Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 20:43:07 UTC

APT group: Lucky Cat

Names	Lucky Cat *(Symantec)*
Country	China
Motivation	Information theft and espionage
First seen	2011
Description	(Symantec) A series of attacks, targeting both Indian military research and south Asian shipping organizations, demonstrate the minimum level of effort required to successfully compromise a target and steal sensitive informatio The attackers use very simple malware, which required little development time or skills, in conjunction with freely available Web hosting, to implement a highly effective attack. It is a case of the attackers obtaining a maximum retu on their investment. The attack shows how an intelligent attacker does not need to be particularly technically skilled order to steal the information they are after. The attack begins, as is often the case, with an email sent to the victim. A malicious document is attached to the email, which, when loaded, activates the malware. The attackers use tailored emails to encourage the victim to open the email. For example, one email sent to an academic claimed to be a call fo papers for a conference (CFP). The vast majority of the victims were based in India, with some in Malaysia. The victim industry was mostly militar research and also shipping based in the Arabian and South China seas. In some instances the attackers appeared to have a clear goal, whereby specific files were retrieved from certain compromised computers. In other cases, the attackers used more of a 'shotgun' like approach, copying every file from a computer. Military technologies were obviously the focus of one particular attack with what appeared to be source code stolen. 45 different attacker IP addresses were observed. Out of those, 43 were within the same IP address range based in Sichuan province, China. The remaining two were based in South Korea. The pattern of attacker connections implies that the IP addresses are being used as a VPN, probably in an attempt to render the attackers anonymous. The attacks have been active from at least April 2011 up to February 2012. The attackers are intelligent and focused, employing the minimum amount of work necessary for the maximum gain. They do not use zero day exploits or complicated threats, instead they rely on effective social engineering and lax security measures on the part of the victims.
Observed	Sectors: Aerospace, Defense, Engineering, Shipping and Logistics and Tibetan activists. Countries: India, Japan, Malaysia, Tibet.
Tools used	Comfoo, Lucky Cat, Sojax, WMI Ghost.
Information	<https://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/the_luckycat_hackers.pd <https://www.trendmicro.de/cloud-content/us/pdfs/security-intelligence/white-papers/wp_luckycat_redux.pdf>

Last change to this card: 14 April 2020

Download this actor card in PDF or JSON format