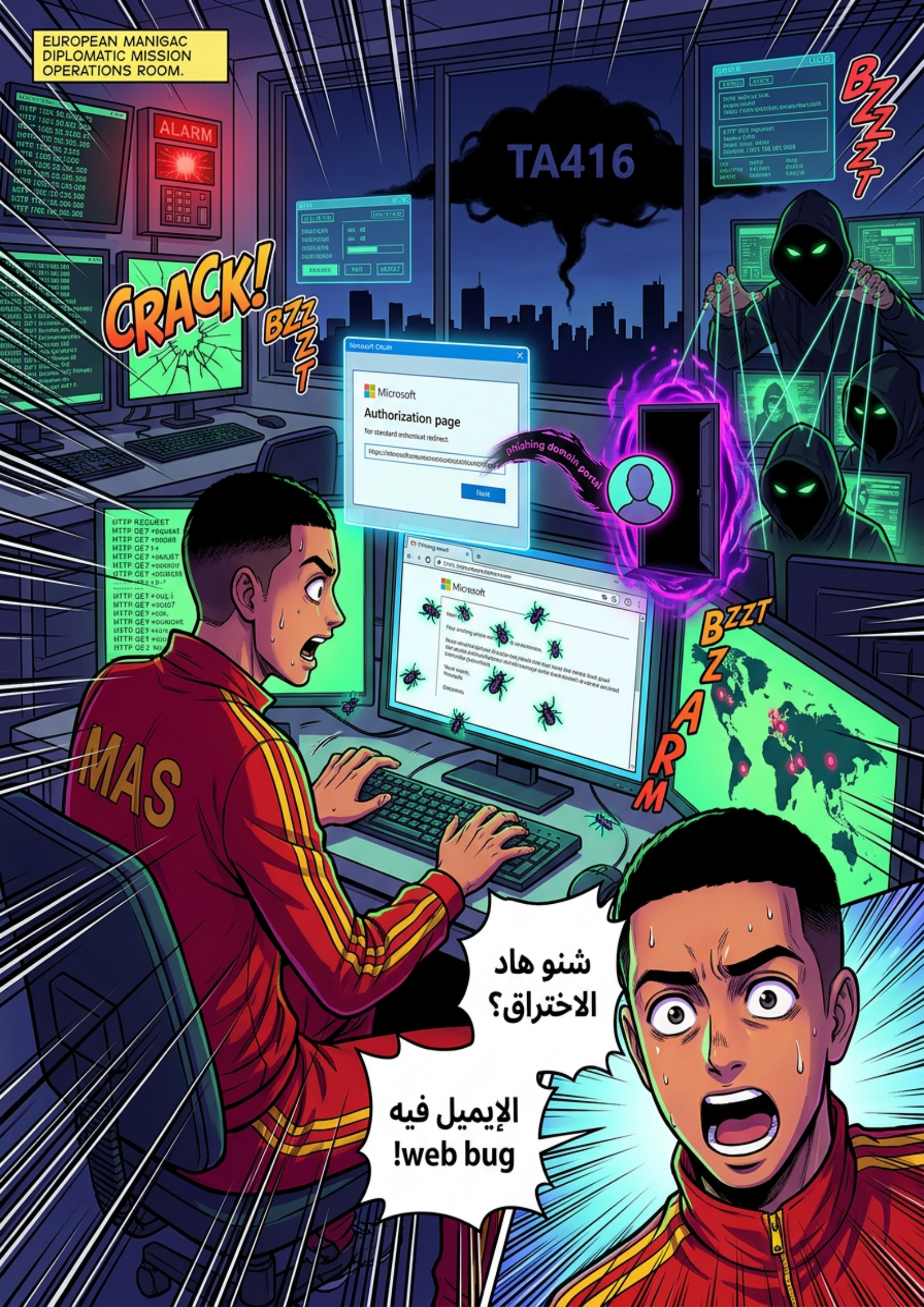
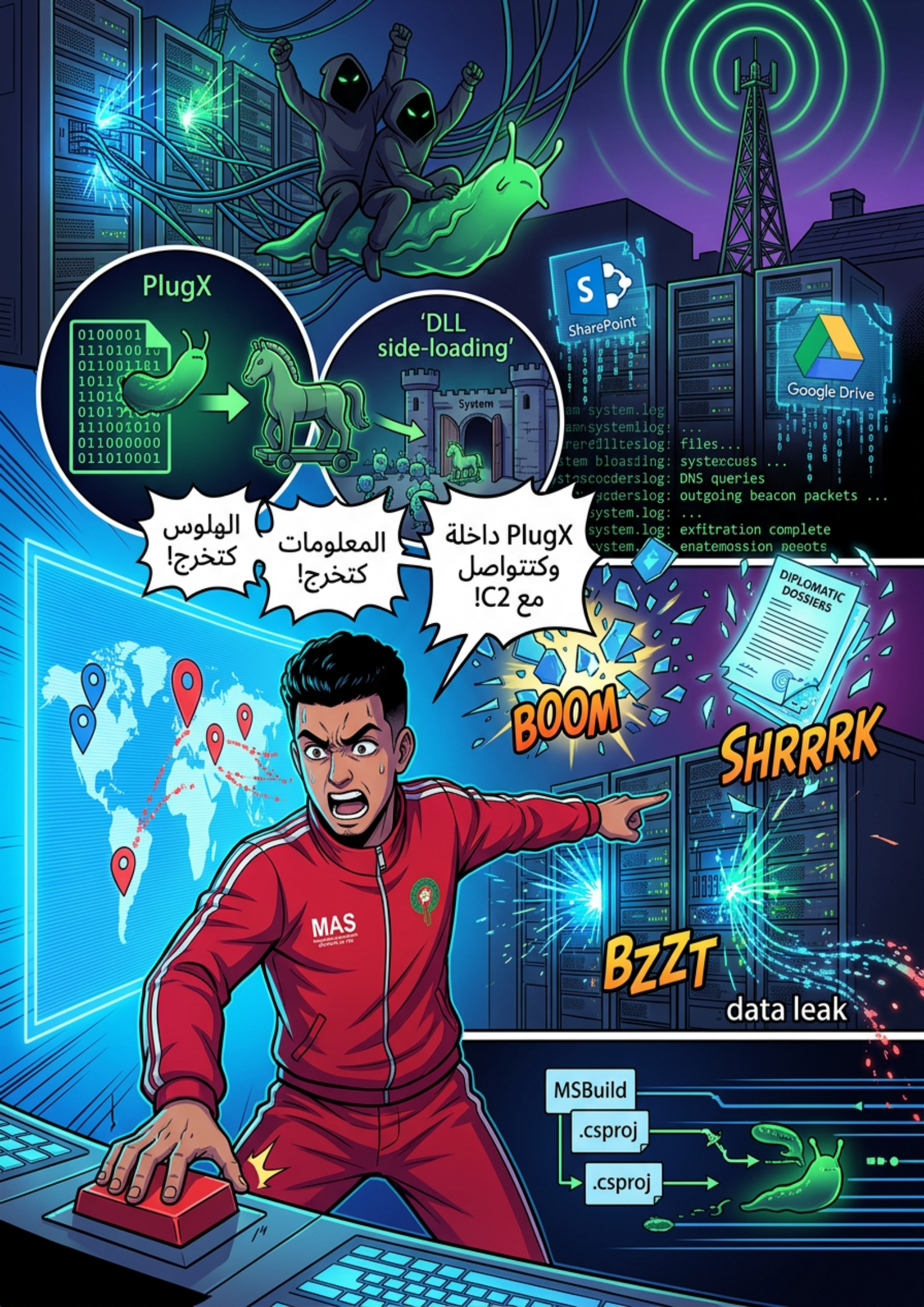
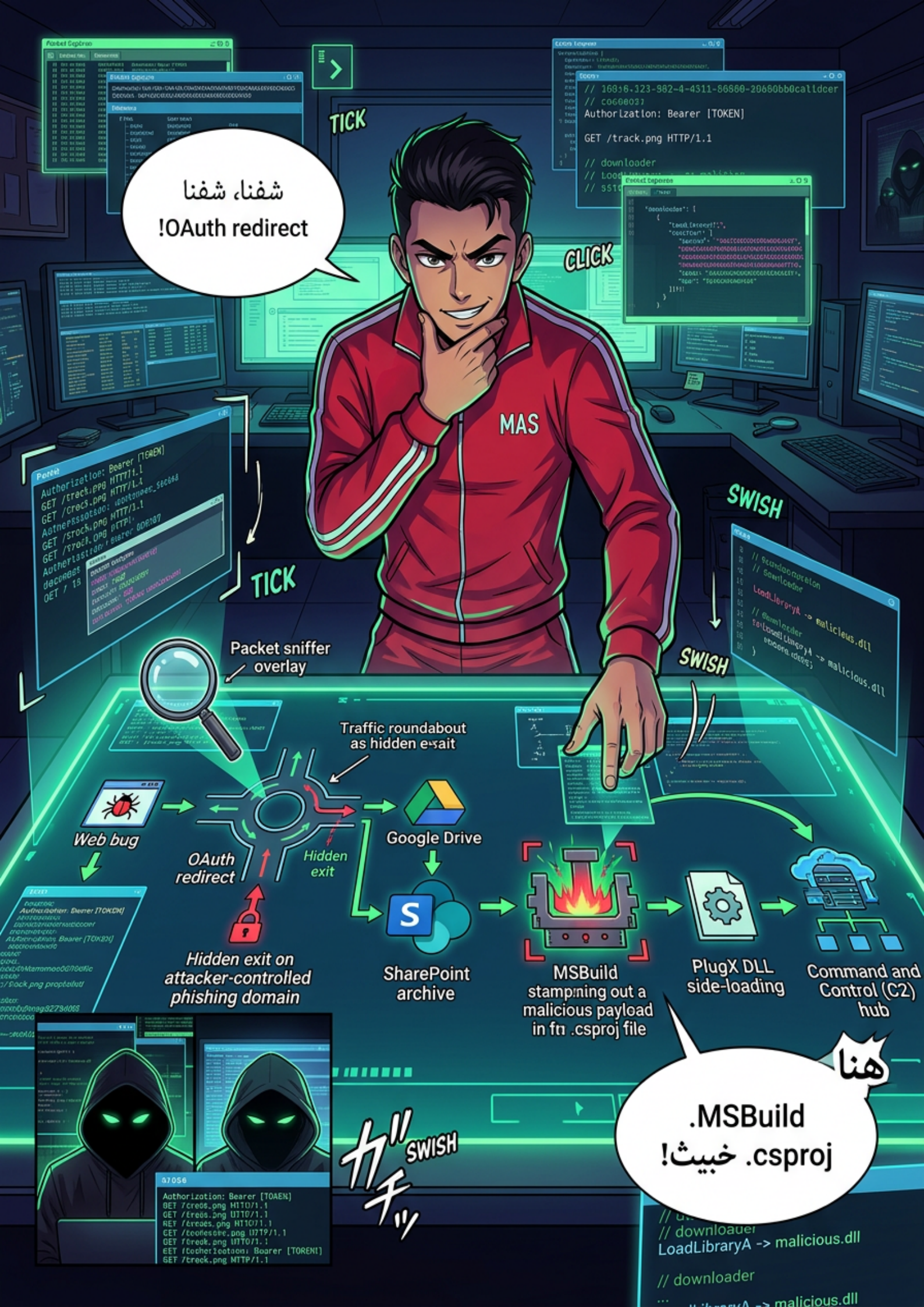
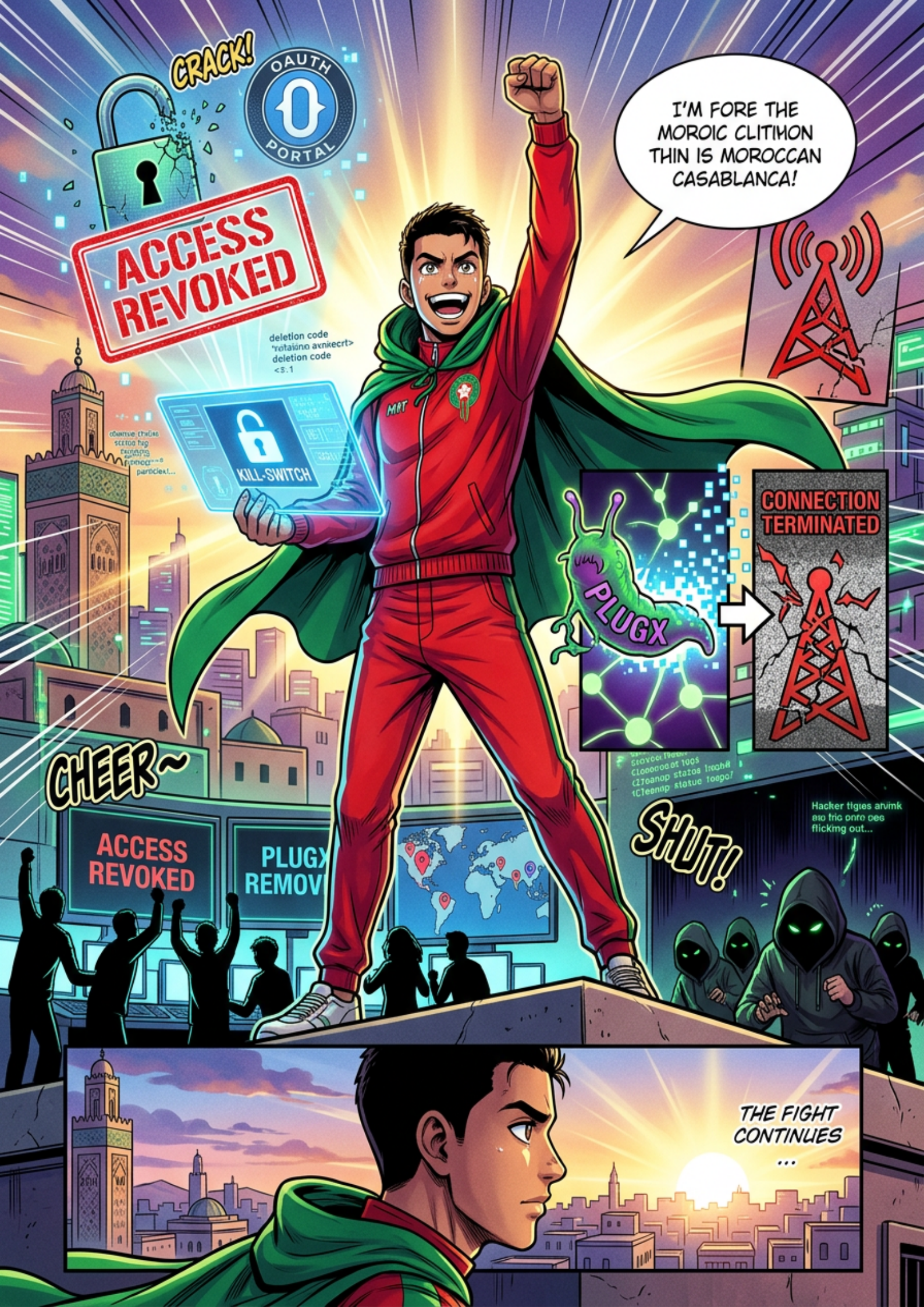

EUROPEAN MANIGAC DIPLOMATIC MISSION OPERATIONS ROOM.
ALARM
TA416
BZZZT
CRACK!
BZZT
Microsoft
Authorization page
phishing domain portal
Microsoft
BZZT
ALARM
MAS
شنو هاد الاختراق؟
الإيميل فيه web bug!


PlugX
0100001
11101001
01100111
1011
11010
01013
11001010
011000000
011010001
'DLL side-loading'
System
SharePoint
Google Drive
system.log
systemlog:
files...
systexcuss ...
DNS queries
outgoing beacon packets ...
system.log: ...
system.log: exfitration complete
الهلوس كتخرج!
المعلومات كتخرج!
PlugX داخلة وكتتواصل مع C2!
DIPLOMATIC DOSSIERS
BOOM
SHRRRK
BZZT
data leak
MAS
MSBuild
.csproj
.csproj


TICK
شفنا، شفنا
!OAuth redirect
CLICK
MAS
SWISH
TICK
SWISH
Packet sniffer overlay
Traffic roundabout as hidden exit
Web bug
OAuth redirect
Hidden exit
Google Drive
Hidden exit on attacker-controlled phishing domain
SharePoint archive
MSBuild stamping out a malicious payload in the .csproj file
PlugX DLL side-loading
Command and Control (C2) hub
هنا
.MSBuild
.csproj خبيث!
SWISH
LoadLibraryA -> malicious.dll
// downloader


CRACK!
OAUTH
PORTAL
ACCESS REVOKED
I'M FORE THE MOROIC CLITIHON THIN IS MOROCCAN CASABLANCA!
deletion code
deletion code
KILL-SWITCH
PLUGX
CONNECTION TERMINATED
CHEER~
ACCESS REVOKED
PLUGX REMOV
SHUT!
THE FIGHT CONTINUES ...