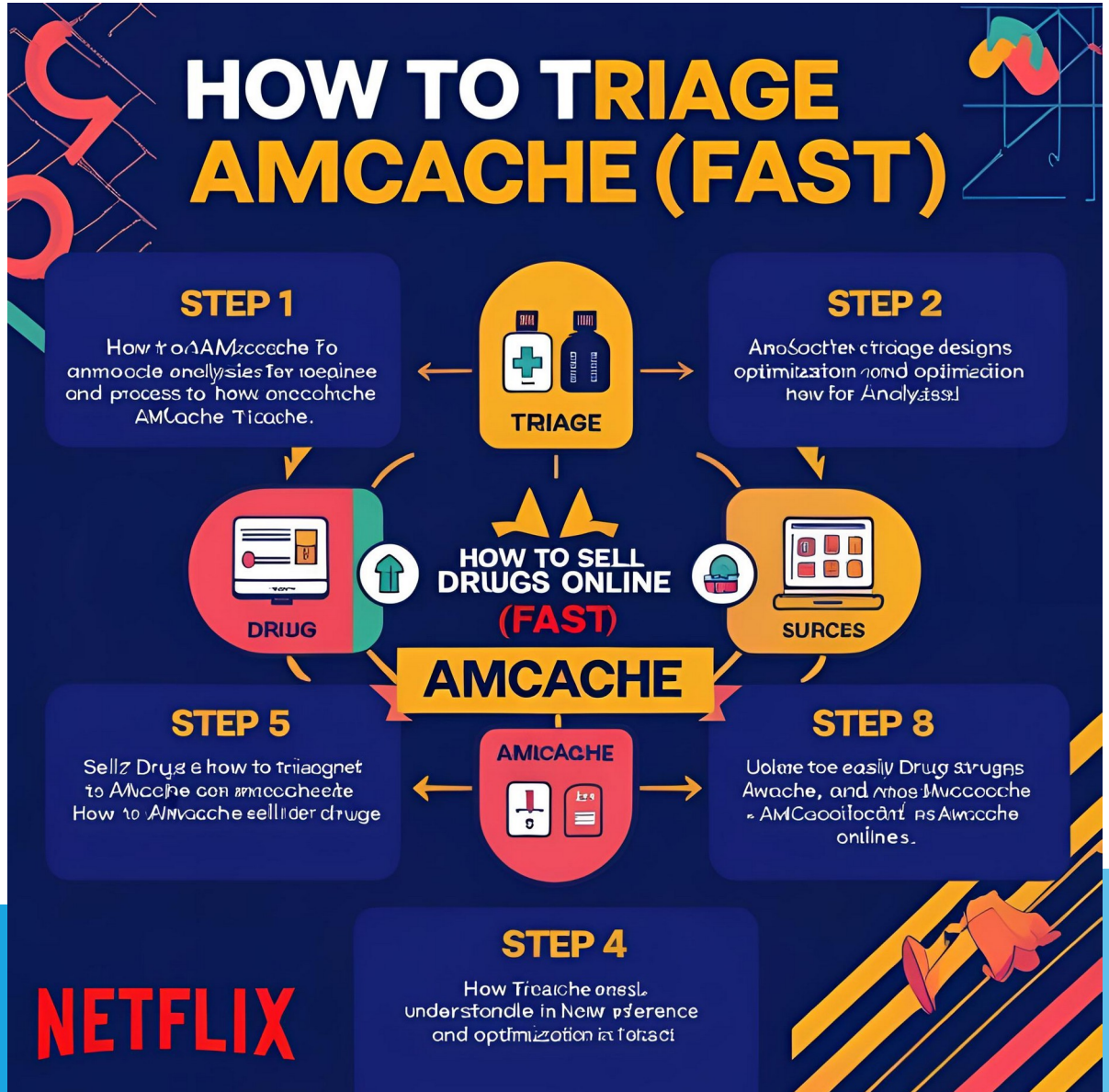
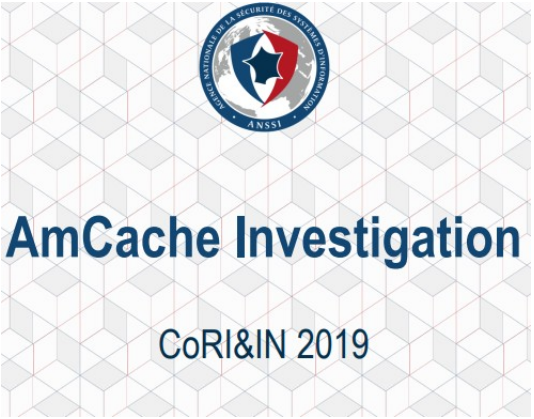

HOW TO TRIAGE AMCACHE (FAST)
STEP 1
STEP 2
TRIAGE
HOW TO SELL DRUGS ONLINE (FAST)
DRUG
SURCES
AMCACHE
AMCACHE
STEP 5
STEP 8
STEP 4
NETFLIX

What is AMCache?

- AMCache is a Windows registry hive that logs information about executed programs
- Stores metadata about binaries:
  - File path
  - SHA-1 hash
  - File version, size
  - First execution date
- Present on modern Windows systems (Amcache.hve)
- C:\Windows\AppCompat\Programs\Amcache.hve



Basic triage approach

- Python script to extract SHA-1 hashes from Amcache.hve
- Idea was simple… and old

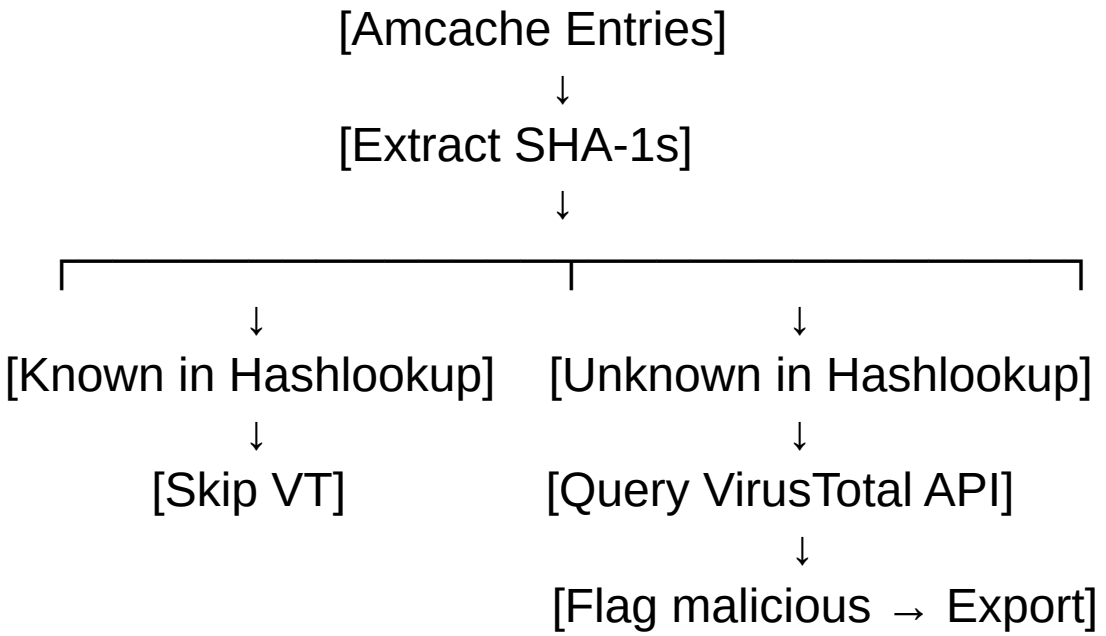
  "I've had this in mind for years — but never scripted it properly"
- Based on:
  - https://github.com/cristianzsh/amcache-evilhunter
  - python3 amcache_evilhunter.py -i path/to/Amcache.hve [OPTIONS]

[Amcache.hve]
↓
[Extract SHA-1s]
↓
[Query VirusTotal API]
↓
[Flag malicious → Export]

[Amcache.hve]
↓
[Extract SHA-1s]
↓
[Send each to VirusTotal]
↓
[Wait... and wait...]

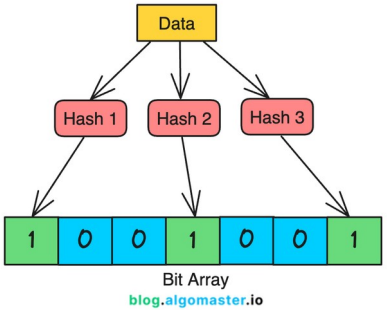
Improvement

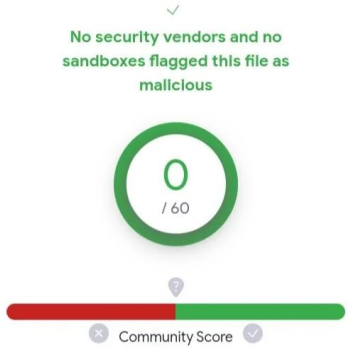
- Why scan calc.exe with 70 AV engines, again?
- Solution: fork and use hashlookup.circl.lu
  - Open-source
  - Uses NSRL and other trusted datasets
  - Fast & anonymous



Way forward

- Better whitelisting
  - Local DB (hashlookup bloom filter)
  - Other trusted whitelist ?
- Beyond VirusTotal (Optional/Complementary):
  - MalwareBazaar, Hybrid Analysis, or Triage APIs
  - Local YARA scan for known malware traits
- Automation Ideas:
  - Turn script into a worker for OpenRELiK
  - Live IR with velociraptor





Key takeaways

- Don’t waste your triage time on calc.exe.
- Github.com/forenser84/amcache-evilhunter