
شنو هاد postinstall؟!
npm
ICP
cjn37-uyaaa-...raw.icp0.io
NEM
MAS
التوكينات كيتسرقو!
exfiltrate -> telemetry.api-monitor[.]com
CRACK
ZZZT
ZZZT
> postinstall
> postinstall hook script executed
> postinstall hook executed
> exfiltrate .npmrc
> exfiltrate .npmrc
> exfiltrate .npmrc
> postinstall hook executed
> exfiltrate .npmrc
> exfiltrate -> telemetry.api-monitor[.]com
npm


INFECTED
INFECTED
INFECTED
INFECTED
INFECTED
INFECTED
INFECTED
Server
Server
npm
npm
Developer Machine
aws
PyPI
wheel
Cargo
Exfiltration targets
@automagik/genie
@openwehconcept/...
PyPI
Twine
telemetry.api-monitor.com
raw.lcp0.io
UNAUTHORIZED PUBLISH DETECTED
PYPI WHEELS TAMPERED
PIPELINES BURNING
المستودعات مصابة!
M.A.S
canister الـ
كيتلقى الداتا!
PyPI
npm
Cargo
Package
SZHKK-BOOM!
SHATTER!


1.4.3–1.4.4
4.260421.33–40
Telemetry trails
telemetry.api-monitor URL
ICP
ICP
4.260421.33–40
شوفو هاد cjn37
raw.icp0.io
خاصنا نوقفو
التوكينات دابا!
CLACK
BEEP
steal tokens
postinstall
postinstall :
var tokens = elemetry-monitor
twine_upload {
twine.parastet.t= "tanmet.pyPI"
upload script="pyPI".
}
CVE
API
JS
obfuscated_JS
postinstall hook
python():
API
API
Twine
MongoDB
SSH keys
CLICK
telemetry.api-monitor[.]com
API
CVE


patch v↑
tokens revoked
npm
pypi
ICP
sealated
سدّينا الثغرة!
revoke tokens
MAS
registry secured
postinstall
سدّينا الـpackage نجاو!
community developers
patch deployed
tokens revoked
malware removed