Operation Digital Eye - Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 12:44:23 UTC

APT group: Operation Digital Eye

Names	Operation Digital Eye *(SentinelLabs)*
Country	China
Motivation	Information theft and espionage
First seen	2024
Description	(SentinelLabs) From late June to mid-July 2024, a suspected China-nexus threat actor targeted large business-to-business IT service providers in Southern Europe, an activity cluster that we dubbed 'Operation Digital Eye'. The intrusions could have enabled the adversaries to establish strategic footholds and compromise downstream entities. SentinelLabs and Tinexta Cyber detected and interrupted the activities in their initial phases. The threat actors used a lateral movement capability indicative of the presence of a shared vendor or digital quartermaster maintaining and provisioning tooling within the Chinese APT ecosystem. The threat actors abused Visual Studio Code and Microsoft Azure infrastructure for C2 purposes, attempting to evade detection by making malicious activities appear legitimate. Our visibility suggests that the abuse of Visual Studio Code for C2 purposes had been relatively rare in the wild prior to this campaign. Operation Digital Eye marks the first instance of a suspected Chinese APT group using this technique that we have directly observed.
Observed	Sectors: Business-to-business IT service providers. Countries: Southern Europe.
Tools used	mim221, Mimikatz, PHPsert, Living off the Land.
Information	<https://www.sentinelone.com/labs/operation-digital-eye-chinese-apt-compromises-critical-digital-infrastructure-via-visual-studio-code-tunnels/>

Last change to this card: 27 December 2024

Download this actor card in PDF or JSON format
