# Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 14:23:59 UTC



## Tool: RoyalCli

| | |
|---|---|
| Names | RoyalCli |
| Category | Malware |
| Type | Backdoor, Info stealer, Exfiltration |
| Description | RoyalCli is a backdoor which appears to be an evolution of BS2005 and uses familiar encryption and encoding routines. The name RoyalCli was chosen by us due to a debugging path left in the binary. RoyalCli and BS2005 both communicate with the attacker's command and control (C2) through Internet Explorer (IE) by using the COM interface IWebBrowser2. |
| 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.royalcli> |
| AlienVault OTX | <https://otx.alienvault.com/browse/pulses?q=tag:RoyalCli> |

Last change to this tool card: 14 May 2020

Download this tool card in JSON format

### All groups using tool RoyalCli

| 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)*

Source: https://apt.etda.or.th/cgi-bin/listgroups.cgi?u=dc1d097f-ddef-41bd-9316-229867d167be