

gammax Ransomware Group Profile | SOCRadar

By SOCRadar

Archived: 2026-08-09 02:00:10 UTC

1. [Ransomware Intelligence](#)
2. > [Groups](#)
3. > gammax

Description

Gammax is a newly emerged extortion and crypto-ransomware operation that began in July 2026, focusing on commercial enterprises and utilities. The group employs a double-extortion model by exfiltrating sensitive data before encrypting files, using a dedicated dark web leak site to compel ransom payments from victims.

Key insights

- Targets small-to-medium businesses and utilities primarily for financial gain.
- Utilizes a double-extortion model, threatening public release of exfiltrated data if ransoms are not paid.
- Gains initial access through targeted phishing, weak RDP exploits, and leaked credentials.
- Employs rapid data exfiltration tactics to pressure victims into paying ransoms.
- Caches communications via Tor for anonymity and conducts attacks with obfuscated malicious scripts.

Threat Level & Status Breakdown

For gammax · Based on incidents in selected period



0.7threat level



Aggressiveness2/ 10



Lethality0/ 10



Criticality0/ 10

 Status Breakdown

Claimed100.0%4

First seenJul 2026

Last seenAug 2026

Avg ransom—

Payment rate—

Statusactive

Sophistication0

Last updatedAug 8, 2026

Recent activity

Monthly attack count for gammax in the selected period

4Total attacks

2peak in Jul

2avg / month

No intelligence data for this group.

TTPs & Attack Vectors

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

Defense Evasion

T1562

Impair Defenses

Execution

T1059

Command and Scripting Interpreter

T1140

Deobfuscate/Decode Files or Information

T1105

Ingress Tool Transfer

Impact

T1486

Data Encrypted for Impact

T1490

Inhibit System Recovery

Lateral Movement

T1021

Remote Services

T1021.001

Remote Desktop Protocol

Other

T1041

T1041

T1203

T1203

Persistence

T1078

Valid Accounts

T1547

Boot or Logon Autostart Execution



Victims(4)

Company	Domain	Country	Industry	Status	Discovered	
King International LLC	kingsinternational.us	United States	Other	Claimed	2 days ago	>
شركة – MTCO محمود الطحيني وشركاه للتجارة	mtest.com.sa	Saudi Arabia	Professional Services	Claimed	8 days ago	>
AguAseo	aguaseo.com	Colombia	Energy & Utilities	Claimed	9 days ago	>
RE/MAX 1st Choice	remax-1stchoice.com	Canada	Retail & E-Commerce	Claimed	9 days ago	>

Affected countries(6)

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

Source: <https://socradar.io/free-tools/ransomware-intelligence/groups/gammax>