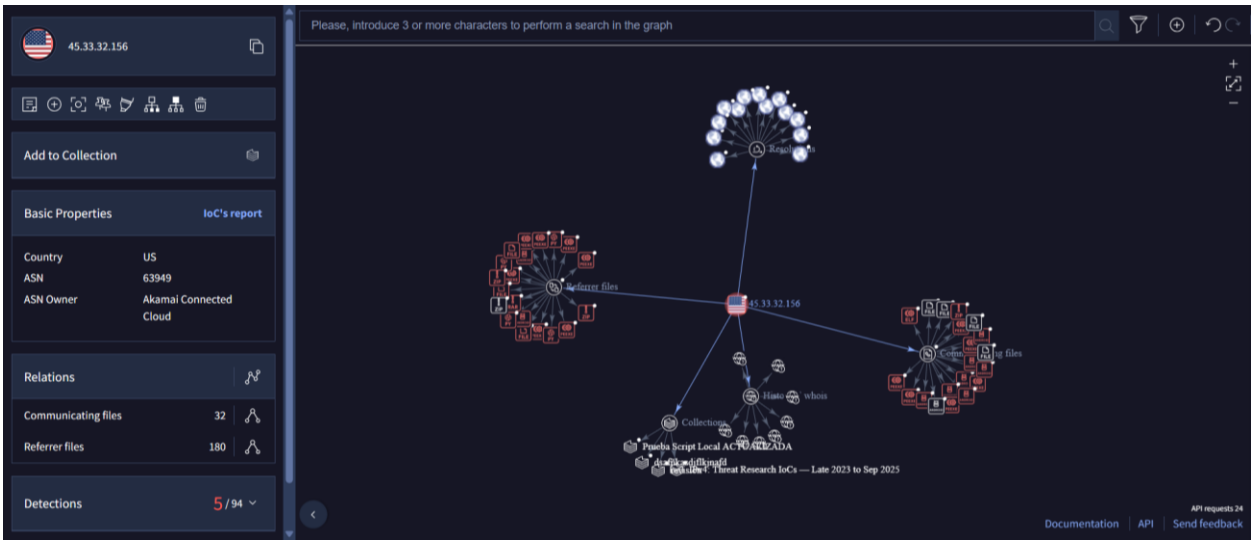
INFORME DE INTELIGENCIA DE AMENAZAS – Q1 2026
CONFIDENCIAL - USO INTERNO

Tabla de infraestructura conocida por campaña:

Campaign ID	IOC Type	Indicator Value	Actor Group
CAMPAIGN_RED_STORM	IP	45.33.32.156	APT28
CAMPAIGN_PHANTOM_LEDGER	Domain	portal-verify.secure-login-cdn.net	Financial_Hunters
CAMPAIGN_LEDGER	Domain	scanme.nmap.org	Virus Total
CAMPAISH_DARK_WEB	Hash	a1b2c3d4e5f6....	Ransomware_Grp
CAMPAIGN_SILENT_VIPE	IP	102.134.55.21	Lazarus



https://www.virustotal.com/graph/45.33.32.156

Notas:

- Se enfoca en spear-phishing a instituciones financieras.
- Utiliza dominios que imitan CDNs legítimos.