Threat Group Cards: A Threat Actor Encyclopedia

APT group: RedGolf

Names	RedGolf *(Recorded Future)*
Country	China
Sponsor	State-sponsored
Motivation	Information theft and espionage
First seen	2014
Description	(Recorded Future) Recorded Future's Insikt Group has identified a large cluster of new operational infrastructure associated with use of the custom Windows and Linux backdoor KEYPLUG. We attribute this activity to a threat activity group tracked as RedGolf, which is highly likely to be a Chinese state-sponsored group. RedGolf closely overlaps with threat activity reported in open sources under the aliases APT 41/Barium and has likely carried out state-sponsored espionage activity in parallel with financially motivated operations for personal gain from at least 2014 onward. A 2020 US Department of Justice indictment states that a RedGolf-associated threat actor boasted of connections to the Chinese Ministry of State Security (MSS); the indicted actors were also linked to the Chengdu-based company Chengdu 404 Network Technology (成都市肆零肆网络科技有限公司).
Observed	Sectors: Aviation, Automotive, Education, Government, IT, Media and religious organizations. Countries: USA.
Tools used	Cobalt Strike, KEYPLUG, PlugX.
Information	<https://go.recordedfuture.com/hubfs/reports/cta-2023-0330.pdf>

Last change to this card: 13 March 2024

Download this actor card in PDF or JSON format