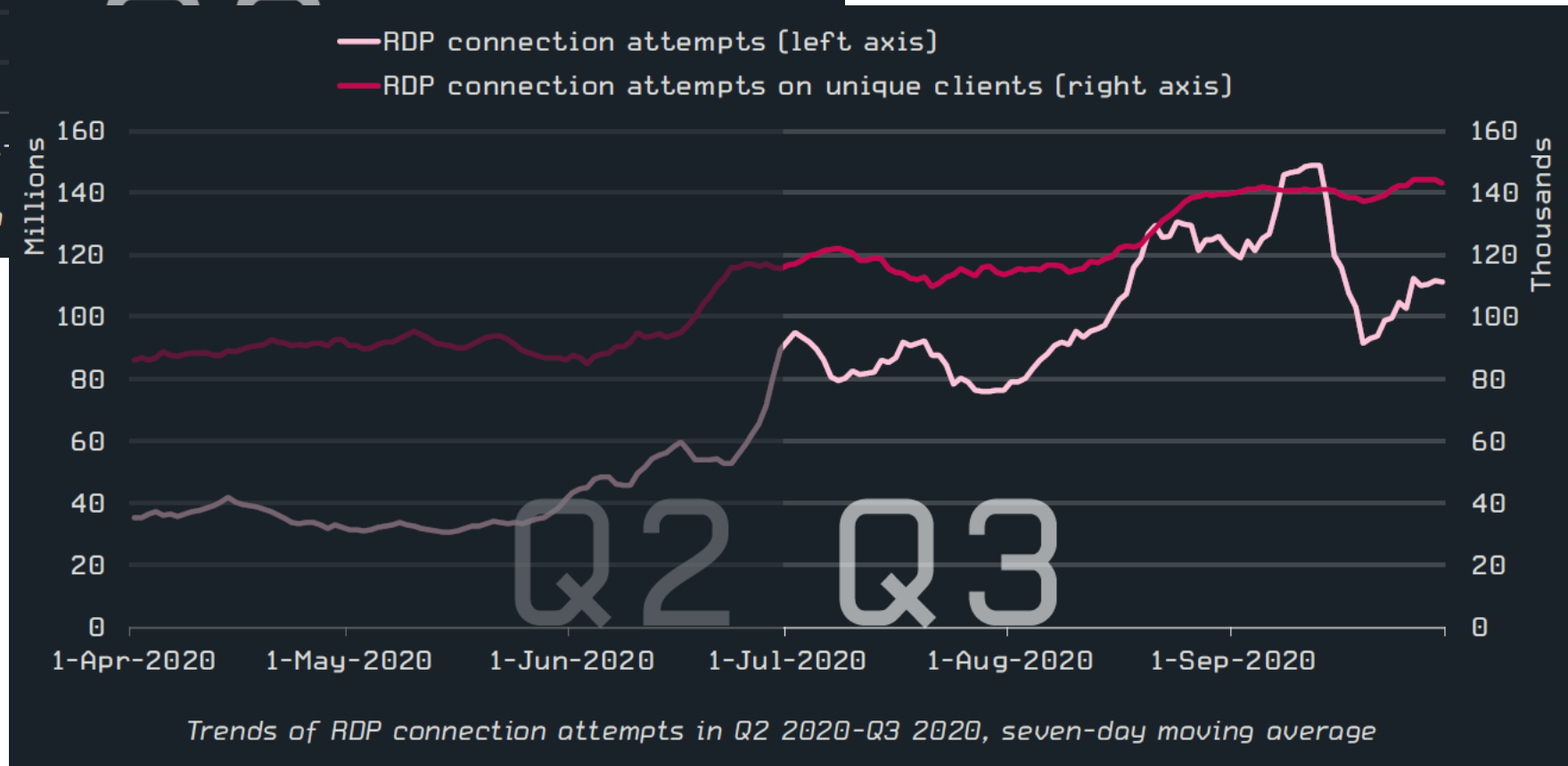
Útoky skrz vzdálený přístup



ALEF



Trends of RDP connection attempts in

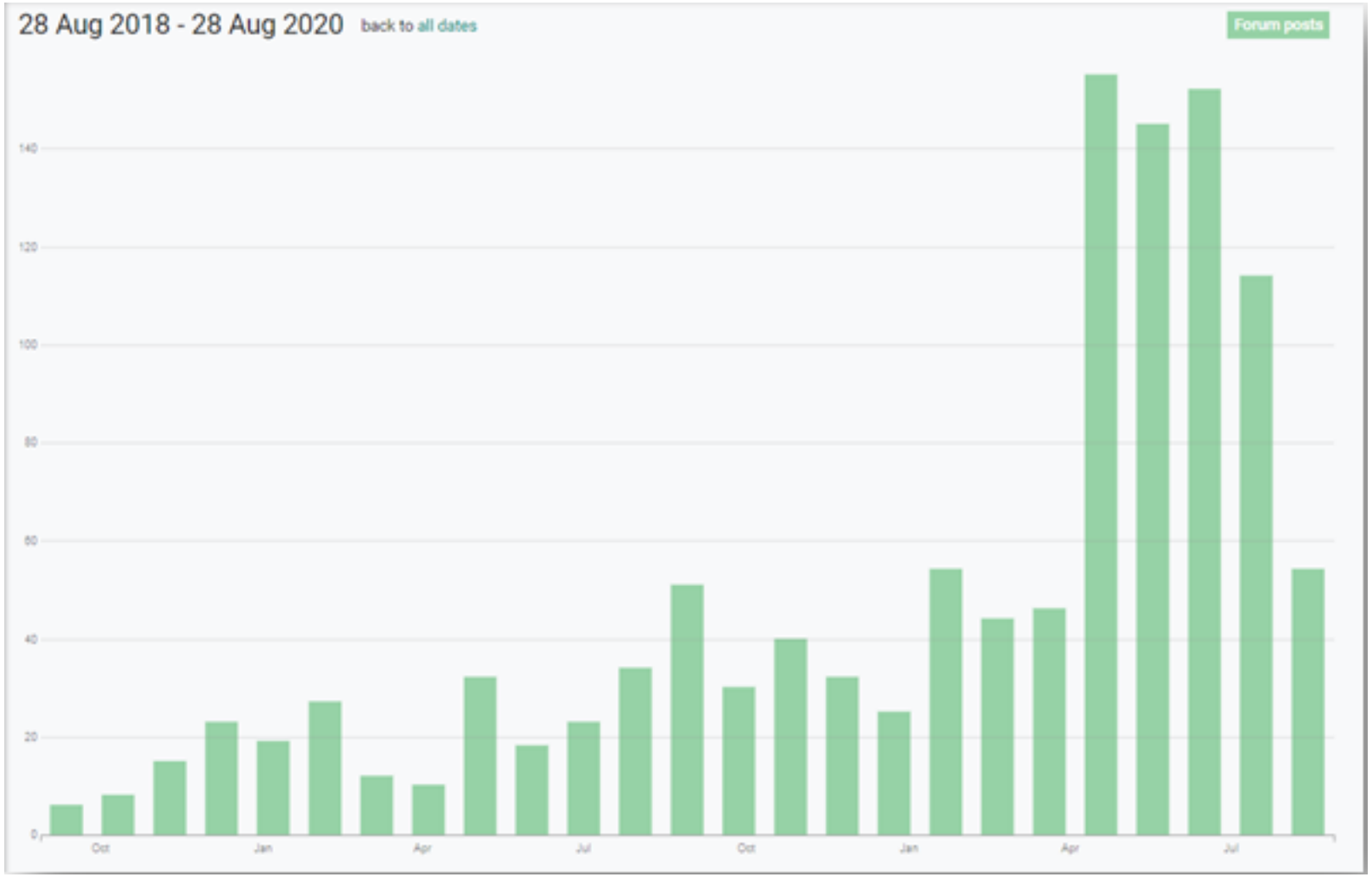


Trends of RDP connection attempts in Q2 2020-Q3 2020, seven-day moving average

Zdroj: ESET

ALEF

Útoky skrz vzdálený přístup



Zdroj: Digital Shadows

Útoky na zdravotnická zařízení

15 notable ransomware attacks on healthcare providers in 2019

Mackenzie Garrity - Wednesday, December 18th, 2019 Print | Email

Between hospitals having to turn to paper records and others notifying patients that their information may have been exposed, ransomware attacks have caused hospital executives to make cybersecurity a priority.

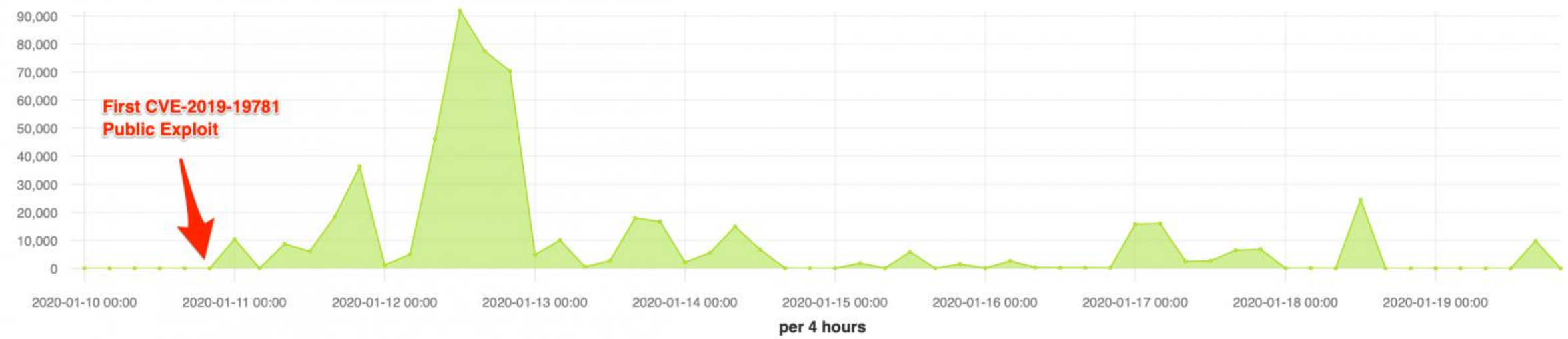
Below are 15 notable ransomware attacks this past year.

ALEF

Zdroj: Becker‘s Health IT

Útoky na nemocnice skrz vzdálený přístup...

10. září 2020 DoppelPaymer zasáhnul univerzitní kliniku v Düsseldorfu



ALEF

Zdroj: Internet Storm Center

Útoky skrz vzdálený přístup

- Publikace IP adres nezáplatovaných Fortinet SSL VPN bran

    ...a následně publikace přihlašovacích údajů k nim

https://[redacted]/remote/fgt_lang?lang=/../../../..//////////dev/cmdb/sslvpn_websession
https://[redacted]/remote/fgt_lang?lang=/../../../..//////////dev/cmdb/sslvpn_websession
https://[redacted]/remote/fgt_lang?lang=/../../../..//////////dev/cmdb/sslvpn_websession
https://[redacted]/remote/fgt_lang?lang=/../../../..//////////dev/cmdb/sslvpn_websession
https://[redacted]/remote/fgt_lang?lang=/../../../..//////////dev/cmdb/sslvpn_websession
https://[redacted]/remote/fgt_lang?lang=/../../../..//////////dev/cmdb/sslvpn_websession
https://[redacted]/remote/fgt_lang?lang=/../../../..//////////dev/cmdb/sslvpn_websession
https://[redacted]/remote/fgt_lang?lang=/../../../..//////////dev/cmdb/sslvpn_websession
https://[redacted]/remote/fgt_lang?lang=/../../../..//////////dev/cmdb/sslvpn_websession
https://[redacted]/remote/fgt_lang?lang=/../../../..//////////dev/cmdb/sslvpn_websession

Nesmíme zapomenout na sociotechniku

Zdroj: Bleeping Computer

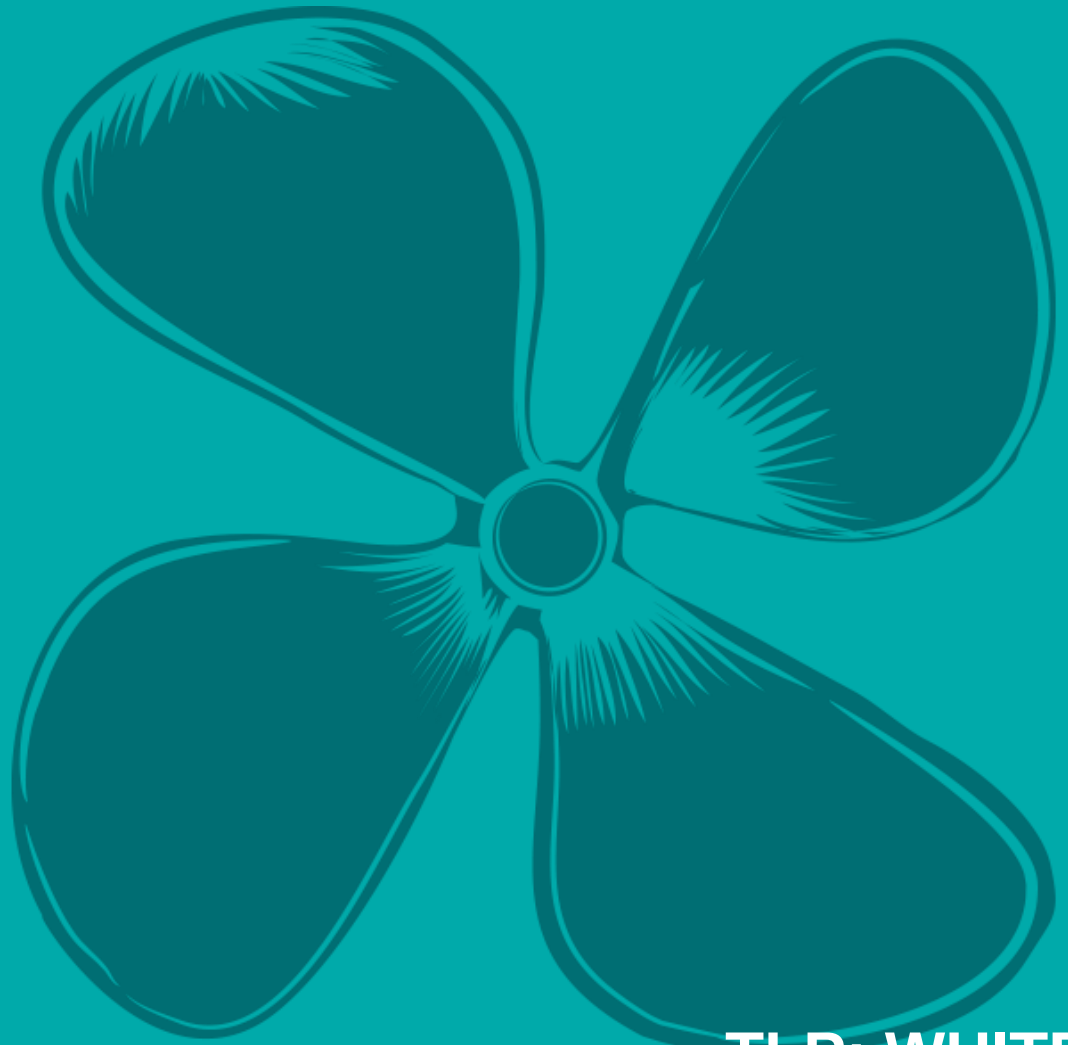
Na co se tedy zaměřit?

- Nespoléhejte jen na formální bezpečnostní standardy a soulad s nimi
  - Soulad s bezpečnostní normou neznamená, že je náš systém zabezpečený
- Sledujte aktuální dění...

  ...a poučte se z chyb těch, kteří přišli před vámi, jinak si je sami dříve nebo později zopakujete...

ALEF

Děkuji Vám za pozornost



TLP: WHITE

Než se rozloučíme...

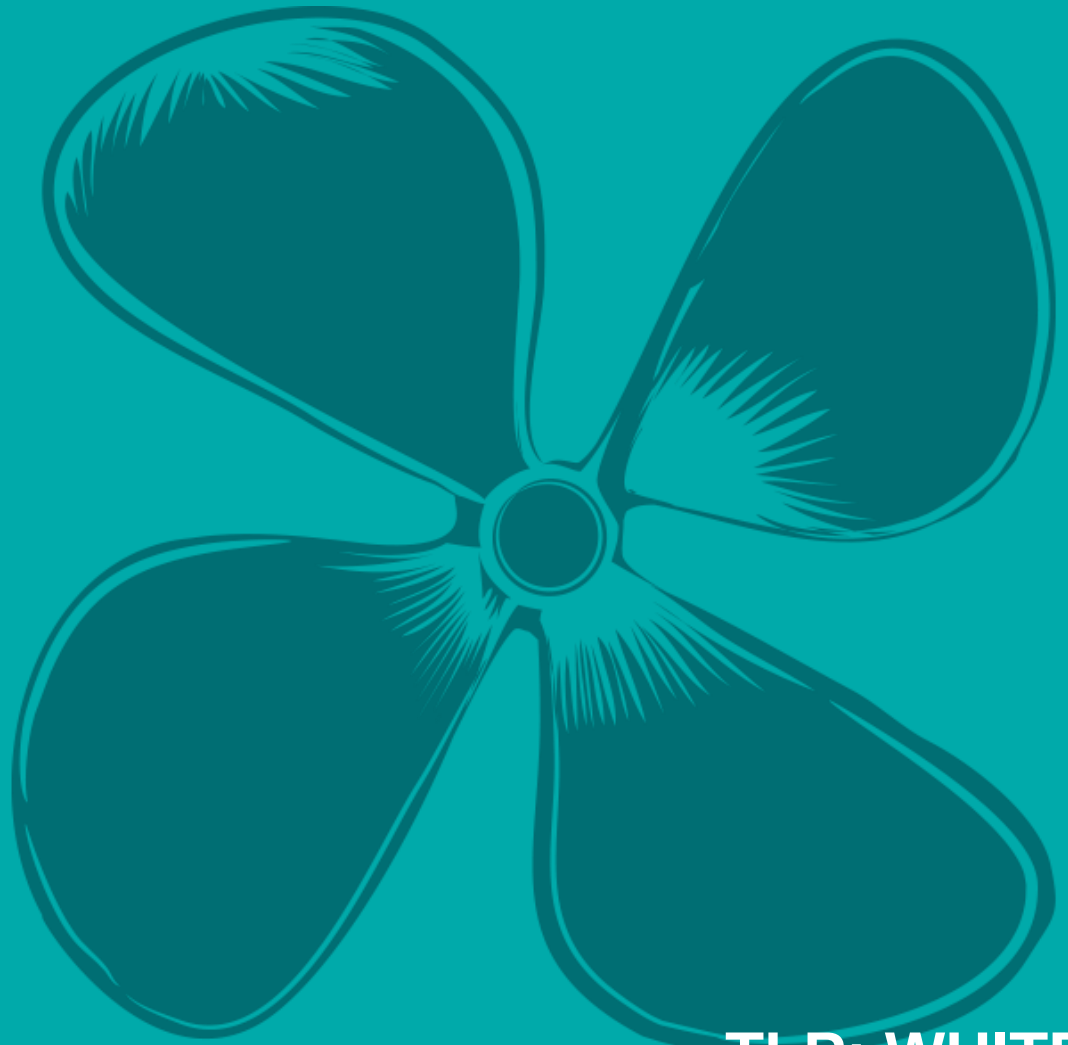
Od ledna 2021 nová YouTube série zaměřená na základní praktické dovednosti v IT bezpečnosti.

Detaily najdete na:

https://UntrustedNetwork.net/cs/

ALEF

Děkuji Vám za pozornost



TLP: WHITE