Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-06 02:12:49 UTC

Other threat group: TA551, Shathak

Names	TA551 *(Proofpoint)* Gold Cabin *(SecureWorks)* Shathak *(?)* Monster Libra *(Palo Alto)* G0127 *(MITRE)*	
Country	Russia	
Motivation	Financial gain	
First seen	2016	
Description	(Palo Alto) TA551 (also known as Shathak) is an email-based malware distribution campaign that often targets English-speaking victims. The campaign discussed in this blog has targeted German, Italian and Japanese speakers. TA551 has historically pushed different families of information-stealing malware like Ursnif and Valak. After mid-July 2020, this campaign has exclusively pushed IcedID malware, another information stealer.	
Observed		
Tools used	BokBot, Gozi, Sliver, Valak.	
Operations performed	Oct 2021	TA551 Uses 'SLIVER' Red Team Tool in New Activity <https://www.proofpoint.com/us/blog/security-briefs/ta551-uses-sliver-red-team-tool-new-activity>
	Jan 2021	From IcedID to Domain Compromise <https://www.cybereason.com/blog/threat-analysis-from-icedid-to-domain-compromise>
Information	<https://unit42.paloaltonetworks.com/ta551-shathak-icedid/> <https://unit42.paloaltonetworks.com/valak-evolution/> <https://github.com/pan-unit42/iocs/tree/master/TA551>	
MITRE ATT&CK	<https://attack.mitre.org/groups/G0127/>	

Playbook	<https://pan-unit42.github.io/playbook_viewer/?pb=monsterlibra>

Last change to this card: 16 August 2025

Download this actor card in PDF or JSON format
