

Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 19:19:50 UTC

APT group: LazyScripter

Names	LazyScripter (<i>Malwarebytes</i>) G0140 (<i>MITRE</i>)
Country	[Unknown]
Motivation	Information theft and espionage
First seen	2018
Description	(Malwarebytes) Malwarebytes' Threat Intelligence analysts are continually researching and monitoring active malware campaigns and actor groups as the prevalence and sophistication of targeted attacks rapidly evolves. In this paper, we introduce a new APT group we have named LazyScripter, presenting in-depth analysis of the tactics, techniques, procedures, and infrastructure employed by this actor group.
Observed	Sectors: Aviation . Countries: Canada .
Tools used	Adwind , EmpireProject , Empoder , Invoke-Ngrok , Koadic , KOCTOPUS , Luminosity RAT , Nishang , njRAT , Octopus , QuasarRAT , RemcosRAT , RMS .
Information	< https://resources.malwarebytes.com/files/2021/02/LazyScripter.pdf >
MITRE ATT&CK	< https://attack.mitre.org/groups/G0140/ >

Last change to this card: 16 August 2025

Download this actor card in [PDF](#) or [JSON](#) format

Source: <https://apt.etda.or.th/cgi-bin/showcard.cgi?u=84510b1b-3499-4a9f-bbeb-90b391e3d2cf>