Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-02 12:05:04 UTC

APT group: Mikroceen

Names	Mikroceen *(ESET)* SixLittleMonkeys *(Kaspersky)*	
Country	China	
Motivation	Information theft and espionage	
First seen	2017	
Description	(ESET) In this joint blogpost with fellow researchers from Avast, we provide a technical analysis of a constantly developed RAT that has been used in various targeted campaigns against both public and private subjects since late 2017. We observed multiple instances of attacks involving this RAT, and all of them happened in Central Asia. Among the targeted subjects were several important companies in the telecommunications and gas industries, and governmental entities. Moreover, we connect the dots between the latest campaign and three previously published reports: Kaspersky's Microcin against Russian military personnel, Palo Alto Networks' BYEBY against the Belarussian government and Checkpoint's Vicious Panda against the Mongolian public sector. Also, we discuss other malware that was typically a part of the attacker's toolset together with the RAT. We chose the name Mikroceen to cover all instances of the RAT, in acknowledgement of Kaspersky's initial report on the family. The misspelling is intentional, in order to avoid the established microbiological notion, but also to have at least phonemic agreement.	
Observed	Sectors: Defense, Government, Oil and gas, Telecommunications. Countries: Belarus, Mongolia, Russia and Central Asia.	
Tools used	Gh0st RAT, logon.dll, logsupport.dll, Microcin, Mimikatz, pcaudit.bat, sqllauncher.dll.	
Operations performed	Mar 2021	Exchange servers under siege from at least 10 APT groups <https://www.welivesecurity.com/2021/03/10/exchange-servers-under-siege-10-apt-groups/>

Information	<https://www.welivesecurity.com/2020/05/14/mikroceen-spying-backdoor-high-profile-networks-central-asia/> <https://decoded.avast.io/luigicamastra/apt-group-planted-backdoors-targeting-high-profile-networks-in-central-asia/> <https://securelist.com/microcin-is-here/97353/>

Last change to this card: 20 April 2021

Download this actor card in PDF or JSON format
