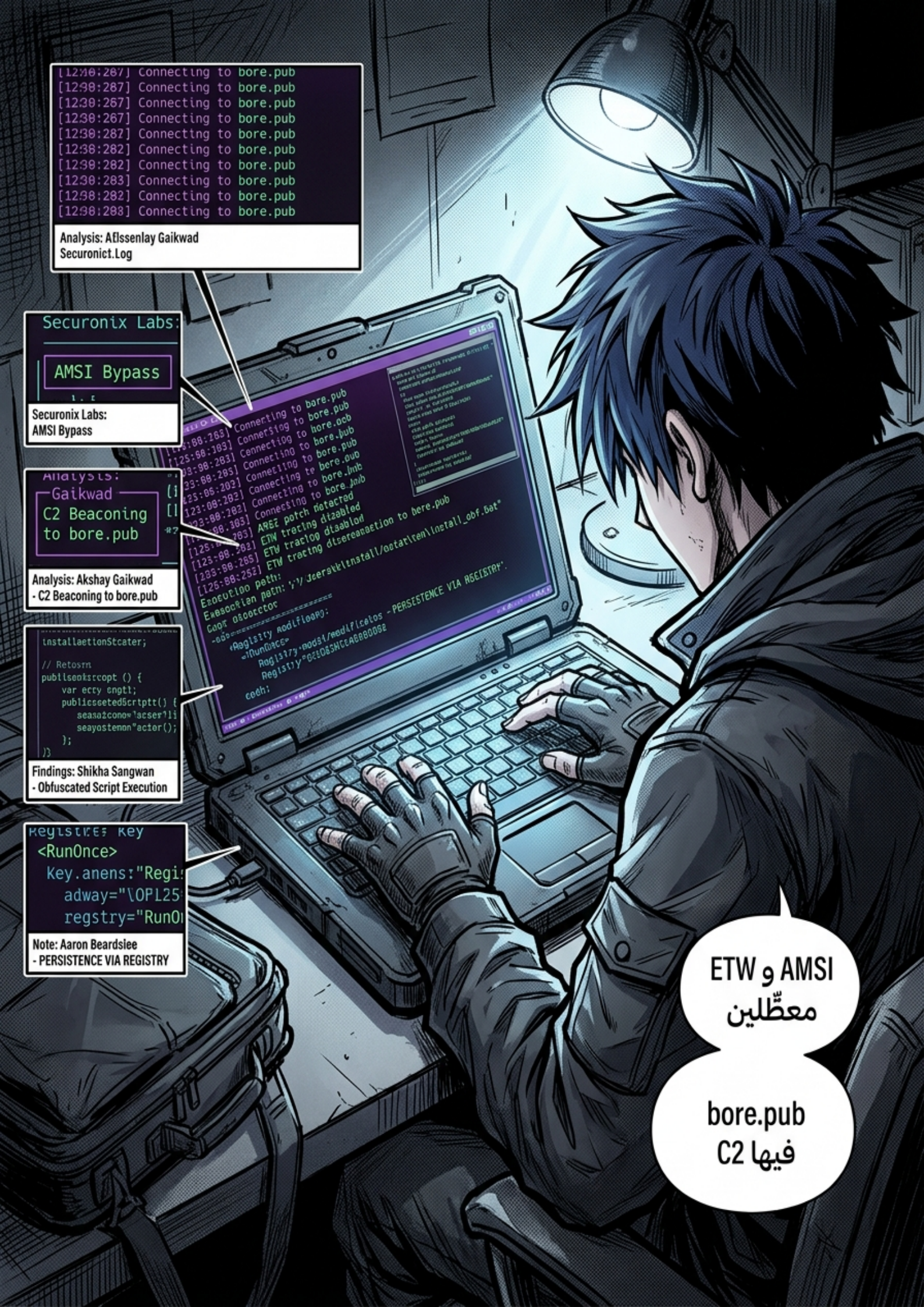

PID: DEEP#DOOR
TARGET: AWS & GOOGLE CLOUD
| BORE.PUB
شنو هاد bore.pub؟
DEEP#DOOR كيستهدف AWS و Google Cloud


تهديد نشط
تنبيه أمني: تم تعطيل Windows Defender!
エクスフィルトレーション
كايطفيو
يحك بيج بتاع
جدول المهام
سحب كلمات المرور...
رموز السحابة...
محرر السجل
Suspicious Run Keys
HKCU\Software\Microsoft\Windows\CurrentVersion\Run -> backup.vbs
كايطفيو Defender!


[12:00:267] Connecting to bore.pub
[12:00:287] Connecting to bore.pub
[12:00:267] Connecting to bore.pub
[12:00:267] Connecting to bore.pub
[12:00:287] Connecting to bore.pub
[12:00:282] Connecting to bore.pub
[12:00:282] Connecting to bore.pub
[12:00:283] Connecting to bore.pub
[12:00:282] Connecting to bore.pub
[12:00:288] Connecting to bore.pub
Analysis: Alissenlay Gaikwad
Securonict.Log
Securonix Labs:
AMSI Bypass
Securonix Labs:
AMSI Bypass
Gaikwad
C2 Beaconing
to bore.pub
Analysis: Akshay Gaikwad
- C2 Beaconing to bore.pub
Findings: Shikha Sangwan
- Obfuscated Script Execution
<RunOnce>
Note: Aaron Beardsiee
- PERSISTENCE VIA REGISTRY
ETW و AMSI
معطّلين
bore.pub
فيها C2


تمت تفعيل مراقبة 'Registry Run' ومفاتيح الإقلاع
تدقيق 'Scheduled Tasks'
التحقق من مجلد 'Startup'
لقد حاصرناه!
تم تأمين النظام!
راقب Registry و Scheduled Tasks!
الدالّة تعمل!
تم اكتشاف البرنامج الضار
بدء الحجر
SECURONIX QUARANTINE
حاصرناه! تم عزل التهديد
SECURONIX