Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 17:28:47 UTC

Tool: DDKONG

Names	DDKONG
Category	Malware
Type	Backdoor
Description	(Palo Alto) The malware in question is configured with the following three exported functions: • ServiceMain • Rundll32Call • DllEntryPoint The ServiceMain exported function indicates that this DLL is expected to be loaded as a service. If this function is successfully loaded, it will ultimately spawn a new instance of itself with the Rundll32Call export via a call to rundll32.exe. The Rundll32Call exported function begins by creating a named event named 'RunOnce'. This event ensures that only a single instance of DDKong is executed at a given time. If this is the only instance of DDKong running at the time, the malware continues. If it's not, it dies. This ensures that only a single instance of DDKong is executed at a given time.
Information	<https://unit42.paloaltonetworks.com/unit42-rancor-targeted-attacks-south-east-asia-using-plaintee-ddkong-malware-families/>
MITRE ATT&CK	<https://attack.mitre.org/software/S0255/>
Malpedia	<https://malpedia.caad.fkie.fraunhofer.de/details/win.ddkong>
AlienVault OTX	<https://otx.alienvault.com/browse/pulses?q=tag:DDKONG>

Last change to this tool card: 23 April 2020

Download this tool card in JSON format

All groups using tool DDKONG

Changed	Name	Country	Observed	
APT groups				
	Rancor		2017	

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

Source: https://apt.etda.or.th/cgi-bin/listgroups.cgi?u=84cd6758-4303-4a23-a102-3853651997fa