# Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 16:55:42 UTC



## Tool: Joanap

| | |
|---|---|
| Names | Joanap<br>SierraJuliett-MikeOne<br>SierraJuliett-MikeTwo |
| Category | Malware |
| Type | Backdoor, Info stealer |
| Description | (US-CERT) Joanap malware is a fully functional RAT that is able to receive multiple commands, which can be issued by HIDDEN COBRA actors remotely from a command and control server. Joanap typically infects a system as a file dropped by other HIDDEN COBRA malware, which users unknowingly downloaded either when they visit sites compromised by HIDDEN COBRA actors, or when they open malicious email attachments. |
| Information | <https://www.us-cert.gov/ncas/alerts/TA18-149A><br><https://www.acalvio.com/lateral-movement-technique-employed-by-hidden-cobra/> |
| Malpedia | <https://malpedia.caad.fkie.fraunhofer.de/details/win.joanap> |
| AlienVault OTX | <https://otx.alienvault.com/browse/pulses?q=tag:joanap> |

Last change to this tool card: 14 May 2020

Download this tool card in JSON format

### All groups using tool Joanap

| Changed | Name | Country | Observed | |
|---|---|---|---|---|
| **APT groups** | | | | |
| | Lazarus Group, Hidden Cobra, Labyrinth Chollima |  | 2007-May 2025 |  |

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

Source: https://apt.etda.or.th/cgi-bin/listgroups.cgi?u=471c76f9-bbf1-4794-a1ac-4961ff3436af