Threat Group Cards: A Threat Actor Encyclopedia

Tool: QUEUESEED

Names	QUEUESEED IcyWell Kapeka
Category	Malware
Type	Backdoor
Description	(BleepingComputer) C++ backdoor for Windows that collects basic system information and executes commands from a remote server. It handles file operations, command execution, and configuration updates and can delete itself. Communications are secured via HTTPS, and data is encrypted using RSA and AES. It stores its data and maintains persistence on infected systems by encrypting its configuration in the Windows registry and setting up tasks or registry entries for automatic execution.
Information	<https://www.bleepingcomputer.com/news/security/russian-sandworm-hackers-targeted-20-critical-orgs-in-ukraine/>

Last change to this tool card: 23 April 2024

Download this tool card in JSON format

All groups using tool QUEUESEED

Changed	Name	Country	Observed	
APT groups				
	Sandworm Team, Iron Viking, Voodoo Bear		2009-Dec 2024	

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