# Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 18:43:58 UTC



## Tool: Orat

| | |
|---|---|
| Names | Orat |
| Category | Malware |
| Type | Loader |
| Description | (SecureWorks) CTU researchers have only observed this basic loader tool in the context of BRONZE PRESIDENT intrusions. ORat is the name assigned by the malware author, as denoted by the program debug database string in the analyzed sample: D:\vswork\Plugin\ORat\build\Release\ORatServer\Loader.pdb. The tool uses the Windows Management Instrumentation (WMI) event consumer for persistence by installing a script to the system's WMI registry. Messages sent from ORat to its command and control (C2) server start with the string 'VIEWS0018x'. If the data received from the C2 server starts with the same string, then the remainder of the payload is decompressed using ORat's 'deflate' algorithm and called as a function. ORat acts as a flexible loader tool rather than a fully featured remote access tool. |
| Information | <https://www.secureworks.com/research/bronze-president-targets-ngos> |

Last change to this tool card: 04 April 2022

Download this tool card in JSON format

### All groups using tool Orat

| Changed | Name | Country | Observed | |
|---|---|---|---|---|
| **APT groups** | | | | |
| | Mustang Panda, Bronze President | | 2012-Jun 2025 | |

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

Source: https://apt.etda.or.th/cgi-bin/listgroups.cgi?u=19552048-5564-480f-9e53-1411a008c8b4