Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-06 03:12:57 UTC

APT group: EmpireMonkey, CobaltGoblin

Names	EmpireMonkey *(?)* CobaltGoblin *(?)* Anthropoid Spider *(CrowdStrike)*	
Country	[Unknown]	
Motivation	Financial crime	
First seen	2018	
Description	(Blueliv) EmpireMonkey is an advanced financially motivated cybercriminal gang. The group gained notoriety for a heist they conducted in February 2019 against the Maltese Bank of Valletta, which initially resulted in roughly €13 million in losses, though much of this was subsequently recovered or frozen. While a thorough post-mortem of the Bank of Valletta attack has yet to be made public, it is highly likely that the threat actors sent malicious spear phishing emails to employees at Bank of Valletta and other European financial institutions. In October 2018, HSBC Malta reported receiving phishing emails that bore hallmarks of the subsequent EmpireMonkey attack against Bank of Valletta. This group seems to be directly related to Carbanak, Anunak and/or FIN7.	
Observed	Sectors: Financial. Countries: Malta and Worldwide.	
Tools used	MedusaLocker.	
Operations performed	Mar 2021	Nine Entertainment warns ransomware recovery 'will take time' <https://www.itnews.com.au/news/nine-entertainment-warns-ransomware-recovery-will-take-time-562755>
Counter operations	Jan 2020	6 Suspects Arrested in Maltese Bank Hacking Heist <https://www.bankinfosecurity.com/6-suspects-arrested-in-maltese-bank-hacking-heist-a-13674>
Information	<https://blueliv.com/resources/white-papers/Finance_whitepaper_ENG.pdf>	

Last change to this card: 26 April 2021

Download this actor card in PDF or JSON format
