Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-06 00:06:54 UTC

Tool: Matryoshka RAT

Names	Matryoshka RAT Matryoshka
Category	Malware
Type	Backdoor, Dropper, Loader, Info stealer
Description	(ClearSky) The Matryoshka infection framework is built of three parts: • Dropper o Obfuscating code and signaling to the C2 that the file has been executed o Launching the loader and using it to execute functions. o Comparing anti-analysis logic and reporting it back to C2 • Reflective Loader o Employing anti-debugging and anti-sandboxing techniques o Runtime API Address resolver o Covert DLL injection of the RAT library o Persistence file on disk • RAT component o Configuring the Reflective Loader to survive reboots and process exits o DNS Command and Control communication o Common RAT functionalities
Information	<https://s3-eu-west-1.amazonaws.com/minervaresearchpublic/CopyKittens/CopyKittens.pdf>
MITRE ATT&CK	<https://attack.mitre.org/software/S0167/>
Malpedia	<https://malpedia.caad.fkie.fraunhofer.de/details/win.matryoshka_rat>
AlienVault OTX	<https://otx.alienvault.com/browse/pulses?q=tag:Matryoshka>

Last change to this tool card: 30 December 2022

Download this tool card in JSON format

All groups using tool Matryoshka RAT

Changed	Name	Country	Observed	
APT groups				
	CopyKittens, Slayer Kitten		2013-Jan 2017	
	Magic Hound, APT 35, Cobalt Illusion, Charming Kitten		2012-Jun 2025	

2 groups listed (2 APT, 0 other, 0 unknown)

Source: https://apt.etda.or.th/cgi-bin/listgroups.cgi?u=dc27057d-c0bb-48f2-a418-4293b46366fc