Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 20:31:03 UTC

Tool: ComRAT

Names	ComRAT
Category	Malware
Type	Backdoor
Description	(G Data) In February 2014, the experts of the G DATA SecurityLabs published an analysis of Uroburos, the rootkit with Russian roots. We explained that a link exists between Uroburos and the Agent.BTZ malware, which was responsible for 'the most significant breach of U.S. military computers ever.' Nine months later, after the buzz around Uroburos, aka Snake or Turla, we now identified a new generation of Agent.BTZ. We dubbed it ComRAT and, by now, analyzed two versions of the threat (v3.25 and v3.26).
Information	<https://www.gdatasoftware.com/blog/2014/11/23937-the-uroburos-case-new-sophisticated-rat-identified> <http://www.intezer.com/new-variants-of-agent-btz-comrat-found/> <http://www.intezer.com/new-variants-of-agent-btz-comrat-found-part-2/> <https://www.welivesecurity.com/2020/05/26/agentbtz-comratv4-ten-year-journey/>
MITRE ATT&CK	<https://attack.mitre.org/software/S0126/>
AlienVault OTX	<https://otx.alienvault.com/browse/pulses?q=tag:comrat>

Last change to this tool card: 27 May 2020

Download this tool card in JSON format

All groups using tool ComRAT

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=7a9cd633-86ef-4ef1-b6d3-6832edb3a8cc