

Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 22:31:23 UTC

[Home](#) > [List all groups](#) > [List all tools](#) > List all groups using tool RoyalDNS

Tool: RoyalDNS

| | |
|----------------|--|
| Names | RoyalDNS Royal DNS |
| Category | Malware |
| Type | Backdoor , Tunneling |
| Description | RoyalDNS is a DNS based backdoor used by APT15 that persistences on a system through a service called 'Nwsapagent'. |
| Information | < https://www.nccgroup.trust/uk/about-us/newsroom-and-events/blogs/2018/march/apt15-is-alive-and-strong-an-analysis-of-royalcli-and-royaldns/ > < https://github.com/nccgroup/Royal_APT > |
| Malpedia | < https://malpedia.caad.fkie.fraunhofer.de/details/win.royal_dns > |
| AlienVault OTX | < https://otx.alienvault.com/browse/pulses?q=tag:RoyalDNS > |

Last change to this tool card: 28 December 2022

Download this tool card in [JSON](#) format

All groups using tool RoyalDNS

| Changed | Name | Country | Observed |
|-------------------|---|---|---------------|
| APT groups | | | |
| | Ke3chang , Vixen Panda , APT 15 , GREF , Playful Dragon |  | 2010-Oct 2024 |

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