# NewCore RAT - Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 13:56:46 UTC



## Tool: NewCore RAT

| | |
|---|---|
| Names | NewCore RAT |
| Category | Malware |
| Type | Reconnaissance, Backdoor, Keylogger, Info stealer, Exfiltration, Tunneling |
| Description | (Fortinet) This RAT is a DLL file. Its malicious routines are contained in its imported function “ProcessTrans”. However, executing the DLL without using the downloader will not work as the C&C server string is not embedded in its body. When the downloader calls the function “ProcessTrans”, it supplies to the function the C&C server string and a handle to the C&C server internet session. In this case, Heuristic detection based on behavior will not work on the DLL alone.<br><br>This RAT is capable of the following:<br><br>• Shutdown the machine<br>• Restart the machine<br>• Get disk list<br>• Get directory list<br>• Get file information<br>• Get disk information<br>• Rename files<br>• Copy files<br>• Delete files<br>• Execute files<br>• Search files<br>• Download files<br>• Upload files<br>• Screen monitoring<br>• Start command shell<br><br>NewCore RAT may just be a rehashed PCClient RAT, but it proves to be effective in evading AV detection by using a combination of simple techniques such as DLL- |

| | |
|---|---|
| | hijacking, file-less execution of downloaded malware, and passing C&C information as parameter from downloader to the downloaded file. |
| Information | <https://www.fortinet.com/blog/threat-research/rehashed-rat-used-in-apt-campaign-against-vietnamese-organizations.html><br><https://securelist.com/cycldek-bridging-the-air-gap/97157/> |
| Malpedia | <https://malpedia.caad.fkie.fraunhofer.de/details/win.newcore_rat> |
| AlienVault OTX | <https://otx.alienvault.com/browse/pulses?q=tag:NewCore> |

Last change to this tool card: 04 June 2020

Download this tool card in JSON format

### All groups using tool NewCore RAT

| Changed | Name | Country | Observed | |
|---|---|---|---|---|
| **APT groups** | | | | |
| | Goblin Panda, Cycldek, Conimes |  | 2013-Jun 2020 | |
| | Naikon, Lotus Panda |  | 2010-Apr 2022 | |

*2 groups listed (2 APT, 0 other, 0 unknown)*

---

Source: https://apt.etda.or.th/cgi-bin/listgroups.cgi?u=55a366cc-0771-4854-85a3-5eed99e33f9e