


Mphasis SOC – Information Security News
Date & Time Issued: 06-JUL-2024, 14:30 IST

Title	New Volcano Demon Ransomware	
Summary	<ul style="list-style-type: none"> A novel malware known as Volcano Demon has been observed targeting Windows workstations and servers, obtaining administrative credentials from the network. The threat actor doesn't have a leak site and instead uses phone calls to executives in IT and leadership to demand and demand for money. The Volcano Demon ransomware group, first reported by cybersecurity researchers in July 2024, has been active since at least June 2024. The group primarily targets organizations in the manufacturing and logistics sectors. 	
Severity	Medium 	
Attack Vectors	<ul style="list-style-type: none"> Volcano Demon was successful in locking both Windows workstations and servers after utilizing common administrative credentials harvested from the network. Prior to the attack, data was exfiltrated to C2 services for double extortion techniques. Once inside the system, the group deploys its flag ransomware strain, LukaLocker, an x64 PE binary written and compiled using C++. LukaLocker has both Windows and Linux variants. Before the encryption, the ransomware terminates various antivirus and endpoint protection solutions, backup and recovery tools, database and virtualization software, email servers (Microsoft Exchange), and remote access and monitoring tools. Then, it encrypts files using the Chacha8 cipher while appending them with the .nba extension. To thwart analysis mechanisms and evade detection, LukaLocker employs API obfuscation and dynamic API resolution. In addition, the threat actor's clear activity logs to cover their tracks. Volcano Demon does not maintain a data leak website, but rather uses phone calls to leadership and IT executives to extort them into paying a ransom. 	
Indicator of Compromise	INDICATOR TYPE	INDICATORS
	File hashes	<ul style="list-style-type: none"> f83abe3d9717238755f1276c87b3b320d8c30421984a897099ce3741d9143906 4e58629158a6c46ad420f729330030f5e0b0ef374e9bb24cd203c89ec3262669

Recommendations	<ul style="list-style-type: none">• Security administrators should block IOCs on all applicable security solutions post-validation.• Implement multi-factor authentication (MFA) and credential-based access solutions.• Use Endpoint Detection and Response (EDR) to quickly identify and respond to ransomware indicators.• Take data backups regularly to minimize damage and data loss.• Prioritize and periodically apply security patches to fix vulnerabilities.• Educate and train employees to recognize and report cybersecurity threats.• Conduct annual technical audits or security assessments and maintain digital hygiene.• Refrain from paying ransom as it rarely ensures data recovery and can lead to more attacks. <p>NOTE: The recommended settings/controls should be implemented after due shall be tested on Pre-Prod or test environment before implementing. diligence and impact analysis.</p>
References	<ul style="list-style-type: none">• https://www.halcyon.ai/blog/halcyon-identifies-new-ransomware-operator-volcano-demon-serving-up-lukalocker• https://cybersecuritynews.com/ransomware-threats-via-phone-calls/
<p>The information contained in this message is proprietary. It is for Mphasis and its customers only. Copyright © 2024. All rights reserved by Mphasis.</p>	