Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 17:42:38 UTC

APT group: UNC2891

Names	UNC2891 *(Mandiant)*
Country	[Unknown]
Motivation	Financial gain
First seen	2020
Description	(Mandiant) The Mandiant Advanced Practices team previously published a threat research blog post that provided an overview of UNC1945 (LightBasin) operations where the actor compromised managed services providers to gain access to targets in the financial and professional consulting industries. Since that time, Mandiant has investigated and attributed several intrusions to a threat cluster we believe has a nexus to this actor, currently being tracked as UNC2891. Through these investigations, Mandiant has discovered additional techniques, malware, and utilities being used by UNC2891 alongside those previously observed in use by UNC1945. Despite having identified significant overlaps between these threat clusters, Mandiant has not determined they are attributable to the same actor.
Observed	Sectors: Financial.
Tools used	BINBASH, CAKETAP, MIGLOGCLEANER, SLAPSTICK, STEELCORGI, STEELHOUND, SUN4ME, Tiny SHell, WINGCRACK, WINGHOOK, WIPERIGHT.
Information	<https://www.mandiant.com/resources/unc2891-overview>

Last change to this card: 03 April 2022

Download this actor card in PDF or JSON format