Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 12:55:18 UTC

APT group: LightBasin

Names	LightBasin *(CrowdStrike)* UNC1945 *(FireEye)* TH-239 *(Yoroi)* DecisiveArchitect *(CrowdStrike)* Luminal Panda *(CrowdStrike)*
Country	China
Motivation	Information theft and espionage
First seen	2016
Description	(CrowdStrike) CrowdStrike Services, CrowdStrike Intelligence and Falcon OverWatch™ have investigated multiple intrusions within the telecommunications sector from a sophisticated actor tracked as the LightBasin activity cluster, also publicly known as UNC1945. Active since at least 2016, LightBasin employs significant operational security (OPSEC) measures, primarily establishing implants across Linux and Solaris servers, with a particular focus on specific telecommunications systems,1 and only interacting with Windows systems as needed. LightBasin's focus on Linux and Solaris systems is likely due to the combination of critical telecommunications infrastructure running on those operating systems, in addition to the comparatively lax security measures and monitoring solutions on Linux/Solaris systems that are typically in place on Windows operating systems within an organization. LightBasin managed to initially compromise one of the telecommunication companies in a recent CrowdStrike Services investigation by leveraging external DNS (eDNS) servers — which are part of the General Packet Radio Service (GPRS) network and play a role in roaming between different mobile operators — to connect directly to and from other compromised telecommunication companies' GPRS networks via SSH and through previously established implants. CrowdStrike identified evidence of at least 13 telecommunication companies across the world compromised by LightBasin dating back to at least 2019. There is some overlap with UNC2891.
Observed	Sectors: Financial, IT, Telecommunications.
Tools used	CordScan, EVILSUN, FRP, Impacket, LEMONSTICK, LOGBLEACH, OKSOLO, OPENSHACKLE, ProxyChains, PupyRAT, SIGTRANslator, SLAPSTICK, SMBExec,

	STEELCORGI, Tiny SHell, Living off the Land.
Information	<https://www.crowdstrike.com/blog/an-analysis-of-lightbasin-telecommunications-attacks/> <https://www.mandiant.com/resources/live-off-the-land-an-overview-of-unc1945> <https://www.crowdstrike.com/en-us/blog/liminal-panda-telecom-sector-threats/>

Last change to this card: 26 December 2024

Download this actor card in PDF or JSON format
