Penquin Turla - Threat Group Cards: A Threat Actor Encyclopedia

Tool: Penquin Turla

Names	Penquin Turla
Category	Malware
Type	Backdoor
Description	(Kaspersky) This newly found Turla component supports Linux for broader system support at victim sites. The attack tool takes us further into the set alongside the Uroburos rootkit and components first associated with this actor a couple years ago. We suspect that this component was running for years at a victim site, but do not have concrete data to support that statement just yet. The Linux Turla module is a C/C++ executable statically linked against multiple libraries, greatly increasing its file size. It was stripped of symbol information, more likely intended to increase analysis effort than to decrease file size. Its functionality includes hidden network communications, arbitrary remote command execution, and remote management. Much of its code is based on public sources.
Information	<https://securelist.com/the-penquin-turla-2/67962/> <https://securelist.com/files/2017/04/Penquins_Moonlit_Maze_PDF_eng.pdf> <https://securelist.com/files/2017/04/Penquins_Moonlit_Maze_AppendixB.pdf>
Malpedia	<https://malpedia.caad.fkie.fraunhofer.de/details/elf.penquin_turla>

Last change to this tool card: 13 May 2020

Download this tool card in JSON format

All groups using tool Penquin Turla

Changed	Name	Country	Observed

APT groups

	Turla, Waterbug, Venomous Bear		1996-2024	

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

Source: https://apt.etda.or.th/cgi-bin/listgroups.cgi?u=03f49e14-c41f-43e5-a48d-43a15224640e