Winter Vivern - Threat Group Cards: A Threat Actor Encyclopedia

APT group: Winter Vivern

Names	Winter Vivern *(SentinelLabs)* UAC-0114 *(CERT-UA)* TA473 *(Proofpoint)* UNC4907 *(Mandiant)* TAG-70 *(Recorded Future)*
Country	[Unknown]
Motivation	Information theft and espionage
First seen	2020
Description	(SentinelLabs) The Winter Vivern Advanced Persistent Threat (APT) is a noteworthy yet relatively underreported group that operates with pro-Russian objectives. DomainTools initially publicized the group in early 2021, naming it based on an initial command-and-control beacon URL string “wintervivern,” which is no longer in use. Subsequently, Lab52 shared additional analysis several months later, identifying new activity associated with Winter Vivern. The group has avoided public disclosure since then, until recent attacks targeting Ukraine. A part of a Winter Vivern campaign was reported in recent weeks by the Polish CBZC, and then the Ukraine CERT as UAC-0114. In this activity, CERT-UA and the CBZC collaborated on the release of private technical details which assisted in our research to identify a wider set of activity on the threat actor, in addition to new victims and previously unknown specific technical details. Overall, we find that the Winter Vivern APT is a resource-limited but highly creative group that shows restraint in the scope of their attacks. Our analysis indicates that Winter Vivern activity aligns closely with global objectives that support the interests of Belarus and Russia’s governments. Also see MoustachedBouncer.

Observed	Sectors: Defense, Government. Countries: Georgia, India, Lithuania, Moldova, Poland, Slovakia, Tunisia, Ukraine, USA, Uzbekistan and Europe.	
Tools used	APERETIF.	
Operations performed	Early 2023	Exploitation is a Dish Best Served Cold: Winter Vivern Uses Known Zimbra Vulnerability to Target Webmail Portals of NATO-Aligned Governments in Europe <https://www.proofpoint.com/us/blog/threat-insight/exploitation-dish-best-served-cold-winter-vivern-uses-known-zimbra-vulnerability>
	Jul 2023	Zimbra 0-day used to target international government organizations <https://blog.google/threat-analysis-group/zimbra-0-day-used-to-target-international-government-organizations/>
	Oct 2023	Winter Vivern exploits zero-day vulnerability in Roundcube Webmail servers <https://www.welivesecurity.com/en/eset-research/winter-vivern-exploits-zero-day-vulnerability-roundcube-webmail-servers/>
	Oct 2023	Russia-Aligned TAG-70 Targets European Government and Military Mail Servers in New Espionage Campaign <https://go.recordedfuture.com/hubfs/reports/cta-2024-0217.pdf>
Information	<https://www.sentinelone.com/labs/winter-vivern-uncovering-a-wave-of-global-espionage/> <https://www.domaintools.com/resources/blog/winter-vivern-a-look-at-re-crafted-government-maldocs/> <https://lab52.io/blog/winter-vivern-all-summer/>	

Last change to this card: 07 March 2024

Download this actor card in PDF or JSON format
