Cardinal RAT - Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 17:42:53 UTC

Tool: Cardinal RAT

Names	Cardinal RAT
Category	Malware
Type	Reconnaissance, Backdoor, Keylogger, Info stealer, Credential stealer, Downloader, Exfiltration, Tunneling
Description	(Palo Alto) The name Cardinal RAT comes from internal names used by the author within the observed Microsoft .NET Framework executables. To date, 27 unique samples of Cardinal RAT have been observed, dating back to December 2015. It is likely that the low volume of samples seen in the wild is partly responsible for the fact that this malware family has remained under the radar for so long. The malware itself is equipped with a number of features, including the following: • Collect victim information • Update settings • Act as a reverse proxy • Execute command • Uninstall itself • Recover passwords • Download and Execute new files • Keylogging • Capture screenshots • Update Cardinal RAT • Clean cookies from browsers
Information	<https://unit42.paloaltonetworks.com/unit42-cardinal-rat-active-two-years/> <https://unit42.paloaltonetworks.com/cardinal-rat-sins-again-targets-israeli-fin-tech-firms/>
MITRE ATT&CK	<https://attack.mitre.org/software/S0348/>
Malpedia	<https://malpedia.caad.fkie.fraunhofer.de/details/win.cardinal_rat>
AlienVault OTX	<https://otx.alienvault.com/browse/pulses?q=tag:cardinal%20rat>

Last change to this tool card: 30 December 2022

Download this tool card in JSON format

All groups using tool Cardinal RAT

Changed	Name	Country	Observed	
APT groups				
	Evilnum	[Unknown]	2018-2022	

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

Source: https://apt.etda.or.th/cgi-bin/listgroups.cgi?u=fca0a40a-ae80-4525-82ad-ca1cf627344a