Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 21:28:25 UTC

APT group: Operation WizardOpium

Names	Operation WizardOpium *(Kaspersky)*
Country	North Korea
Motivation	Information theft and espionage
First seen	2019
Description	(Kaspersky) Kaspersky Exploit Prevention is a component part of Kaspersky products that has successfully detected a number of zero-day attacks in the past. Recently, it caught a new unknown exploit for Google's Chrome browser. We promptly reported this to the Google Chrome security team. After reviewing of the PoC we provided, Google confirmed there was a zero-day vulnerability and assigned it CVE-2019-13720. We are calling these attacks Operation WizardOpium. So far, we have been unable to establish a definitive link with any known threat actors. There are certain very weak code similarities with Lazarus Group, Hidden Cobra, Labyrinth Chollima attacks, although these could very well be a false flag. The profile of the targeted website is more in line with earlier DarkHotel attacks that have recently deployed similar false flag attacks.
Observed	Countries: South Korea.
Tools used	
Information	<https://securelist.com/chrome-0-day-exploit-cve-2019-13720-used-in-operation-wizardopium/94866/> <https://securelist.com/windows-0-day-exploit-cve-2019-1458-used-in-operation-wizardopium/95432/> <https://securelist.com/the-zero-day-exploits-of-operation-wizardopium/97086/>

Last change to this card: 02 July 2020

Download this actor card in PDF or JSON format

Source: https://apt.etda.or.th/cgi-bin/showcard.cgi?u=d25e7c98-dbe9-45c7-8052-1108add0a929