Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 19:04:10 UTC

Tool: Nebulae

Names	Nebulae
Category	Malware
Type	Reconnaissance, Backdoor, Info stealer, Downloader, Exfiltration
Description	(Bitdefender) The analysis of the most recent samples showed that the backdoor is capable of: • Getting LogicalDrive information (Drive type, FreeSpace, VolumeInformation) • Listing, moving and deleting files and directories • Executing a process using CreateProcess or through a CMD shell • Listing and terminating processes • Downloading and uploading files from and to C&C Communication with the C&C is realized by sending and receiving packets of a fixed form through a TCP connection. The format of packets can be visualized on the diagram below and represent an array of bytes of dynamic length with a 77 bytes header that stores the RC4 key used for payload encryption (the key is created by concatenating each fourth byte)
Information	<https://www.bitdefender.com/files/News/CaseStudies/study/396/Bitdefender-PR-Whitepaper-NAIKON-creat5397-en-EN.pdf> <https://www.cybereason.com/blog/deadringer-exposing-chinese-threat-actors-targeting-major-telcos>
MITRE ATT&CK	<https://attack.mitre.org/software/S0630/>
Malpedia	<https://malpedia.caad.fkie.fraunhofer.de/details/win.nebulae>

Last change to this tool card: 30 December 2022

Download this tool card in JSON format

All groups using tool Nebulae

Changed	Name	Country	Observed	
APT groups				
	Naikon, Lotus Panda		2010-Apr 2022	

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

Source: https://apt.etda.or.th/cgi-bin/listgroups.cgi?u=5015e84a-0fd5-4850-9a07-41028e70a7ff