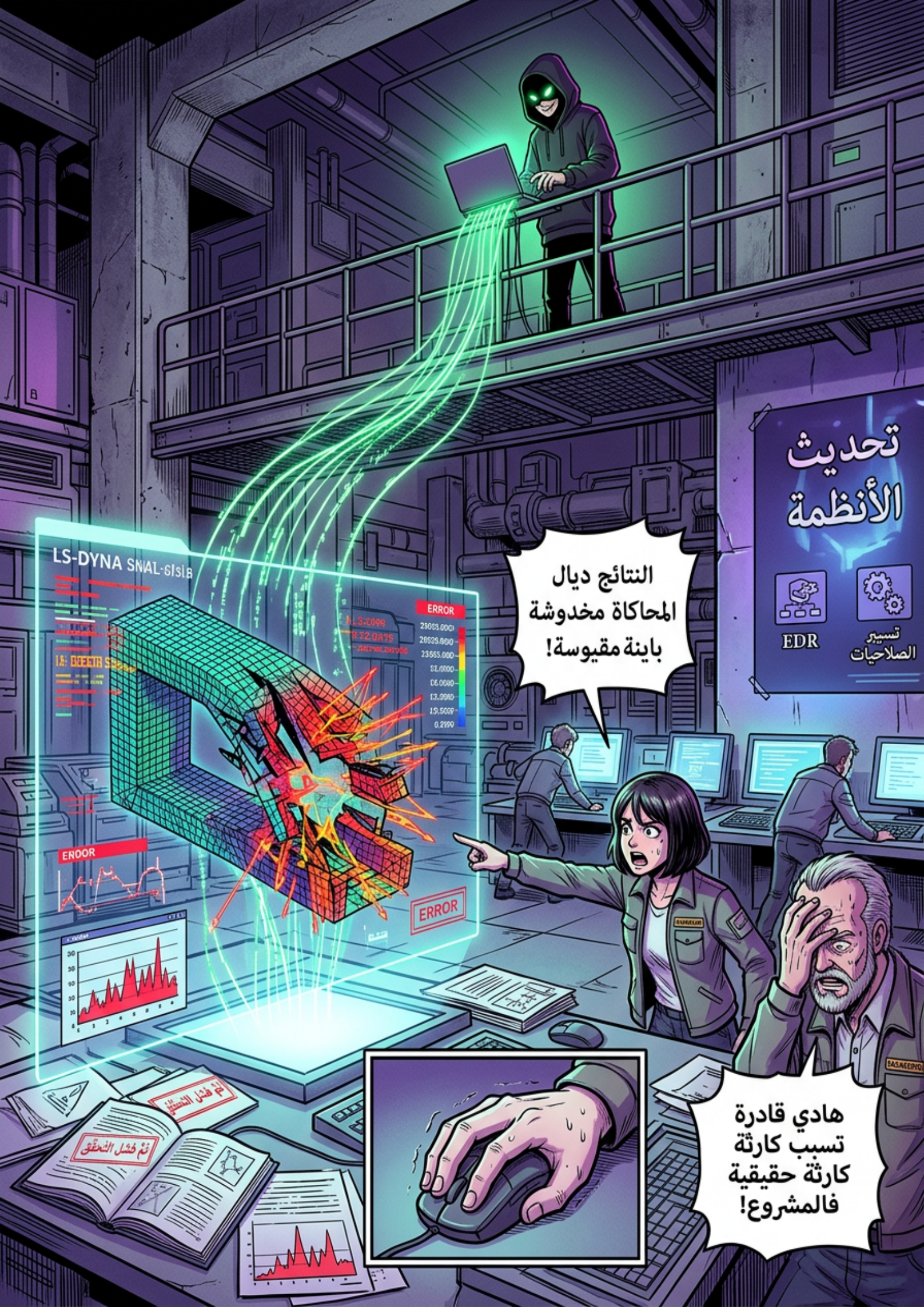
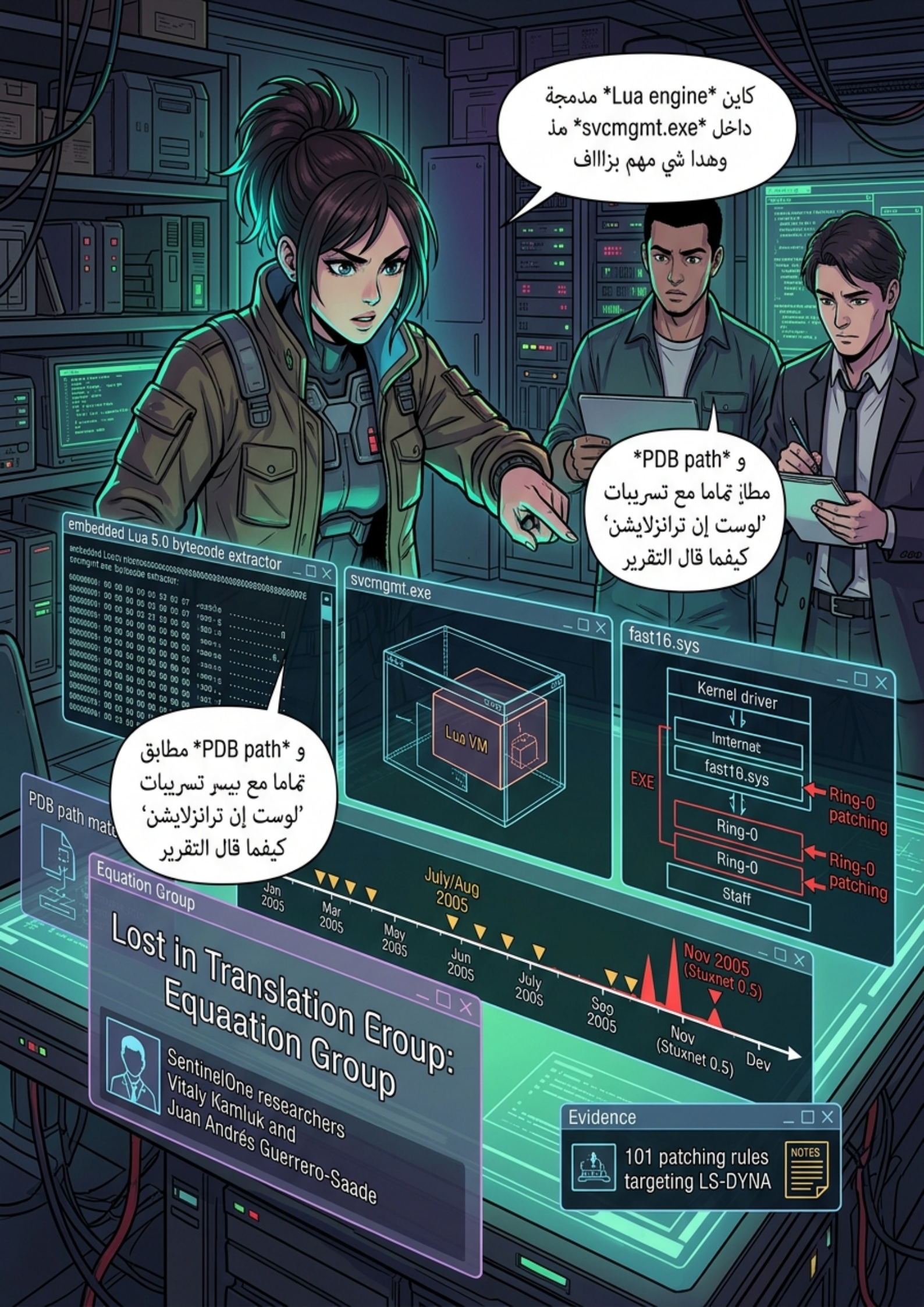

ARTIFACT
fast16
Jul 2005
Aug 2005
ALERT !
شنو هاد "fast16"؟
MAS
توقيتات يوليو وغشت 2005!
> PDB path
Vitaly Kamluk
Juan Andrés Guerrero-Saade
drv_list.txt
Pre-Stuxnet evidence


تحديث الأنظمة
EDR
تسيير الصلاحيات
LS-DYNA
ERROR
ERROR
ERROR
النتائج ديال المحاكاة مخدوشة باينة مقيوسة!
هادي قادرة تسبب كارثة كارثة حقيقية فالمشروع!
نتائج فشل التحقق
نتائج فشل التحقق


كاين *Lua engine* مدمجة
داخل *svcmgmt.exe* مذ
وهدا شي مهم بزاااف
و *PDB path*
مطابق تماما مع تسريبات
'لوست إن ترانزلايشن'
كيفما قال التقرير
embedded Lua 5.0 bytecode extractor
svcmgmt.exe
Lua VM
fast16.sys
Kernel driver
Internet
fast16.sys
EXE
Ring-0 patching
Ring-0
Ring-0
Ring-0 patching
Staff
و *PDB path* مطابق
تماما مع بيسر تسريبات
'لوست إن ترانزلايشن'
كيفما قال التقرير
PDB path mate
Equation Group
Lost in Translation Eroup:
Equaation Group
SentinelOne researchers
Vitaly Kamluk and
Juan Andrés Guerrero-Saade
Jan 2005
Mar 2005
May 2005
Jun 2005
July 2005
July/Aug 2005
Sep 2005
Nov (Stuxnet 0.5)
Nov 2005 (Stuxnet 0.5)
Dev
Evidence
101 patching rules
targeting LS-DYNA
NOTES


Patch kernel driver incompatibility
[COMPLETED]
Upgrade legacy systems beyond Windows XP
[UPGRADED]
Deploy modern EDR
[DEPLOYED]
Enforce strong credential manageme
[ENFORCED AND ROTATED]
SentinelOne
EDR agents sweepin
cleaning infected areas
حدّثّننا الأنظمة وقدرنا نحيد fast16
EDR قوي وتسيير الصلاحيات صارم دابا!