Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 19:09:59 UTC

Tool: ORPCBackdoor

Names	ORPCBackdoor
Category	Malware
Type	Backdoor
Description	(Knownsec 404) Recently, Knownsec 404 Advanced Threat Intelligence Team found a new DLL backdoor in the Arsenal of Bitter during the continuous tracking process, the original name is OLEMAPI32.DLL, the product name is Microsoft Outlook, the discovered backdoor uses a more unique communication method. In contrast to the group's other weapons, the backdoor communication method discovered this time uses RPC to interact with the server. According to the available information, the newly discovered back door is most likely to target Outlook user groups. In order to facilitate follow-up tracking, hunting and differentiation, we named it ORPCBackdoor based on this feature.
Information	<https://paper.seebug.org/2092/> <https://medium.com/@knownsec404team/apt-k-47-mysterious-elephant-a-new-apt-organization-in-south-asia-5c66f954477> <https://medium.com/@knownsec404team/unveiling-the-past-and-present-of-apt-k-47-weapon-asyncshell-5a98f75c2d68>
Malpedia	<https://malpedia.caad.fkie.fraunhofer.de/details/win.orpcbackdoor>

Last change to this tool card: 27 December 2024

Download this tool card in JSON format

All groups using tool ORPCBackdoor

Changed	Name	Country	Observed

APT groups

	Mysterious Elephant	[Unknown]	2023	

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

Source: https://apt.etda.or.th/cgi-bin/listgroups.cgi?u=a83bf18c-31cb-4103-ae7b-9127d86fc766