Threat Group Cards: A Threat Actor Encyclopedia

Tool: SierraAlfa

Names	SierraAlfa
Category	Malware
Type	Worm, Loader
Description	(Novetta) A self-install service-based executable, SierraAlfa begins a chain of infection that ultimately leads to the potential devastation of an entire network of computers. SierraAlfa is responsible for the distribution and activation of WhiskeyAlfa on a victim's network. The observed samples of SierraAlfa were clearly built specifically for the SPE attacks as they contain infrastructure and account information specific to SPE's networks. Two variants have been observed: SierraAlfa-One and SierraAlfa-Two. SierraAlfa-One is the base model, while SierraAlfa-Two provides additional features to ensure the propagation of the malicious payload within.
Information	<https://www.operationblockbuster.com/wp-content/uploads/2016/02/Operation-Blockbuster-RAT-and-Staging-Report.pdf>

Last change to this tool card: 20 April 2020

Download this tool card in JSON format

All groups using tool SierraAlfa

Changed	Name	Country	Observed	
APT groups				
	Lazarus Group, Hidden Cobra, Labyrinth Chollima		2007-May 2025	

1 group listed (1 APT, 0 other, 0 unknown)