Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 18:51:29 UTC

Tool: Rifdoor

Names	Rifdoor
Category	Malware
Type	Backdoor
Description	(AhnLab) Rifdoor was first discovered in November 2015, and it remained active until early 2016. A Rifdoor variant v to attack SEOUL ADEX exhibitors in 2015 and was found in the hacking incidents of security companies in early 201 When it enters the system, Rifdoor generates a file by adding garbage data to the 4 bytes of the last part of the file. Th since the hash value changes each time the system is infected, the malware cannot be found in the system with a simpl value.
Information	<https://global.ahnlab.com/global/upload/download/techreport/%5BAhnLab%5DAndariel_a_Subgroup_of_Lazarus% <https://www.carbonblack.com/2020/04/16/vmware-carbon-black-tau-threat-analysis-the-evolution-of-lazarus/>
MITRE ATT&CK	<https://attack.mitre.org/software/S0433/>
Malpedia	<https://malpedia.caad.fkie.fraunhofer.de/details/win.rifdoor>
AlienVault OTX	<https://otx.alienvault.com/browse/pulses?q=tag:Rifdoor>

Last change to this tool card: 30 December 2022

Download this tool card in JSON format

All groups using tool Rifdoor

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

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