



شنو هاد ال
!Traffic

— هاد LotL هجوم —
ما فيه malware

CRACK!

ALARM!!

81%
Malware-Free

81%
LotL

ALARM!

Elmyr de Hory
mimicry attacks

Packet signature

```
{  
  "type": "data",  
  "action": "subscribe",  
  "url": "https://...",  
  "method": "POST",  
  "headers": {  
    "Content-Type": "application/json"  
  }  
}
```



SUPPLY CHAIN TAMPER!

Dashboard

PACKAGE INTEGRITY: FAILED

HOMOGRAPH DOMAIN



BOOM

RIIIIP

كيدوزو الداتا عبر IP tunnels



السلاسل ديال التوريد مخترقة!

NDR كيشوف
الشذوذ!

كايين Agentic AI
كيتحكم ف
الحركة!

TICK-CLICK-BEEP!

FWOOSH!

SANDBOX ANALYSIS

PACKET INSPECTION

NETWORK VISUALIZATION MAP

Forgeries detected

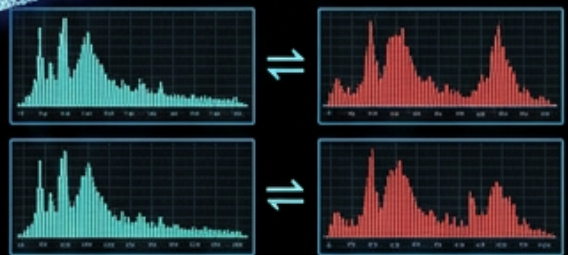


*NORMAL TRAFFIC

*FORGED TRAFFIC -
Brush signatures match

ANOMALY
DETECTED

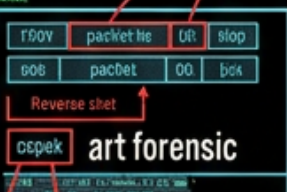
Forgeries detected



NORMAL TRAFFIC

FORGED TRAFFIC -
Brush signatures match

TTP detected



Lateral movement

C2 pattern

Reverse shell

Success h

سدّينا الثغرة!
CVE patched!

Success banner

Success banners

CVE patched
Packages revoked
Takedown complete
Takedown complete

NDR
رجع الأمان!

BOOM

WHAM

Takedown Complete

Restoration complete



PACKAGE ISOLATED

