Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-02 10:48:16 UTC

Tool: TinyPosh

Names	TinyPosh
Category	Malware
Type	Backdoor, Downloader, Loader
Description	(Group-IB) As in the first campaigns, opening the link in the email resulted in the TinyPosh Trojan being downloaded to the victim's computer. The malware achieved persistence in the system, obtained privileges of the account from which the Trojan was launched, and could download and launch the Cobalt Strike Beacon upon command. To hide the real C&C address, the hackers used the Cloudflare Workers server.
Information	<https://www.group-ib.com/blog/oldgremlin>

Last change to this tool card: 19 October 2020

Download this tool card in JSON format

All groups using tool TinyPosh

Changed	Name	Country	Observed	
APT groups				
	OldGremlin		2020-Feb 2021	

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