

## REVIL RANSOMWARE OPĚT NA SCÉNĚ

- REvil začíná mobilizovat jednotky (nábor lidí se očekává v listopadu 2021)
- Jen několik volných míst pro nové spolupracovníky / partnery
- Každý má svůj vlastní unikátní kryptor se sadou vlastních klíčů (žádný masivní deployment proces)
- Minimálně detekovatelný různými antivirovými systémy (6 z 23)
  - <https://dyncheck.com/scan/id/6142d6d2919c8e8ffe466f47a706c578>
  - <https://dyncheck.com/scan/id/afb62bec2f203b25b2ba7492e859b160>
  - ESET, McAfee, Avast, AVG, Trend Micro = čisté

<https://dyncheck.com/scan/id/6142d6d2919c8e8ffe466f47a706c578>

Result Detection rate: 6/23

AV	Status	Alert Screen
360 Total Security Essential	Clean	
AVG Internet Security	Clean	
AhnLab V3 Light	Clean	
Avast Internet Security	Clean	
Avira Internet Security	Clean	
BitDefender Total Security	Dynamic detect after 60 sec.	
BullGuard Internet Security	Clean	
Comodo Internet Security	Dynamic detect ⚠	
DrWeb Total Security	Clean	
Emsisoft Anti-Malware	Dynamic detect after 5 sec.	
Eset Smart Security	Clean	
F-Secure Internet Security	Clean	
Fortinet Smart Security	Clean	
Kaspersky Internet Security	Clean	
Malwarebytes Anti-Malware	Dynamic detect after 60 sec.	
McAfee Internet Security	Clean	
Norton Internet Security	Clean	
Panda Global Protection	Clean	
Sophos Anti-Virus	Dynamic detect after 60 sec.	
Symantec Endpoint Security 14	Clean	
Trend Micro Internet Security	Clean	
Webroot SecureAnywhere	Clean	
Windows Defender	Dynamic detect ⚠	