

Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 14:59:40 UTC

Tool: Pteranodon


Names	Pteranodon Pterodo
Category	Malware
Type	Backdoor , Info stealer , Downloader
Description	(Palo Alto) Pteranodon is a custom backdoor which is capable of the following tasks: <ul style="list-style-type: none"> • Capturing screenshots at a configurable interval and uploading them to the attacker • Downloading and executing additional files • Executing arbitrary commands on the system
Information	https://unit42.paloaltonetworks.com/unit-42-title-gamaredon-group-toolset-evolution/ https://threatpost.com/gamaredon-apt-toolset-ukraine/152568/ https://www.vkremez.com/2019/01/lets-learn-deeper-dive-into-gamaredon.html https://cert.gov.ua/news/42 https://cert.gov.ua/news/46 https://blog.threatstop.com/russian-apt-gamaredon-group https://www.microsoft.com/security/blog/2022/02/04/actinium-targets-ukrainian-organizations/
MITRE ATT&CK	https://attack.mitre.org/software/S0147/
Malpedia	https://malpedia.caad.fkie.fraunhofer.de/details/win.pteranodon
AlienVault OTX	https://otx.alienvault.com/browse/pulses?q=tag:Pteranodon

Last change to this tool card: 05 February 2022

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

All groups using tool Pteranodon

Changed	Name	Country	Observed
APT groups			

	Gamaredon Group		2013-Feb 2025	
--	---------------------------------	---	---------------	---

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

[↑](#)

Source: <https://apt.etda.or.th/cgi-bin/listgroups.cgi?u=ef780da4-a57f4a89-b653-dd7798dfef03>