Cotx RAT - Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-02 12:28:45 UTC

Tool: Cotx RAT

Names	Cotx RAT
Category	Malware
Type	Reconnaissance, Backdoor, Credential stealer
Description	(Proofpoint) The RasTls.dll contains the Cotx RAT code. The malware is written in C++ using object-oriented programming. We named it by borrowing the name of the location of its stored configuration. The encrypted configuration is stored in the side-loaded DLL file RasTls.dll in a PE section named ".cotx". The current encrypted configuration is also stored in the registry key "HKEY_LOCAL_MACHINE\SOFTWARE\Intel\Java\user". The command and control structure of Cotx RAT is proxy aware. It utilizes wolfSSL for TLS encrypted communication. The initial beacon contains "|"-delimited system information. The data included in the beacon is Zlib compressed and encrypted with AES-192 in CBC mode utilizing the same keys as the configuration. The following values are included: • 'id' value from 'software\\intel\\java' subkey • Computer name • 'mark' field from configuration • Username • Windows version • Architecture • Possible malware version. '0.9.7' is hardcoded in the analyzed sample • Local IP addresses • First adapter's MAC address • Connection type (https or _proxy) • 'password' field from configuration
Information	<https://www.proofpoint.com/us/threat-insight/post/chinese-apt-operation-lagtime-it-targets-government-information-technology>
Malpedia	<https://malpedia.caad.fkie.fraunhofer.de/details/win.cotx>

Last change to this tool card: 24 April 2021

Download this tool card in JSON format

All groups using tool Cotx RAT

Changed	Name	Country	Observed	
APT groups				
	TA428		2013-Jan 2022	

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

Source: https://apt.etda.or.th/cgi-bin/listgroups.cgi?u=071fed27-3361-4b37-a553-8e32c65482c8