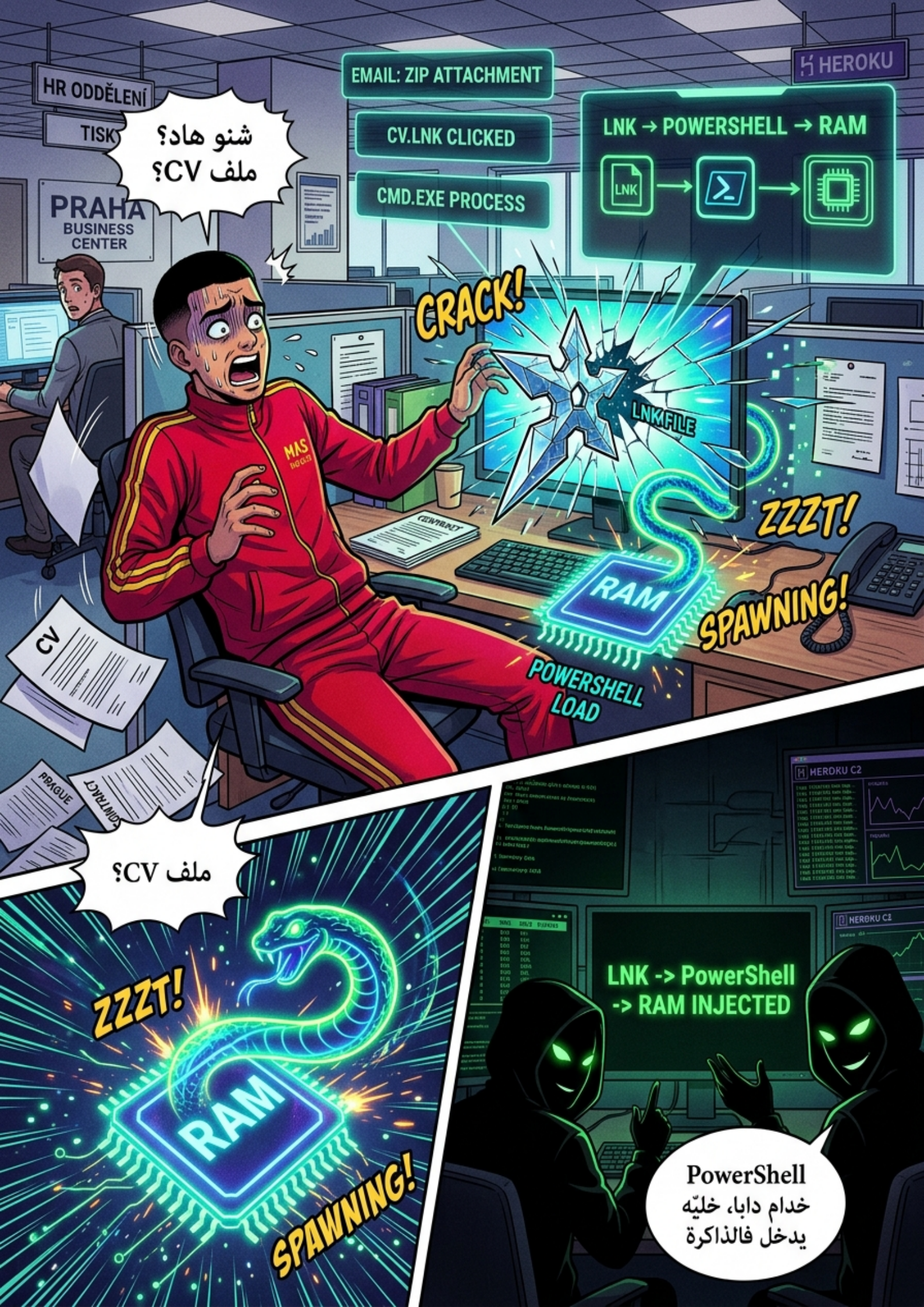
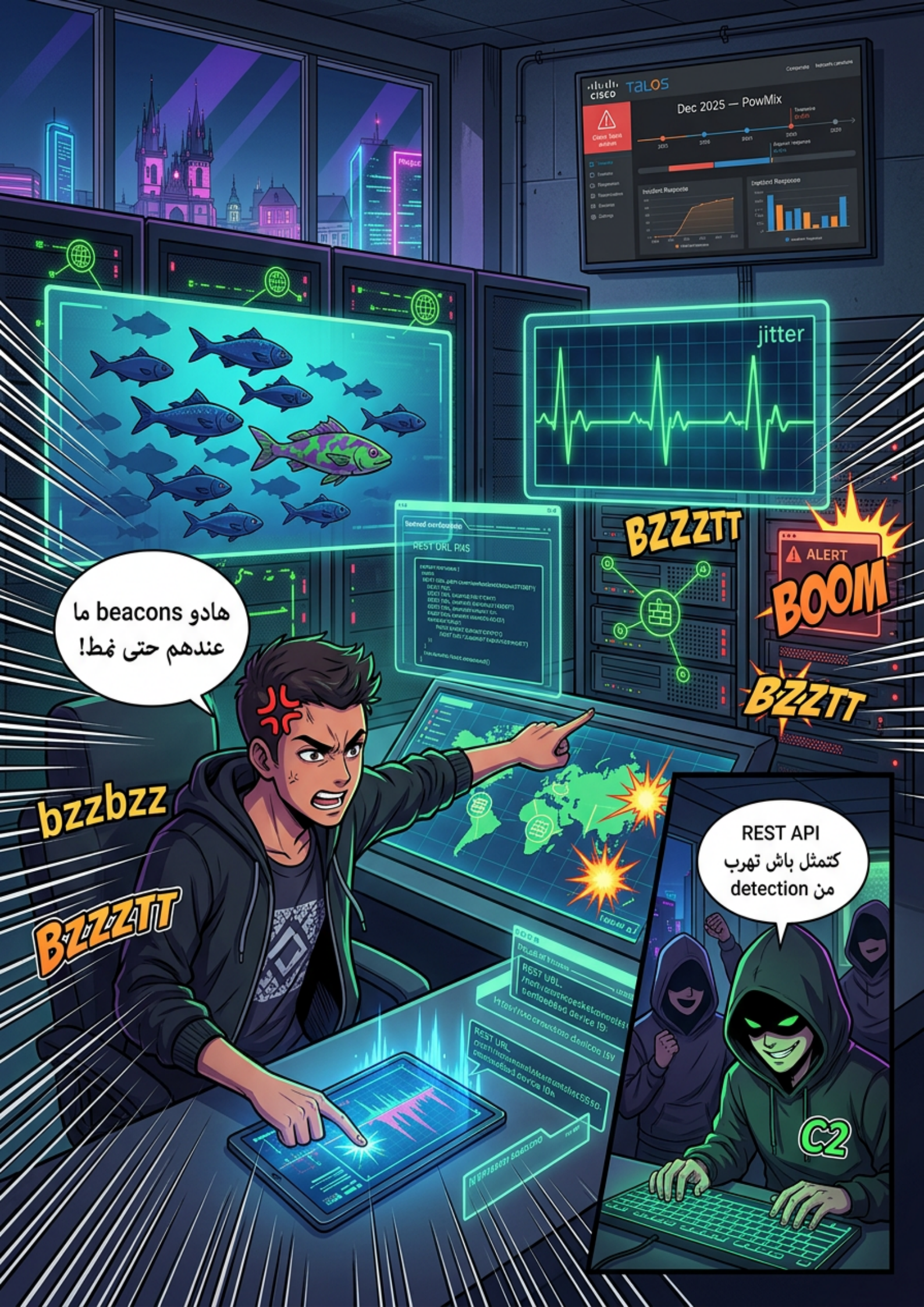
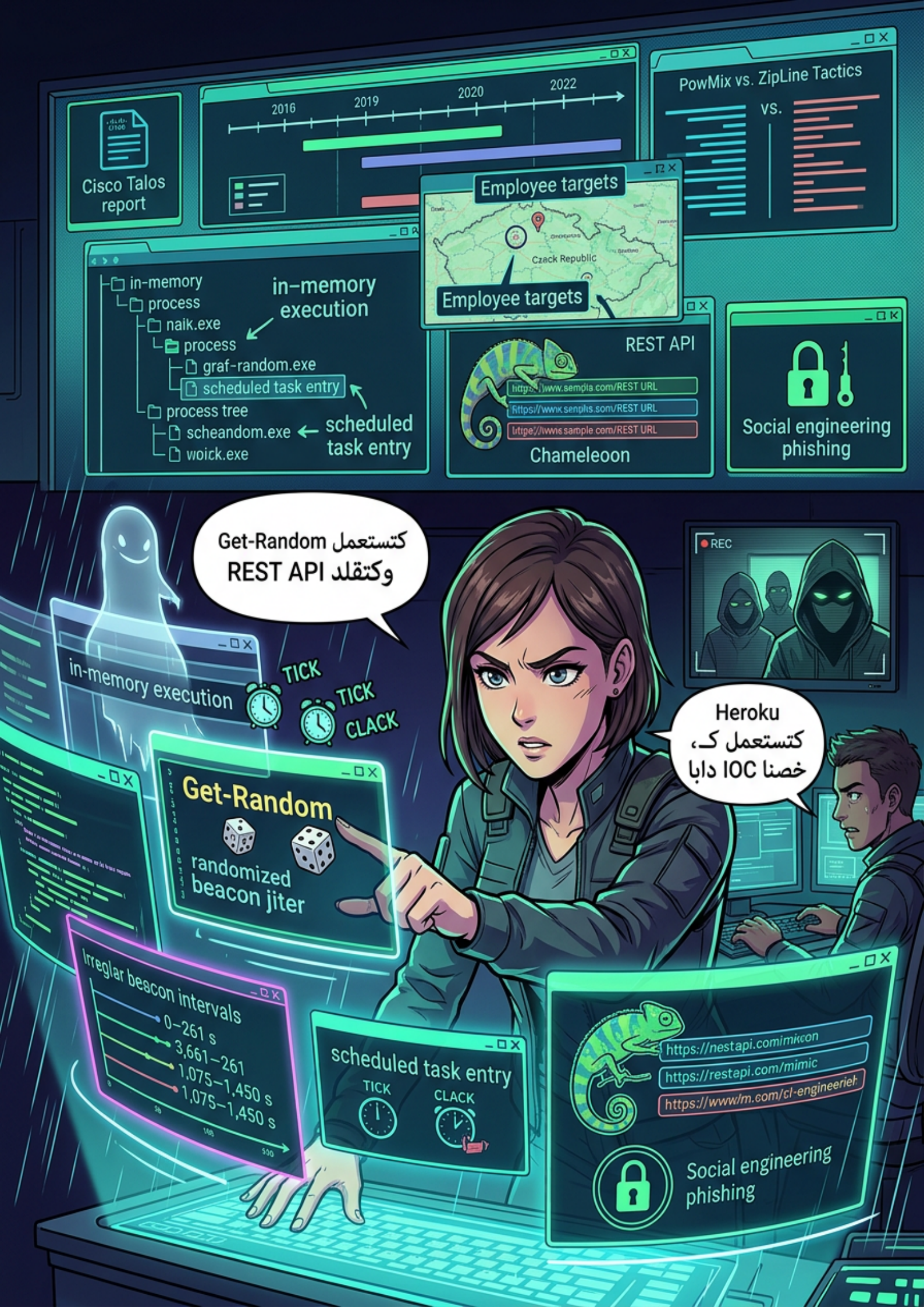
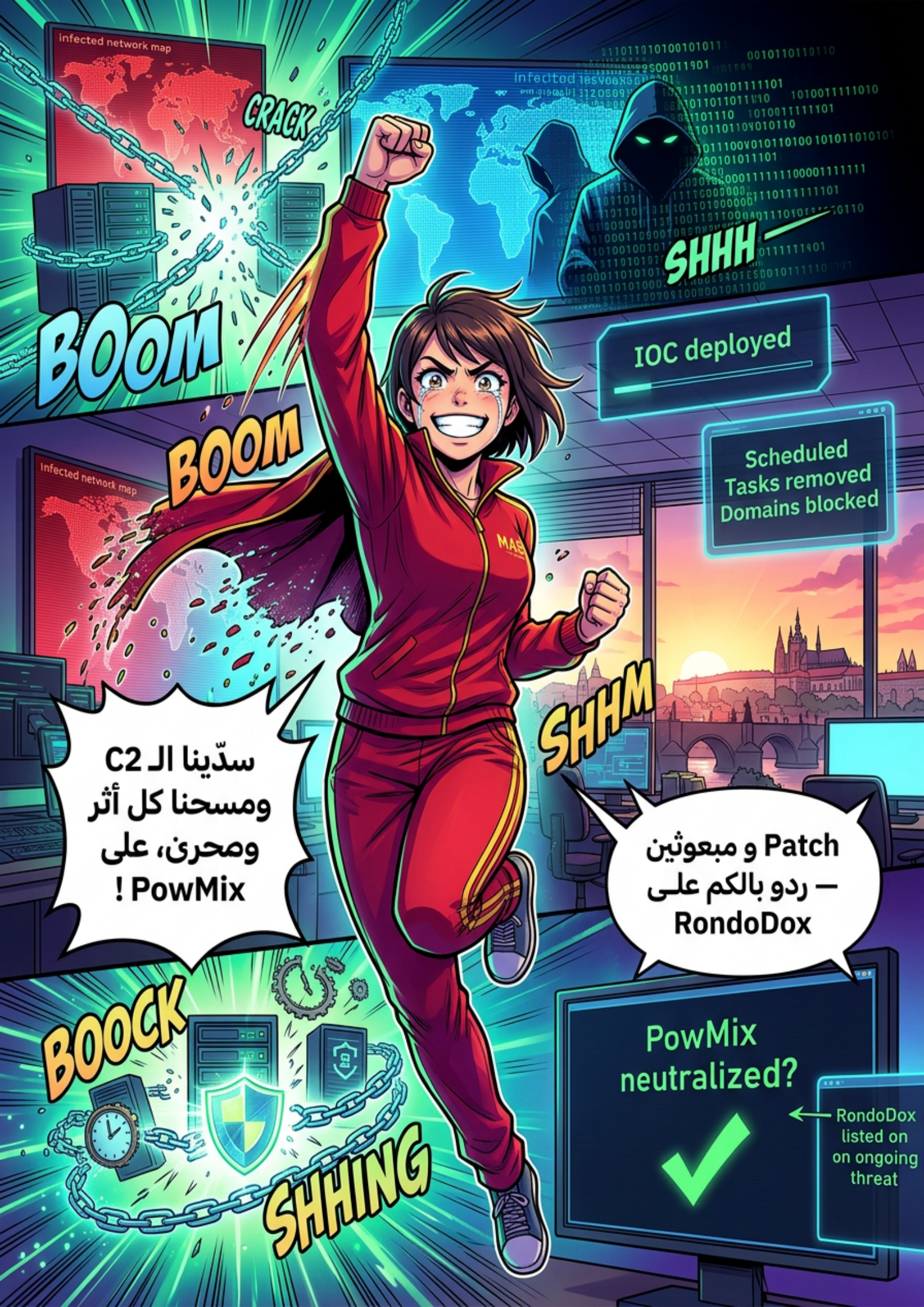

HR ODDĚLENÍ
TISK
PRAHA
BUSINESS CENTER
شنو هاد؟
ملف CV؟
EMAIL: ZIP ATTACHMENT
CV.LNK CLICKED
CMD.EXE PROCESS
HEROKU
LNK → POWERSHELL → RAM
LNK
CRACK!
LNK FILE
ZZZT!
RAM
SPAWNING!
POWERSHELL LOAD
CV
PRAGUE
CONTRACT
ملف CV؟
ZZZT!
RAM
SPAWNING!
HERDKU C2
LNK -> PowerShell
-> RAM INJECTED
PowerShell
خدام دابا، خليّه
يدخل فالذاكرة


CISCO TALOS
Dec 2025 — PowMix
jitter
BZZZTT
ALERT
BOOM
BZZTT
هادو beacons ما
عندهم حتى نمط!
bzzbzz
BZZZTT
REST API
كتمثل باش تهرب
من detection
C2


Cisco Talos report
2016
2019
2020
2022
PowMix vs. ZipLine Tactics
vs.
Employee targets
Czack Republic
Employee targets
in-memory
process
naik.exe
process
graf-random.exe
scheduled task entry
process tree
scheandom.exe
woick.exe
in-memory execution
scheduled task entry
REST API
https://www.sempia.com/REST URL
Https://www.senpis.son/REST URL
https://www.sample.com/REST URL
Chameleoon
Social engineering phishing
Get-Random کتستعمل
REST API وکتقلد
REC
in-memory execution
TICK
TICK
CLACK
Heroku
کتستعمل ک،
خصنا IOC دابا
Get-Random
randomized beacon jiter
Irreglar bescon intervals
0–261 s
3,661–261
1,075–1,450 s
1,075–1,450 s
scheduled task entry
TICK
CLACK
https://nestapi.com/mikcon
https://restepi.com/mimic
https://www/m.com/cl-engineeriel
Social engineering phishing


infected network map
CRACK
BOOM
BOOM
SHHH
IOC deployed
Scheduled Tasks removed Domains blocked
Infected network map
سدّينا الـ C2 ومسحنا كل أثر ومحرن، على PowMix !
SHHM
Patch و مبعوثين — ردو بالكم على RondoDox
BOOCK
SHHING
PowMix neutralized?
RondoDox listed on on ongoing threat