Olympic Destroyer - Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 17:13:08 UTC

Tool: Olympic Destroyer

Names	Olympic Destroyer SOURGRAPE
Category	Malware
Type	Credential stealer, Wiper, Worm, Remote command
Description	(Kaspersky) The main malware module is a network worm that consists of multiple components, including a legitimate PsExec tool from SysInternals' suite, a few credential stealer modules and a wiper. From a technical perspective, the purpose of the malware is to deliver and start the wiper payload which attempts to destroy files on the remote network shares over the next 60 minutes. Meanwhile, the main module collects user passwords from browser and Windows storage and crafts a new generation of the worm that contains old and freshly collected compromised credentials. The new generation of the worm is pushed to accessible local network computers and starts using the PsExec tool, leveraging the collected credentials and current user privileges. Once the wiper has run for 60 minutes it cleans Windows event logs, resets backups, deletes shadow copies from the file system, disables the recovery item in the Windows boot menu, disables all the services on the system and reboots the computer. Those files on the network shares that it managed to wipe within 60 minutes remain destroyed. The malware doesn't use any persistence and even contains protection (also a killswitch) against recurring reinfection. Incidentally, only 1MB of the remote files are fully overwritten with zeroes; larger files were wiped with just 1K of zeroes in the header. The local files are not destroyed and the worm doesn't wipe itself or its components.
Information	<https://securelist.com/olympicdestroyer-is-here-to-trick-the-industry/84295/> <http://blog.talosintelligence.com/2018/02/olympic-destroyer.html> <https://www.lastline.com/labsblog/olympic-destroyer-south-korea/> <https://securelist.com/the-devils-in-the-rich-header/84348/> <https://cyber.wtf/2018/03/28/dissecting-olympic-destroyer-a-walk-through/> <https://securelist.com/olympic-destroyer-is-still-alive/86169/>

	<http://blog.talosintelligence.com/2018/02/who-wasnt-responsible-for-olympic.html> <https://www.lastline.com/labsblog/attribution-from-russia-with-code/>
MITRE ATT&CK	<https://attack.mitre.org/software/S0365/>
Malpedia	<https://malpedia.caad.fkie.fraunhofer.de/details/win.olympic_destroyer>
AlienVault OTX	<https://otx.alienvault.com/browse/pulses?q=tag:Olympic%20Destroyer>

Last change to this tool card: 14 May 2020

Download this tool card in JSON format

All groups using tool Olympic Destroyer

Changed	Name	Country	Observed	
APT groups				
	Hades		2017-Oct 2020	

1 group listed (1 APT, 0 other, 0 unknown)

Source: https://apt.etda.or.th/cgi-bin/listgroups.cgi?u=0662a96f-61af-4f1c-b978-9f42d155cf0c