Operation HangOver, Monsoon, Viceroy Tiger

Archived: 2026-04-05 16:42:01 UTC

Threat Group Cards: A Threat Actor Encyclopedia

APT group: Operation HangOver, Monsoon, Viceroy Tiger

Names	Operation HangOver *(Shadowserver Foundation)* Monsoon *(Forcepoint)* Viceroy Tiger *(CrowdStrike)* Neon *(?)* G0042 *(MITRE)*	
Country	India	
Motivation	Information theft and espionage	
First seen	2010	
Description	(Shadowserver Foundation) On Sunday March 17th 2013 the Norwegian newspaper Aftenposten reported that the telecomm Telenor had filed a case with Norwegian criminal police ("KRIPOS") over what was perceived as an unlawful intrusion into network. The infection was reported to have been conducted via "spear phishing" emails sent to people in the upper tiers of Initially, we had no information or visibility into this case. However, after some time Norwegian CERT (NorCERT) shared s event, which included md5 hashes of malicious files and information about which Command and Control servers were used. However, the data we were given acted as a starting point for more data mining, and within a short period of time it became seeing a previously unknown and very extensive infrastructure for targeted attacks. This paper is the result of the ensuing in The samples we have uncovered seem to have been created from approximately September 2010 until the present day. It app active year for this group, which saw escalation not only in numbers of created malware files but also in targets. There is no will slow down in 2013, as we see new attacks continuously. In a great number of isolated cases and contexts, the word "Appin" shows up and there seems to be some connection with th company called Appin Security Group.	
Observed	Sectors: Defense, Government, Hospitality, Telecommunications. Countries: Austria, Bangladesh, Canada, China, France, Germany, India, Indonesia, Iran, Jordan, Kuwait, Myanmar, Norway Pakistan, Poland, Romania, Russia, Singapore, Sri Lanka, Taiwan, Thailand, UAE, UK, USA and Africa and Far East.	
Tools used	AutoIt backdoor, BackConfig, BADNEWS, TINYTYPHON, Unknown Logger, WSCSPL.	
Operations performed	Jan 2020	Updated BackConfig Malware Targeting Government and Military Organizations in South Asia <https://unit42.paloaltonetworks.com/updated-backconfig-malware-targeting-government-and-military-o
Information	<https://keybase.pub/kung_foo/papers_and_presentations/Unveiling_an_Indian_Cyberattack_Infrastructure.pdf> <https://paper.seebug.org/papers/APT/APT_CyberCriminal_Campagin/2013/Unveiling%20an%20Indian%20Cyberattack%%20appendixes.pdf> <https://www.darkreading.com/attacks-breaches/hangover-persists-more-mac-malware-found/d/d-id/1140147> <https://www.forcepoint.com/sites/default/files/resources/files/forcepoint-security-labs-monsoon-analysis-report.pdf> <https://unit42.paloaltonetworks.com/threat-assessment-hangover-threat-group/> <https://www.sentinelone.com/labs/elephant-hunting-inside-an-indian-hack-for-hire-group/>	
MITRE ATT&CK	<https://attack.mitre.org/groups/G0042/>	
Playbook	<https://pan-unit42.github.io/playbook_viewer/?pb=hangover>	

Last change to this card: 16 August 2025

Download this actor card in PDF or JSON format
