

Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 17:10:24 UTC

[Home](#) > [List all groups](#) > [List all tools](#) > List all groups using tool OwlProxy

Tool: OwlProxy

Names	OwlProxy
Category	Malware
Type	Tunneling
Description	(ESET) Across the victims and malware we analyzed here, an interesting piece of malware stood out and needed a deeper look. From an initial, quick analysis, it was recognized as OwlProxy; an HTTP proxy server. A complete analysis can be found in this Cycraft post. This module also comes in two variants – 32- and 64-bit versions – and as a result it contains a function to test the Windows version as in the Gelsemium components.
Information	< https://www.welivesecurity.com/wp-content/uploads/2021/06/eset_gelsemium.pdf > < https://medium.com/cycraft/taiwan-government-targeted-by-multiple-cyberattacks-in-april-2020-3b20cea1dc20 > < https://lab52.io/blog/chimera-apt-updates-on-its-owlproxy-malware/ >
Malpedia	< https://malpedia.caad.fkie.fraunhofer.de/details/win.owlproxy >

Last change to this tool card: 28 December 2021

Download this tool card in [JSON](#) format

All groups using tool OwlProxy

Changed	Name	Country	Observed
APT groups			
	Gelsemium		2014-2023

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

Source: <https://apt.eta.or.th/cgi-bin/listgroups.cgi?u=47f36fe6-e027-4622-9958-5deb84631ea4>