
CPUID
Sitemap
9 Apr 15:00 UTC → 10 Apr 10:00 UTC
watering-hole attack + trojanized installers
CPUID
Official download
Official download
CPU-Z_setup.exe (official)
→
pub-45c2577...r2.dev/evil.exe
شنو هادا؟
الموقع
مخترق!
CPUID
DOWNLOAD
CRACK!
MAS
API الثانوية
ينقر!
API الثانوية
تبدلات الروابط!


ZIP
ZIP
EXL
CRYPTBASE.dll
C2
cahayailmukreatif.web.id
transitopalermo.com
HVNC
CRACK BOOM
C2
STX RAT دخل للأنظمة!
POST REQUEST cahayailmukreatif.web.id
POST REQUEST transitopalermo.com
STX RAT –
HVNC, infostealing
HVNC كاين وinfostealing!
BOOM
CRACK


war room
قرلي بعي
kaspersky
eSentire
Over 150 victim locations
TICK-CHK
how thes attacka requests to the four suspicious domains
Highlighted 'secondary API' call
Timeline
9 Apr — 10 Apr
(CVE)
TICK-CHK
DLL side-loading flow:
CRYPTBASE.dll
legit exe
malicious payload
STX RAT
gatekeeper
gatekeeper
DLL side-loading وanti-sandbox، هادي الطريقة!
شوفو الlogs! هاد الدومينات ظاهرين!
WEAK OPSEC


BOOM!
PATCH / SEAL API
PATCH
SHING!
PATCH APPLIED
APIPATCH
C2 BLOCKED
سدينا الـ API
وردينا الروابط
الأصلية!
quarantine
meshes
Log UI
external domain
c2 blockeoos.com
BLOCKED
BLOCKED
BLOCKED
دارينا patch،
STX خارج!
poisoned
buttons
signed
original