Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 14:46:56 UTC

Tool: PHOREAL

Names	PHOREAL Rizzo
Category	Malware
Type	Backdoor
Description	(Cylance) Rizzo is a very simple backdoor that is capable of creating a reverse shell, performing simple file I/O and top-level window enumeration. It communicates to a list of four preconfigured C2 servers via ICMP on port 53.
Information	<https://www.cylance.com/content/dam/cylance-web/en-us/resources/knowledge-center/resource-library/reports/SpyRATsofOceanLotusMalwareWhitePaper.pdf>
MITRE ATT&CK	<https://attack.mitre.org/software/S0158/>
Malpedia	<https://malpedia.caad.fkie.fraunhofer.de/details/win.phoreal>
AlienVault OTX	<https://otx.alienvault.com/browse/pulses?q=tag:PHOREAL>

Last change to this tool card: 23 April 2020

Download this tool card in JSON format

All groups using tool PHOREAL

Changed	Name	Country	Observed	
APT groups				
	APT 32, OceanLotus, SeaLotus		2013-Aug 2024	

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