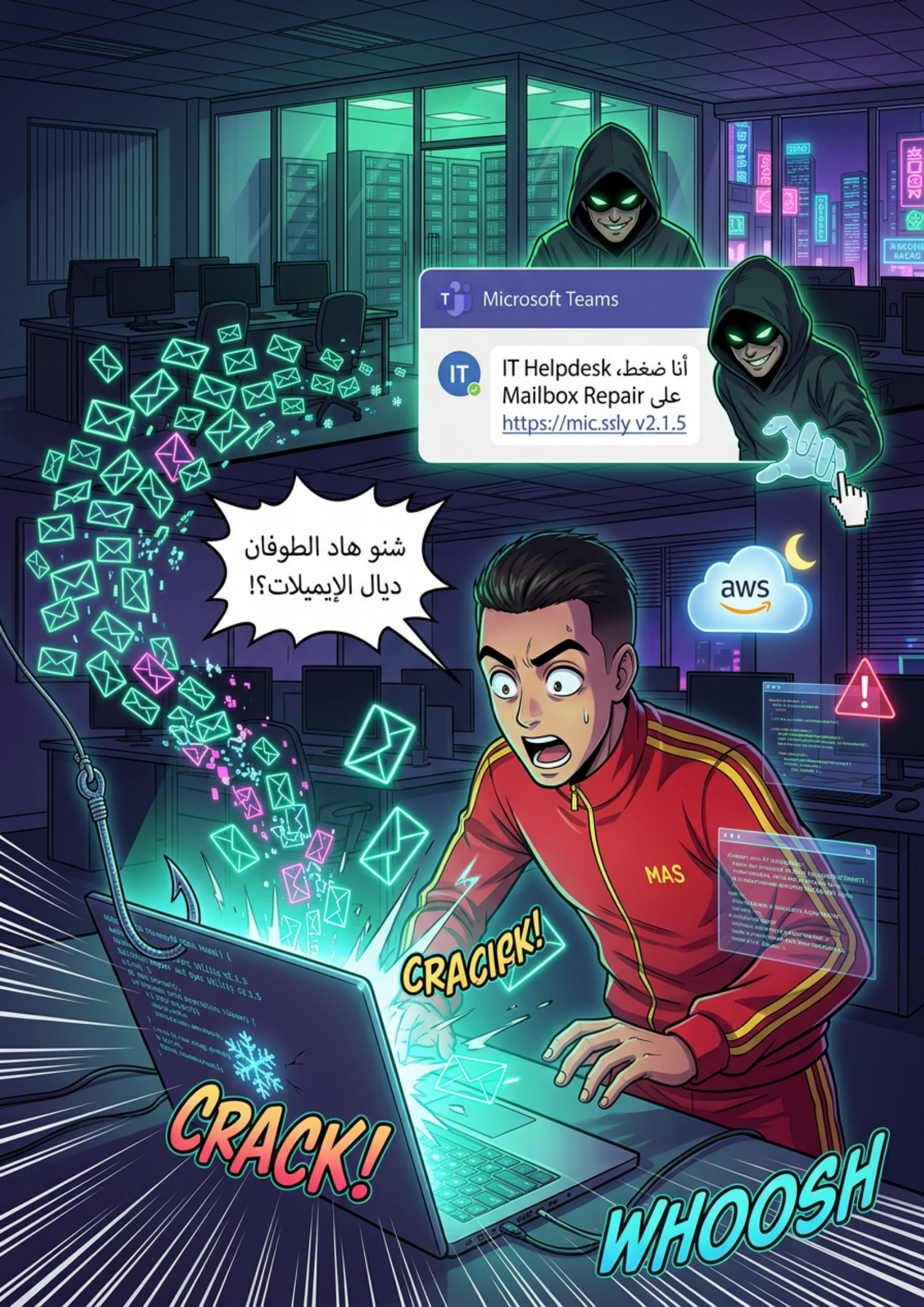
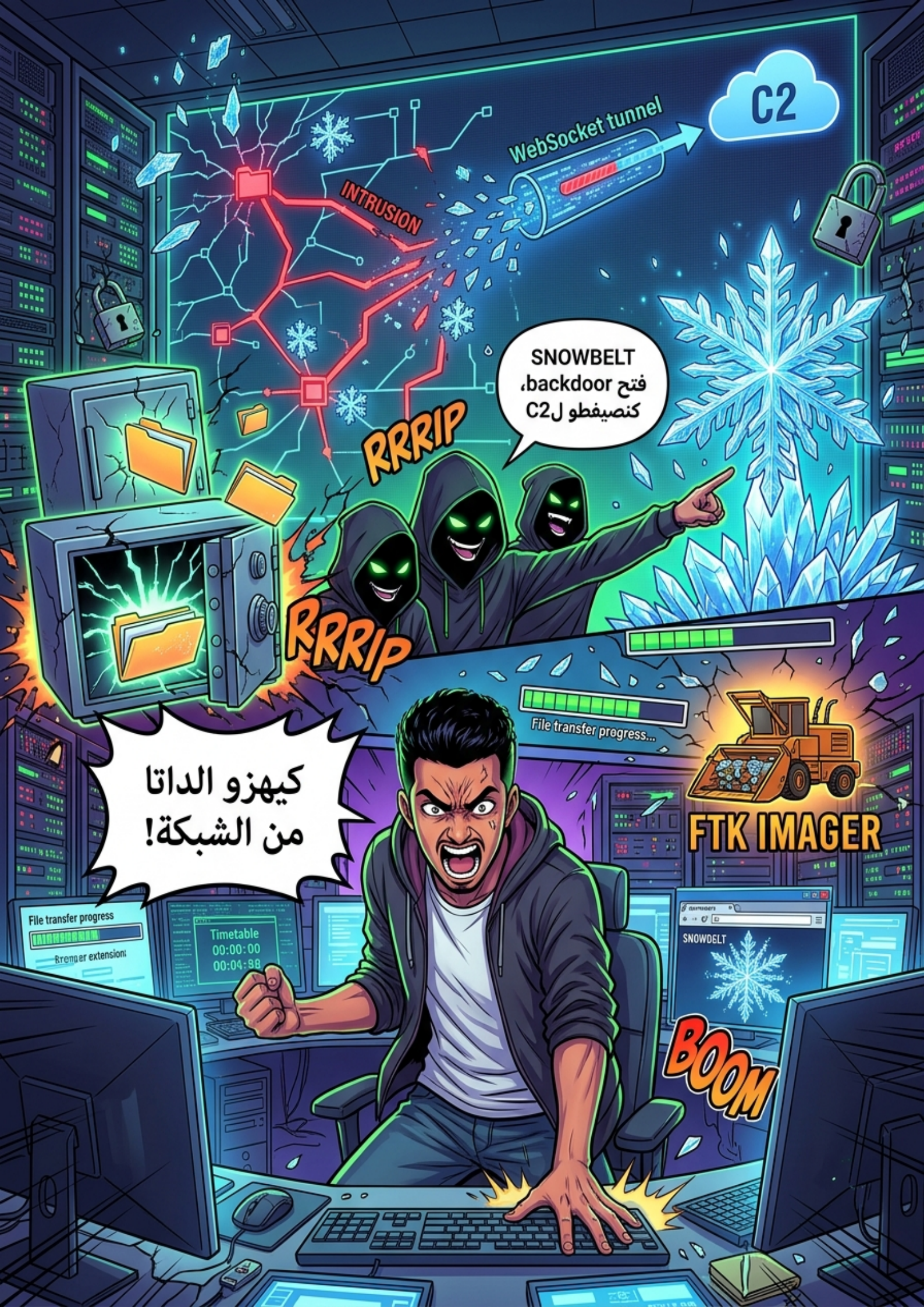
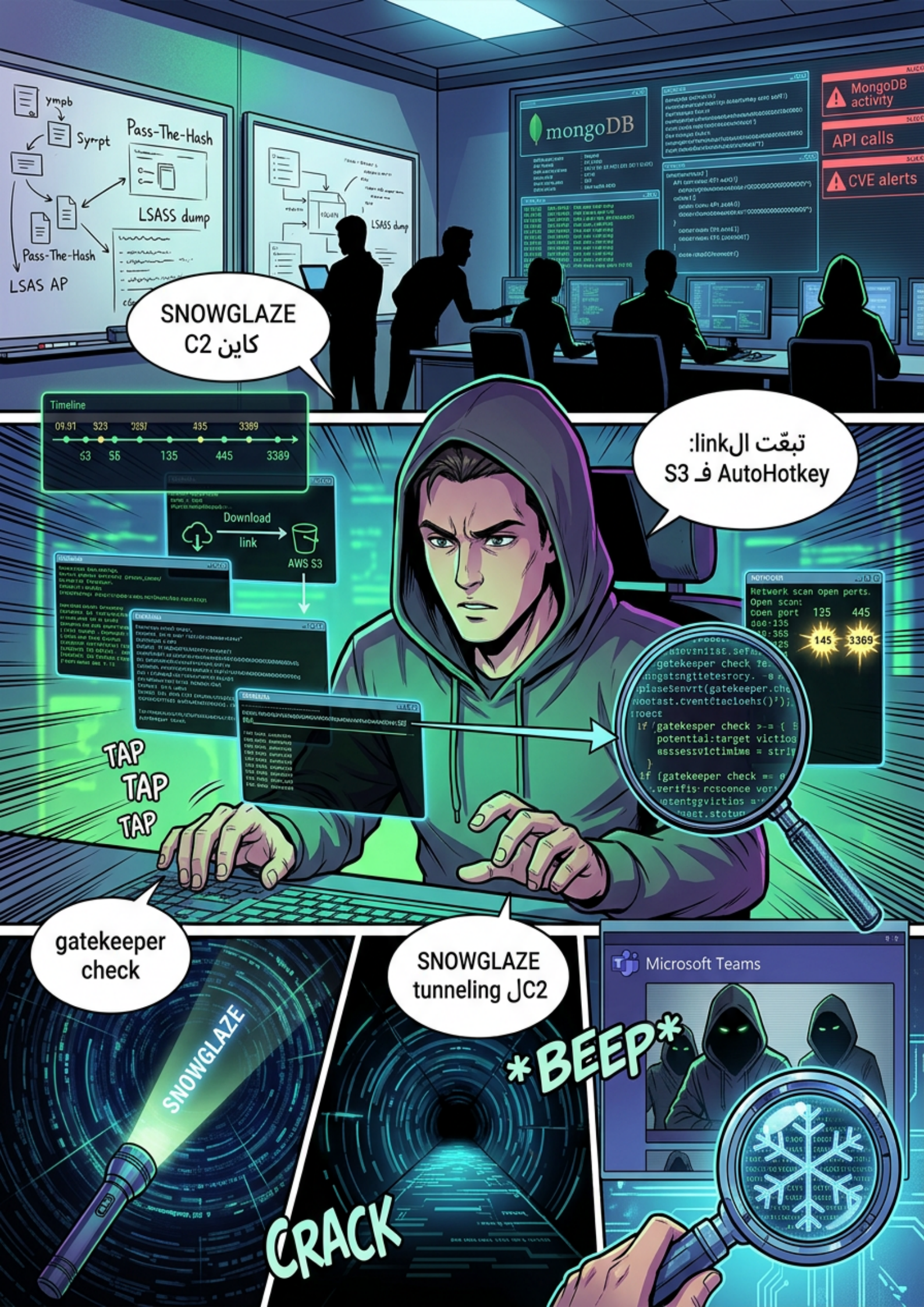
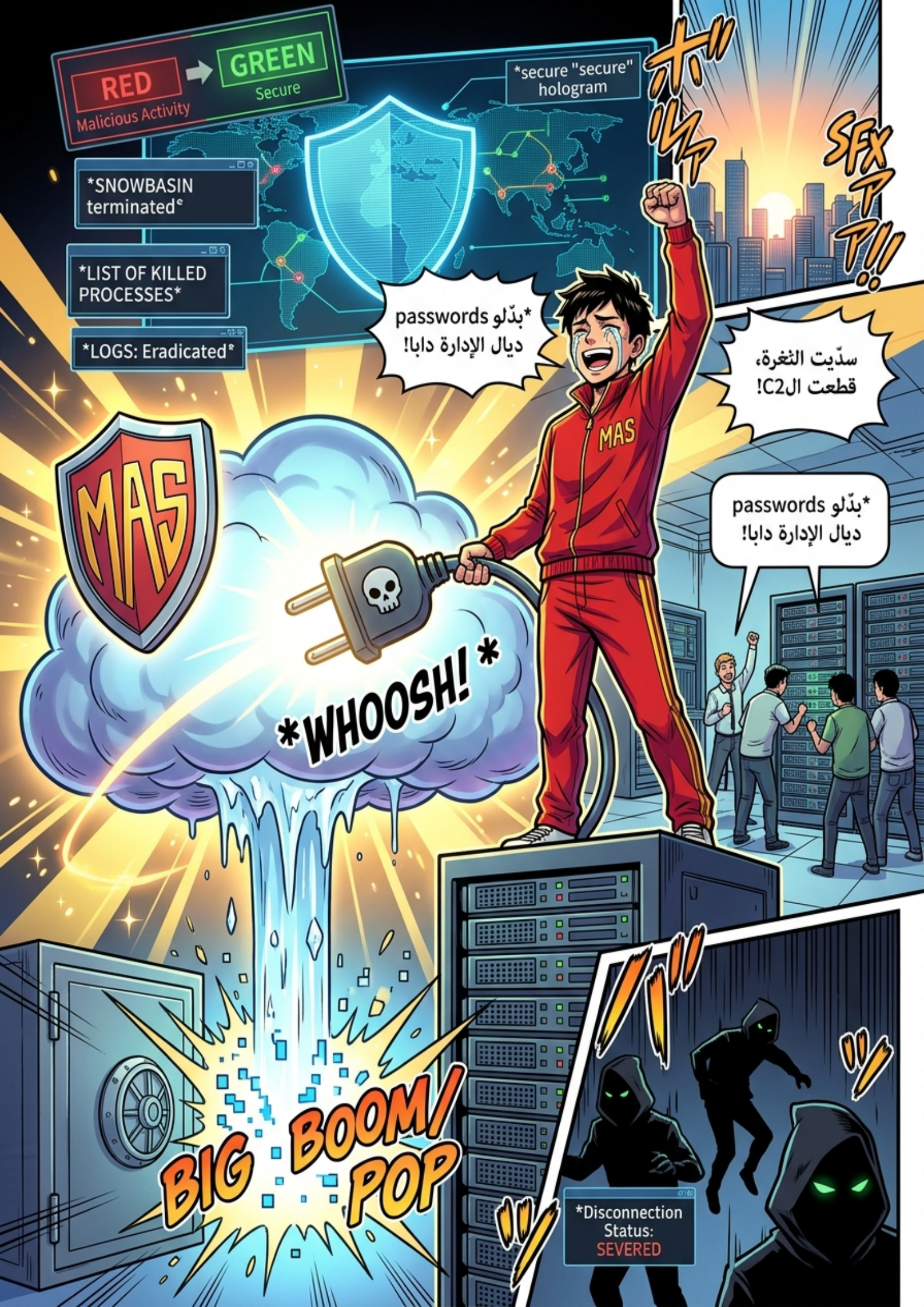

Microsoft Teams
IT
أنا ضغط، IT Helpdesk
على Mailbox Repair
https://mic.ssly v2.1.5
شنو هاد الطوفان
ديال الإيميلات؟!
aws
MAS
CRACK!
CRACIFK!
WHOOSH


C2
WebSocket tunnel
INTRUSION
SNOWBELT
فتح backdoor،
كنصيفطو لC2
RRRIP
RRRIP
File transfer progress...
FTK IMAGER
كيهزو الداتا
من الشبكة!
File transfer progress
Timetable
00:00:00
00:04:38
SNOWDELT
BOOM


Pass-The-Hash
LSASS dump
Pass-The-Hash
mongoDB
MongoDB activity
API calls
CVE alerts
SNOWGLAZE C2 كاين
Timeline
Download
link
AWS S3
تبعّت الlink: AutoHotkey فـ S3
Network scan open ports.
Open scan:
Open port 125 445
145 3369
TAP TAP TAP
gatekeeper check
SNOWGLAZE
SNOWGLAZE tunneling JC2
*BEEP*
Microsoft Teams
CRACK


RED
Malicious Activity
GREEN
Secure
*secure "secure" hologram
*SNOWBASIN terminated*
*LIST OF KILLED PROCESSES*
*LOGS: Eradicated*
SFX
*بدّلو passwords ديال الإدارة دابا!
سدّيت الثغرة، قطعت الC2!
*بدّلو passwords ديال الإدارة دابا!
MAS
*WHOOSH!*
BIG BOOM/ POP
*Disconnection Status: SEVERED