FCCN UNIDADE DA FCT
Tecnologia para o Conhecimento

CSIRT IN A BOX 2022

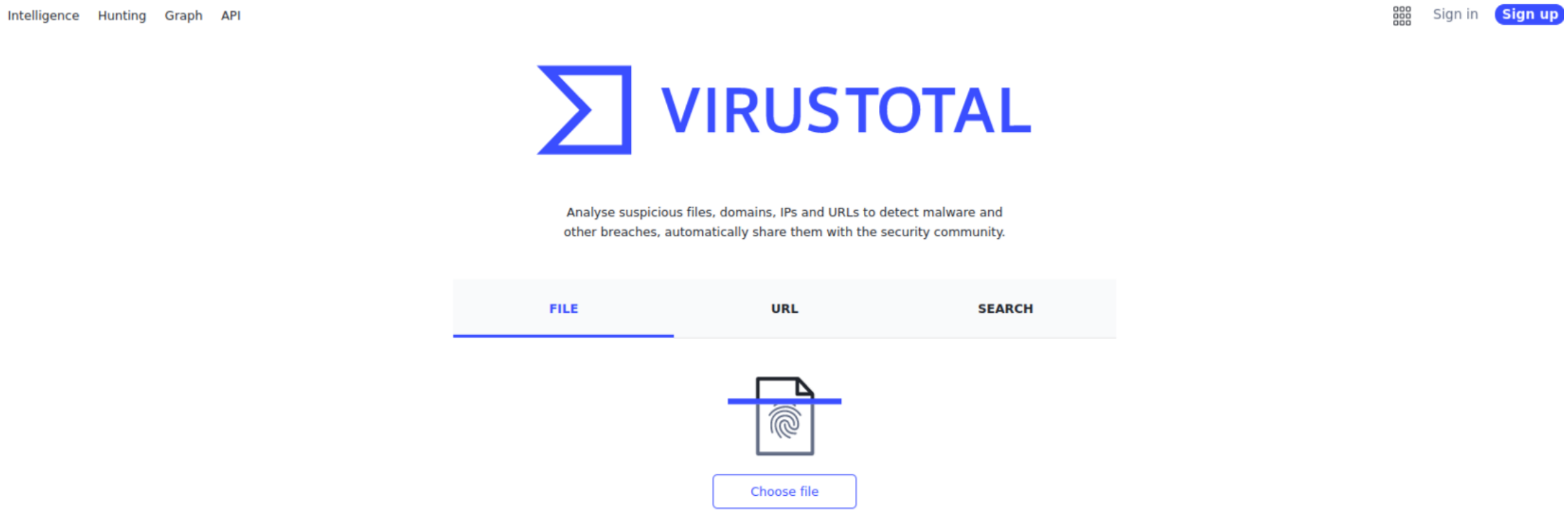
VIRUSTOTAL

Louise Altvater

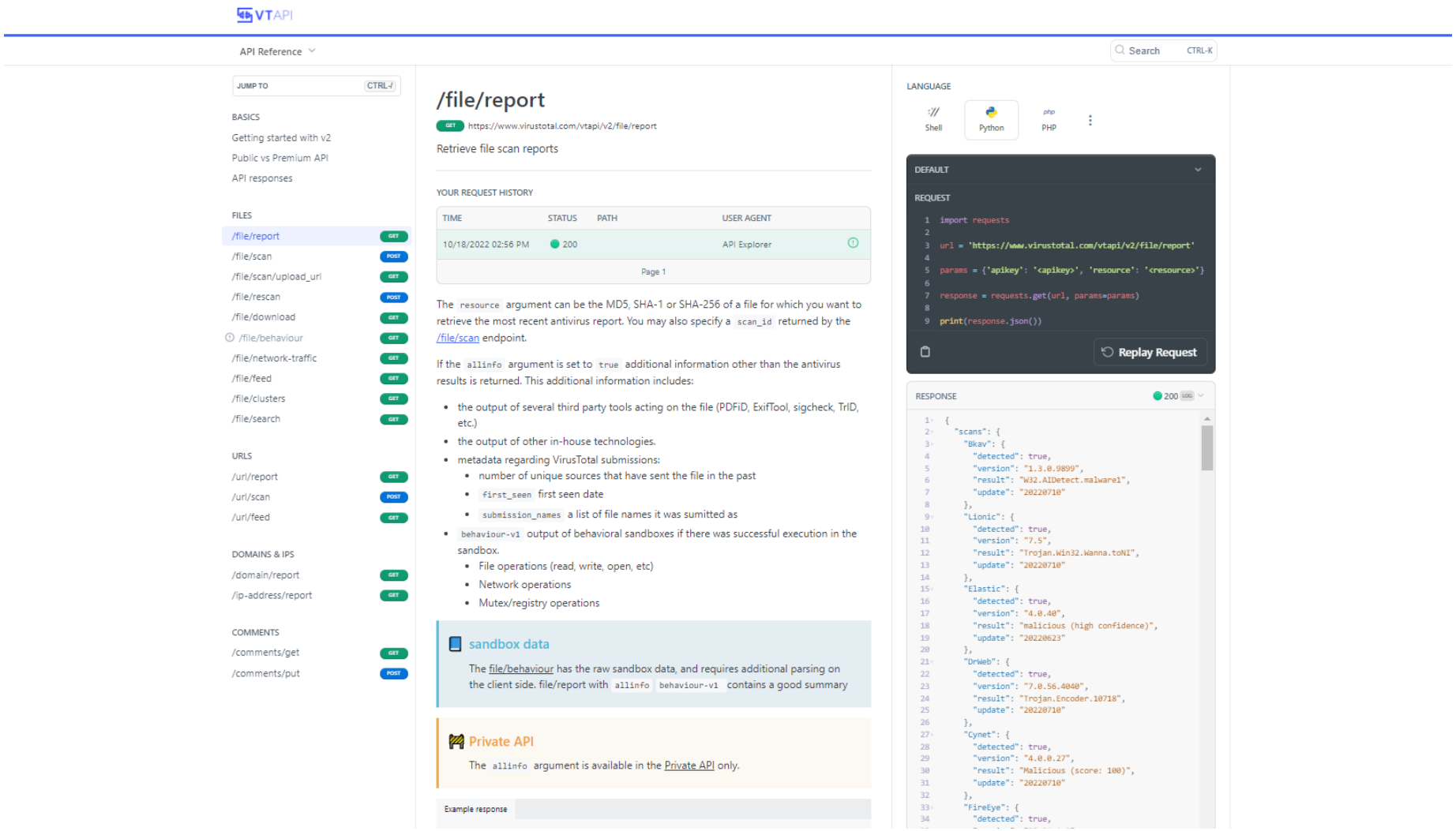
RCTS CERT

CERT RCTS

https://www.virustotal.com/



VTAPI - HTTPS://DEVELOPERS.VIRUSTOTAL.COM/V2.0/



HTTPS://WWW.VIRUSTOTAL.COM/

ANÁLISE DE URLS - HTTP://WWW.ATUALIZARCONTA.COM

- **Ao pesquisar pelo URL através do VirusTotal, podemos confirmar que nosso colega está certo em achar que o email seja suspeito?**
  - Sim

- **Qual foi a classificação que o site recebeu dos diferentes vendors?**
  - Phishing e Malicious

- **Quando é que este URL foi submetido para análise pela primeira vez?**
  - 2017-08-19 18:31:17 UTC

ANÁLISE DE URLS

Qual destes dois URLs parece suspeito:

- http://sandk8s30.dlc.zzbm.360es.cn
- https://www.peterclarkllc.com

ANÁLISE DE BINÁRIOS

ChromeSetup.exe

ChromeSetup.exe

ANÁLISE DE BINÁRIOS

LINUX:

ssh sebastiao@193.136.2.x

Password: …

PUTTY:

No campo Host Name (or IP address)

sebastiao@193.136.2.x

ANÁLISE DE BINÁRIOS

Qual é o hash sum SHA256 de cada um dos ficheiros? (sha256sum NomedoFicheiro)

1. 1e7c91dbce7e273ce973bd366df311e3ce5fe47621b2bc13ae0e1e5922811e03
2. cf8533849ee5e82023ad7adbdbd6543cb6db596c53048b1a0c00b3643a72db30

Qual é o nome dos ficheiros sugeridos pelo VirusTotal e o tamanho de cada ficheiro?

1. GoogleUpdateSetup.exe - 1.36 MB
2. EternalRocks.exe – 5.03 MB

ANÁLISE DE BINÁRIOS

Quais são as táticas de Defense Evasion usadas por este malware?

- Masquerading (T1036), Virtualization/Sandbox Evasion (T1497) e Disable or Modify Tools (T1562.001)

Quantos Contacted IP Addresses estão associados com este ficheiro?

- 5

ANÁLISE DE BINÁRIOS

Alguma sandbox detetou o ficheiro como malicioso?

- Não

O ficheiro possui algum tipo de assinatura?

- Sim, Copyright 2018 Google LLC

Quem são os Signers?

- Google LLC e DigiCert

Obrigada!