# Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 15:01:33 UTC

## APT group: Pusikurac

| | |
|---|---|
| Names | Pusikurac *(Morphisec)* |
| Country | [Unknown] |
| Motivation | Information theft and espionage |
| First seen | 2019 |
| Description | (Morphisec) A new, highly sophisticated campaign that delivers the Orcus Remote Access Trojan is hitting victims in ongoing, targeted attacks. Morphisec identified the campaign after receiving notifications from its advanced prevention solution at several deployment sites. (Morphisec's Moving Target Defense technology immediately stopped the threat.) The attack uses multiple advanced evasive techniques to bypass security tools. In a successful attack, the Orcus RAT can steal browser cookies and passwords, launch server stress tests (DDoS attacks), disable the webcam activity light, record microphone input, spoof file extensions, log keystrokes and more.<br><br>The forensic data captured by Morphisec from the attack showed a high correlation to additional samples in the wild, indicating a single threat actor is behind multiple campaigns, including this one.<br><br>This threat actor specifically focuses on information stealing and .NET evasion. Based on unique strings in the malware, we have dubbed the actor PUSIKURAC. Before executing the attacks, PUSIKURAC registers domains through FreeDns services. It also utilizes legitimate free text storage services like paste, signs its executables, heavily misuses commercial .NET packers and embeds payloads within video files and images. |
| Observed | |
| Tools used | Orcus RAT. |
| Information | <https://blog.morphisec.com/new-campaign-delivering-orcus-rat> |

Last change to this card: 29 April 2020

Download this actor card in PDF or JSON format