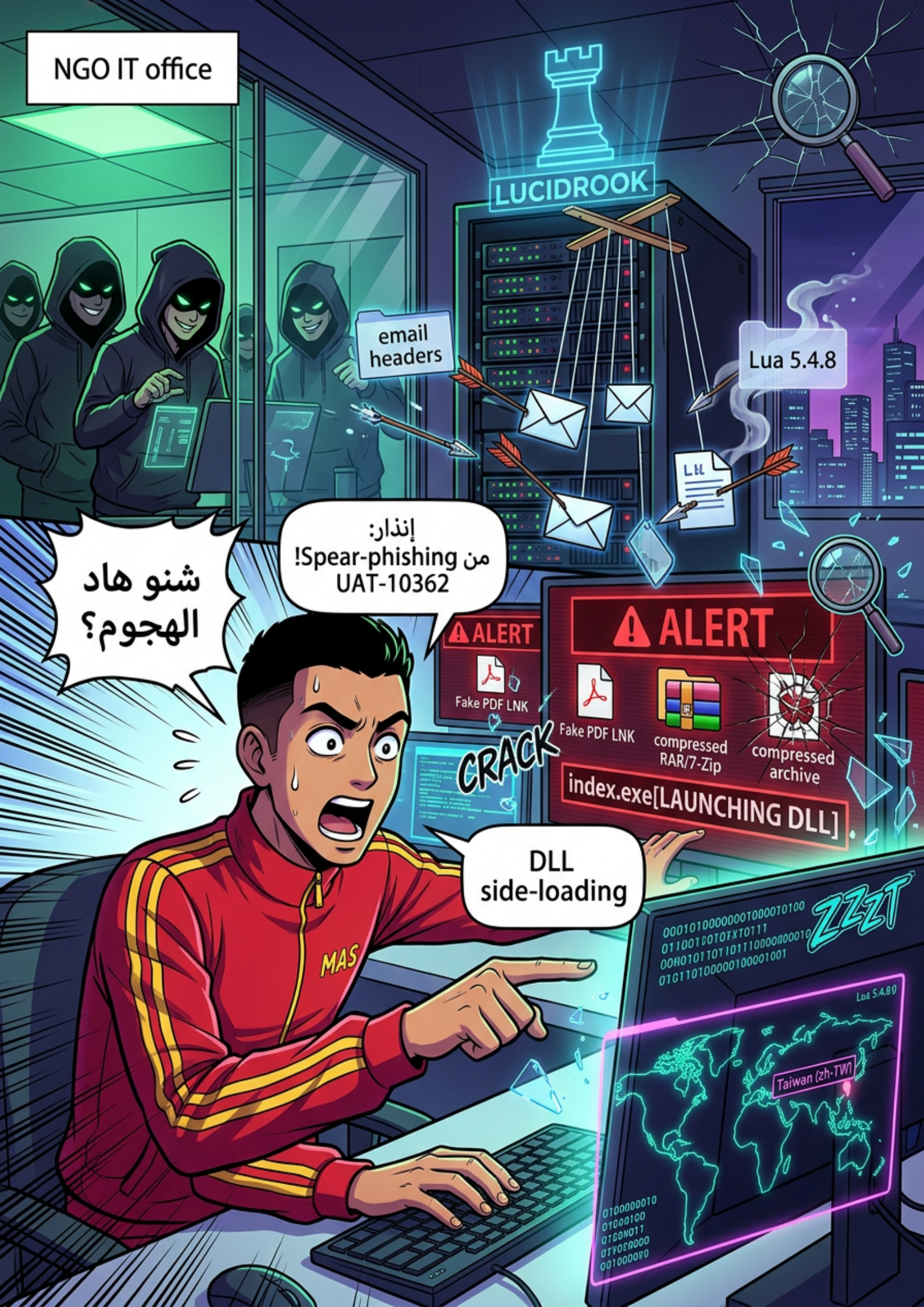
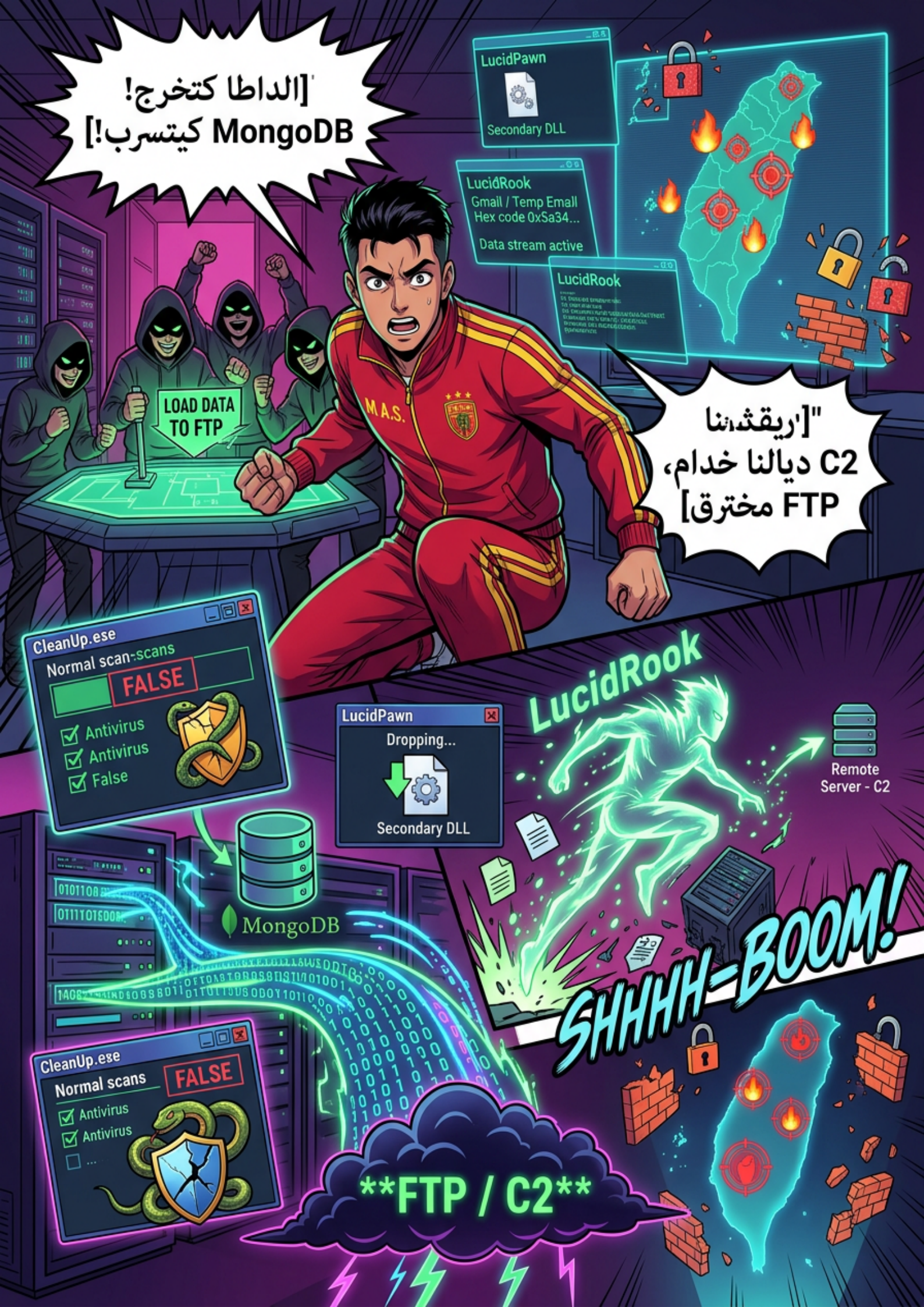
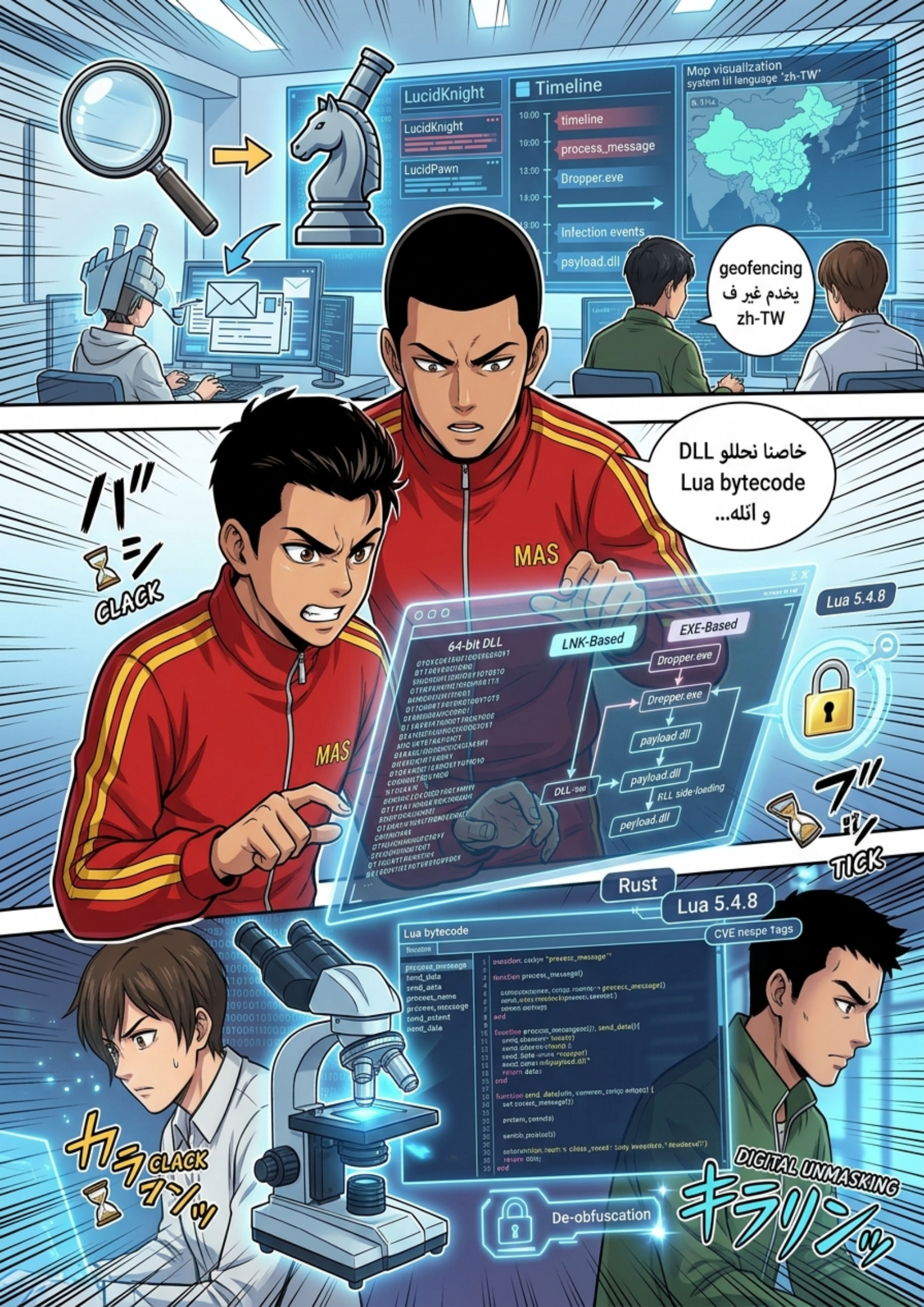
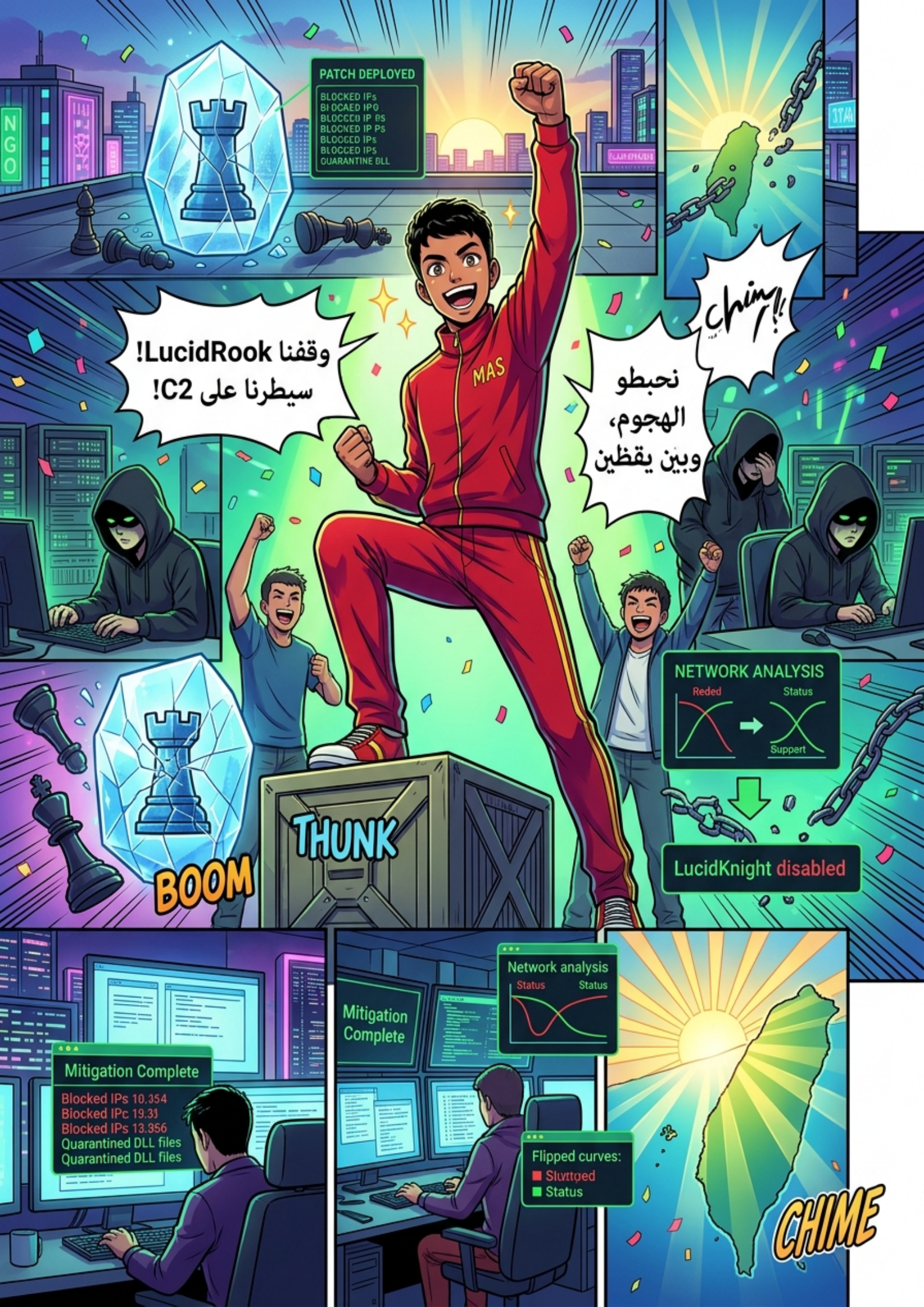

NGO IT office
LUCIDROOK
email headers
Lua 5.4.8
شنو هاد الهجوم؟
إنذار: من Spear-phishing! UAT-10362
ALERT
Fake PDF LNK
CRACK
ALERT
Fake PDF LNK
compressed RAR/7-Zip
compressed archive
index.exe[LAUNCHING DLL]
DLL side-loading
MAS
ZZZT
Lua 5.4.8
Taiwan (zh-TW)


[الداطا كتخرج! MongoDB كيتسرب!]
LucidPawn
Secondary DLL
LucidRook
Gmail / Temp Email
Hex code 0xSa34...
Data stream active
LucidRook
LOAD DATA TO FTP
M.A.S.
"[ريقدتنا C2 ديالنا خدام، FTP مخترق]
CleanUp.ese
Normal scan-scans
FALSE
Antivirus
Antivirus
False
LucidPawn
Dropping...
Secondary DLL
LucidRook
Remote Server - C2
MongoDB
SHHHH-BOOM!
CleanUp.ese
Normal scans
FALSE
Antivirus
Antivirus
FTP / C2


LucidKnight
LucidKnight
LucidPawn
Timeline
timeline
process_message
Bropper.exe
Infection events
psyload.dll
Mop visualization
system lil language 'zh-TW'
geofencing
يخدم غير ف
zh-TW
خاصنا نحللو DLL
Lua bytecode
و اتله...
MAS
MAS
バシ
CLACK
64-bit DLL
LNK-Based
EXE-Based
Dropper.eve
Drepper.exe
payload.dll
payload.dll
RLL side-loading
peyload.dll
Lua 5.4.8
TICK
Rust
Lua 5.4.8
Lua bytecode
CVE nespe tags
CLACK
De-obfuscation
DIGITAL UNMASKING
キラリンッ


PATCH DEPLOYED
BLOCKED IPs
BLOCKED IPs
BLOCKED IPs
BLOCKED IPs
BLOCKED IPs
QUARANTINE DLL
وقفنا LucidRook!
سيطرنا على C2!
نحبطو الهجوم، وبين يقظين
Chim!!
MAS
NETWORK ANALYSIS
Reded
Status
Suppert
LucidKnight disabled
BOOM
THUNK
Mitigation Complete
Blocked IPs 10.354
Blocked IPs 19.31
Blocked IPs 13.356
Quarantined DLL files
Quarantined DLL files
Mitigation Complete
Network analysis
Status
Status
Flipped curves:
Status
CHIME