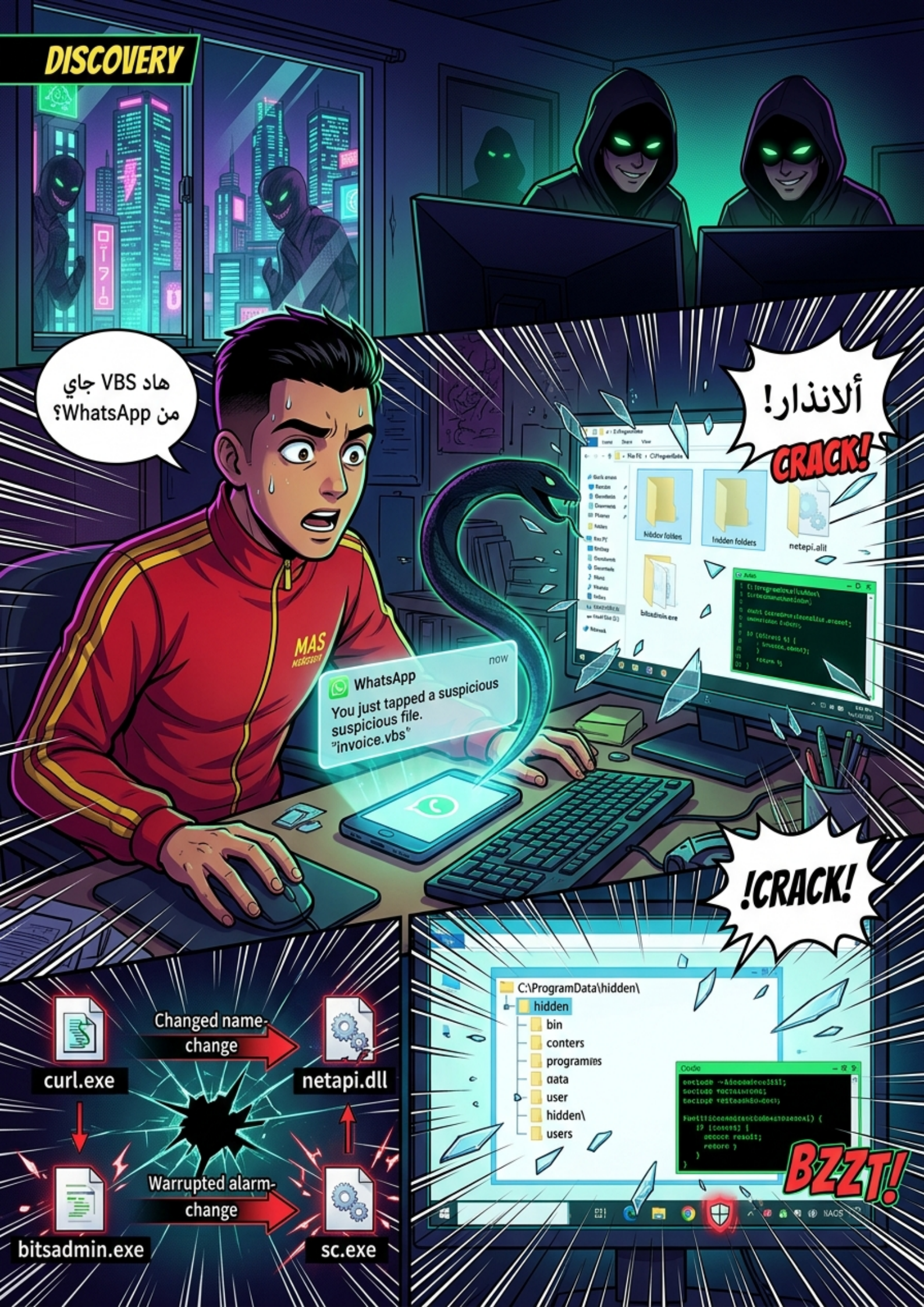
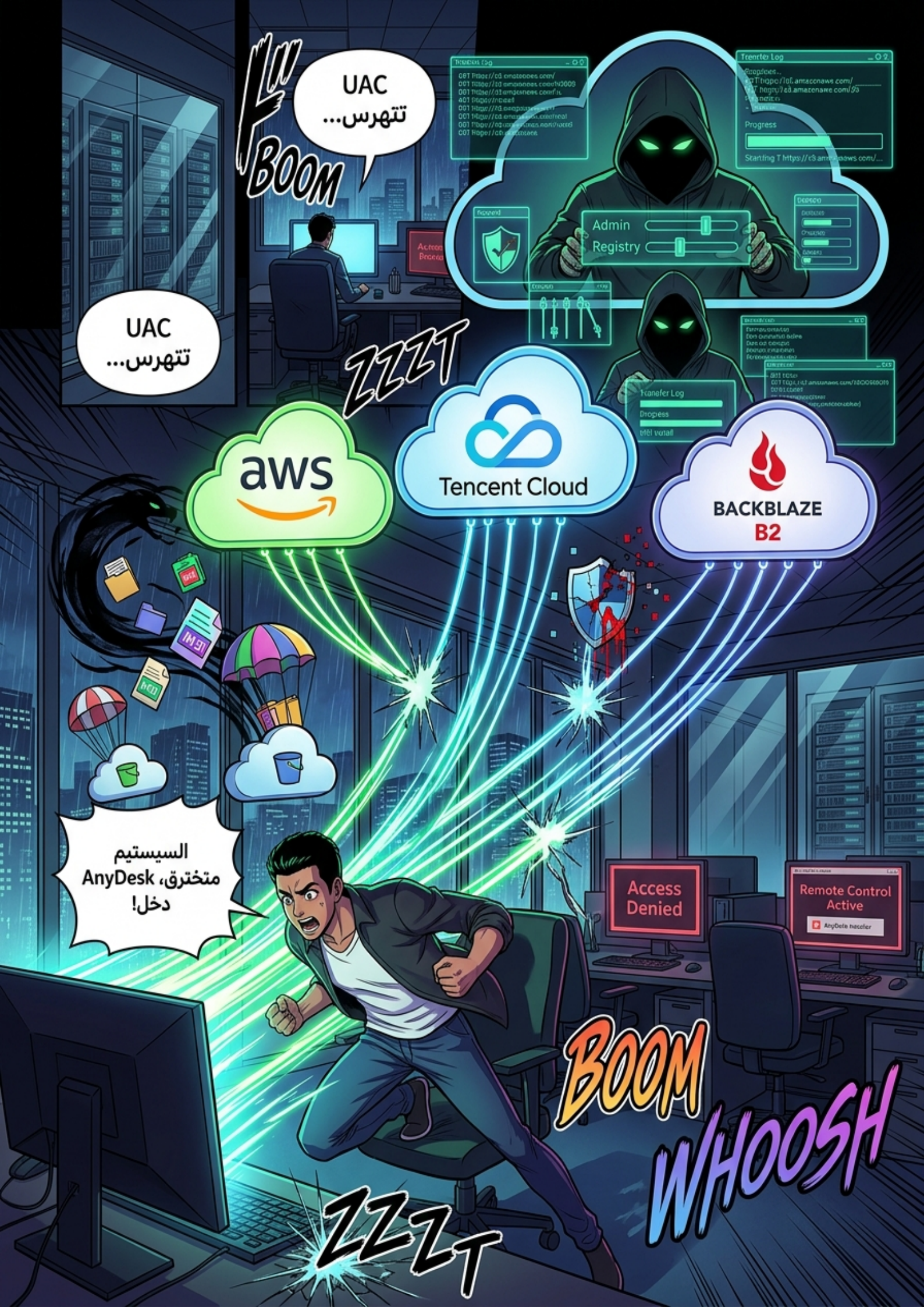
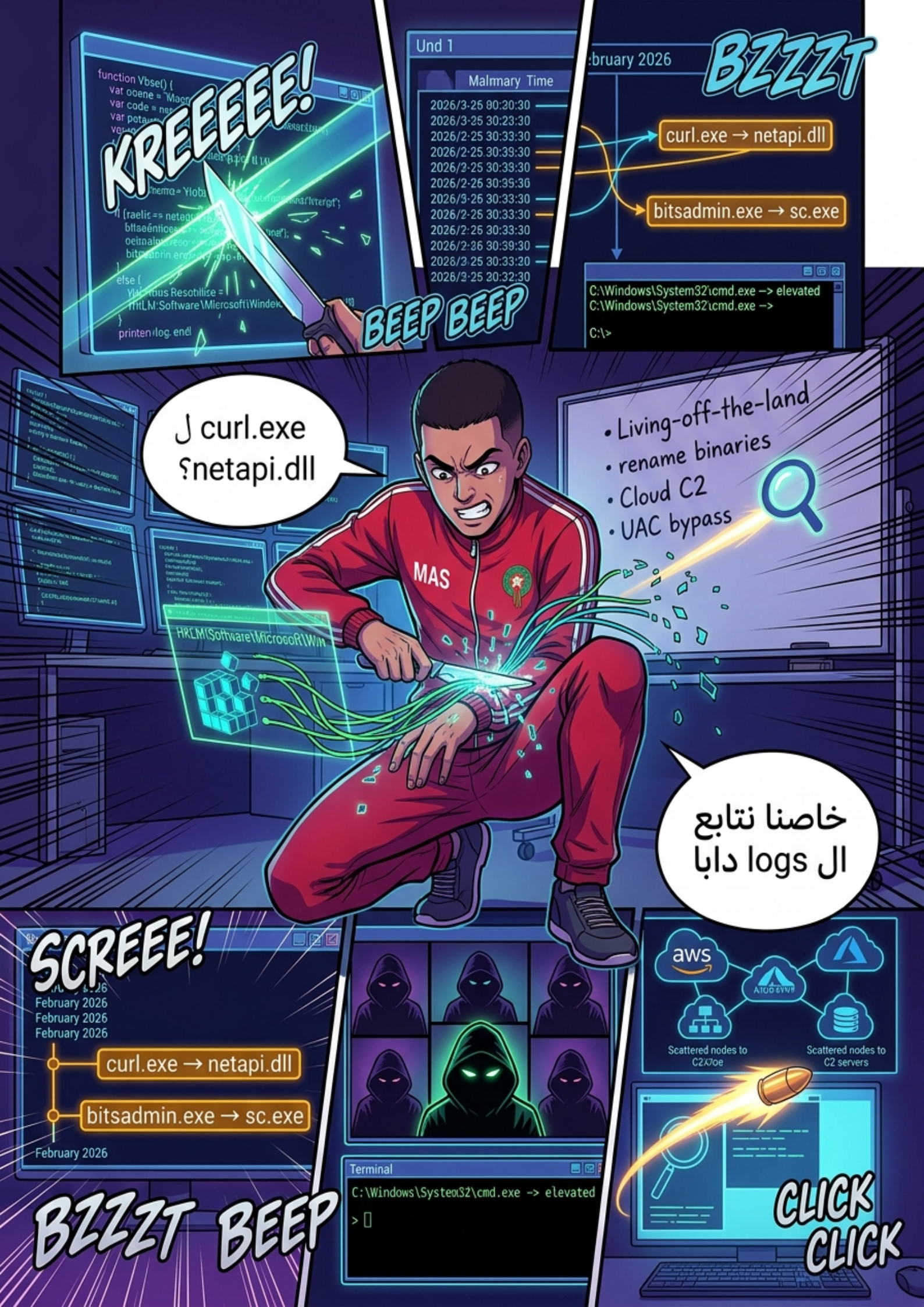
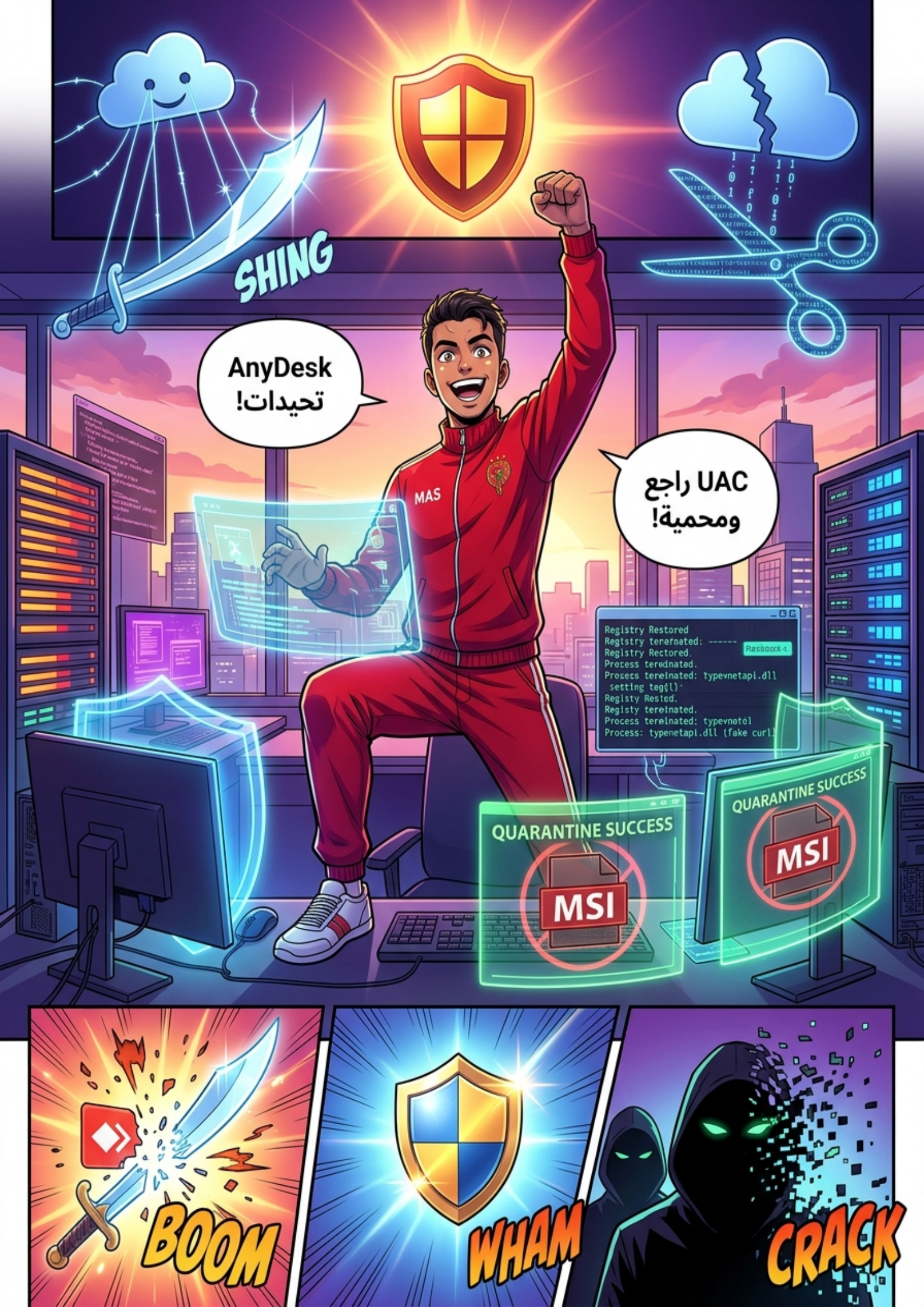

DISCOVERY
هاد VBS جاي من WhatsApp؟
ألانذار!
CRACK!
hidden folders
hidden folders
netapi.alit
bitsadmin.exe
MAS
now
WhatsApp
You just tapped a suspicious suspicious file. "invoice.vbs"
!CRACK!
C:\ProgramData\hidden\
hidden
bin
conters
programms
data
user
hidden\
users
Code
BZZT!
curl.exe
Changed name-change
netapi.dll
Warrupted alarm-change
bitsadmin.exe
sc.exe


UAC تتهرس...
BOOM
UAC تتهرس...
ZZZT
Admin
Registry
Transfer Log
Progress
aws
Tencent Cloud
BACKBLAZE B2
السيستيم متخترق، AnyDesk دخل!
Access Denied
Remote Control Active
BOOM
WHOOSH
ZZZT


KREEEEE!
BEEP BEEP
BZZZT
curl.exe → netapi.dll
bitsadmin.exe → sc.exe
C:\Windows\System32\cmd.exe -> elevated
curl.exe
netapi.dll
• Living-off-the-land
• rename binaries
• Cloud C2
• UAC bypass
MAS
خاصنا نتابع
ال logs دابا
SCREEE!
February 2026
February 2026
February 2026
curl.exe → netapi.dll
bitsadmin.exe → sc.exe
February 2026
BZZZT BEEP
aws
Scattered nodes to C2
Scattered nodes to C2 servers
Terminal
C:\Windows\System32\cmd.exe -> elevated
CLICK CLICK


SHING
AnyDesk
تحيدات!
UAC راجع
ومحمية!
MAS
Registry Restored
Process terminated: typevnetapi.dll
Registry Restored.
Process terminated.
Process terminated: typevnetol
Process: typenetapi.dll (fake curl)
QUARANTINE SUCCESS
MSI
QUARANTINE SUCCESS
MSI
BOOM
WHAM
CRACK