Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 15:06:06 UTC

APT group: Hades

Names	Hades *(Kaspersky)*
Country	Russia
Sponsor	State-sponsored, GRU
Motivation	Sabotage and destruction, Financial crime
First seen	2017
Description	(Kaspersky) In March 2018 we published our research on Olympic Destroyer, an advanced attack that hit organizers, suppliers and partners of the Winter Olympic Games 2018 held in Pyeongchang, South Korea. Olympic Destroyer was a cyber-sabotage attack based on the spread of a destructive network worm. The sabotage stage was preceded by reconnaissance and infiltration into target networks to select the best launchpad for the self-replicating and self-modifying destructive malware. We are calling the actor behind the Olympic Destroyer attack – “Hades”. We have previously emphasized that Hades is different from other threat actors because the whole attack was a masterful operation in deception. Despite that, the attackers made serious mistakes, which helped us to spot and prove the forgery of rare attribution artefacts. The attackers behind Olympic Destroyer forged automatically generated signatures, known as Rich Header, to make it look like the malware was produced by Lazarus Group, Hidden Cobra, Labyrinth Chollima APT, an actor widely believed to be associated with North Korea. If this is new to the reader, we recommend a separate blog dedicated to the analysis of this forgery. Some of the TTPs and operational security used by Hades during the Olympic Destroyer attack bear a certain resemblance to Sofacy, APT 28, Fancy Bear, Sednit APT group activity. When it comes to false flags, mimicking TTPs is much harder than tampering with technical artefacts. It implies a deep knowledge of how the actor being mimicked operates as well as operational adaptation to these new TTPs. However, it is important to remember that Hades can be considered a master in the use of false flags: for now we assess that connection with low to moderate confidence.

Observed	Sectors: Financial, Government, Healthcare. Countries: Russia, South Korea, Ukraine and Europe.	
Tools used	Brave Prince, Gold Dragon, Olympic Destroyer, RunningRAT.	
Operations performed	Jun 2019	Hades, the actor behind Olympic Destroyer is still alive <https://securelist.com/olympic-destroyer-is-still-alive/86169/>
	Feb 2020	Operation “TrickyMouse” Attacks pretend to be from the Center for Public Health of the Ministry of Health of Ukraine and deliver bait document containing the latest news regarding #COVID-19. A backdoor written in C# gets dropped by malicious macro code to perform remote control. <https://twitter.com/RedDrip7/status/1230683740508000256> <https://mp.weixin.qq.com/s/o6KC0k43AuOY5F8FKGbmMg>
Counter operations	Oct 2020	Six Russian GRU Officers Charged in Connection with Worldwide Deployment of Destructive Malware and Other Disruptive Actions in Cyberspace <https://www.justice.gov/opa/pr/six-russian-gru-officers-charged-connection-worldwide-deployment-destructive-malware-and>
Information	<https://securelist.com/olympicdestroyer-is-here-to-trick-the-industry/84295/>	

Last change to this card: 22 June 2023

Download this actor card in PDF or JSON format
