orova Ransomware Group Profile | SOCRadar

By SOCRadar

Archived: 2026-08-10 02:00:17 UTC

1. Ransomware Intelligence
2. Groups
3. orova

Description

Orova is a newly emerged ransomware extortion group that has been active since mid-2026. They focus on compromising corporate networks and leveraging data exfiltration to enforce ransom payments, utilizing a dedicated data leak site on the dark web to publish stolen files if demands are not met.

Key insights

- •Orova employs a data leak site to pressure victims into paying ransom.
- •The group's operations are aligned with modern data-theft extortion tactics.
- •They target corporate networks primarily.
- •Orova has been active since mid-2026.
- •Victims face public exposure of stolen proprietary data.
- •Their model includes both data encryption and data exfiltration.

Threat Level & Status Breakdown

For orova · Based on incidents in selected period

4.2threat level

Aggressiveness10/ 10

Lethality0/ 10

⚡

Criticality2.4/ 10

Status Breakdown

Claimed100.0%35

First seenMay 2026

Last seenAug 2026

Avg ransom—

Payment rate—

Statusactive

Sophistication0

Last updatedAug 9, 2026

Recent activity

Monthly attack count for orova in the selected period

35Total attacks

16peak in Aug

8.8avg / month

↑ 9 vs first month

No intelligence data for this group.

TTPs & Attack Vectors

Tools, initial access, and MITRE ATT&CK techniques for orova

Defense Evasion

T1562

Impair Defenses

Execution

T1140

Deobfuscate/Decode Files or Information

Impact

T1486

Data Encrypted for Impact

T1490

Inhibit System Recovery

Lateral Movement

T1021

Remote Services

Other

T1071.001

T1071.001

T1040

T1040

T1550

T1550

T811

T811

Persistence

T1078

Valid Accounts

T1547

Boot or Logon Autostart Execution

Victims(35)

Company	Domain	Country	Industry	Status	Discovered	
Stoneybrook West	stoneybrookwest.sites.townsq.io	United States	Other	Claimed	4 days ago	>
mystcc	mystcc.org	United States	Other	Claimed	4 days ago	>
Stonecrest POA	stonecrestpoa.com	United States	Other	Claimed	4 days ago	>
Country Oaks Veterinary Clinic	vetstopets.com	United States	Healthcare	Claimed	4 days ago	>
Hilliard's Air Conditioning & Heating Inc	hilliardsairandheat.com	United States	Professional Services	Claimed	4 days ago	>
Magnolia Dental Clinic	magnoliadentalclinic.com	United States	Healthcare	Claimed	4 days ago	>
First Baptist Church of Belleview	fbcbelleview.org	United States	Other	Claimed	4 days ago	>
Gemstone UK	gemstoneuk.com	United States	Other	Claimed	4 days ago	>
Woodside Ranch	ricewoodside.com	United States	Other	Claimed	4 days ago	>
MapQuest	mapquest.com	United States	Professional Services	Claimed	4 days ago	>
FixIT Tek	fixittek.com	United States	Technology	Claimed	5 days ago	>
JK Capital Management Limited	jkcapitalmanagement.com	Hong Kong	Financial Services	Claimed	6 days ago	>
Global Friction Products, Inc.	globalfrictionproducts.com	United States	Manufacturing	Claimed	6 days ago	>

Company	Domain	Country	Industry	Status	Discovered	
Conceptual Designs, Inc.	conceptualdesignsinc.com	United States	Other	Claimed	6 days ago	›
Integrated Site Management	ism-sc.com	United States	Professional Services	Claimed	6 days ago	›
Tat Fung Textile Co. Ltd.	tatfung-tex.com	Hong Kong	Manufacturing	Claimed	6 days ago	›
Sanrio Hong Kong Co., Ltd	sanrio.com.hk	Hong Kong	Retail & E-Commerce	Claimed	6 days ago	›
S.S.I. Holding (Far East) Limited	ssife.com	Hong Kong	Other	Claimed	6 days ago	›
KINGSSON Co., Ltd.	kingsson.com.tw	Taiwan	Other	Claimed	6 days ago	›
Yost Home Improvements	yosthomeimprovements.com	United States	Retail & E-Commerce	Claimed	6 days ago	›

Page 1 of 2

Affected countries(7)

Countries where this group has been reported to target or leak victims.

Source: https://socradar.io/free-tools/ransomware-intelligence/groups/orova