THREAT CURE
RE-ARCHITECT YOUR THREAT LANDSCAPE

ThreatCure

Cyber Threat Advisory

FunSec Ransomware

Threat Actor Malware

CATEGORY

Malware [Ransomware]

SEVERITY

High

Platforms

Windows and Linux

IMPACT

- **Double Extortion Tactics:** Encryption of critical data coupled with theft to pressure victims.
- **Massive Data Leaks:** Alleged publication of over 85 victim datasets.
- **Hacktivism Crossover:** FunkSec's tactics blur lines between hacktivism and cybercrime.

Description

FunkSec, a newly emerged ransomware group, gained prominence in December 2024 by claiming over 85 victims within a month. Operating as a Ransomware-as-a-Service (RaaS), FunkSec employs double extortion tactics, combining data theft and encryption to pressure victims into paying ransoms. Their activities indicate possible ties to hacktivist operations and suggest an inexperienced group leveraging AI-assisted tool development.

The group launched a data leak site (DLS) in December 2024, centralizing their activities and featuring breach announcements, a custom DDoS tool, and their ransomware offering. FunkSec is characterized by unusually low ransom demands, sometimes as low as $10,000, and selling stolen data to third parties at discounted prices.

Recently, FunkSec has been observed targeting organizations in Pakistan, leveraging its double extortion tactics against entities in critical sectors. This activity highlights the increasing focus of ransomware groups on organizations within South Asia.

Indicator of Compromise

SHA256

c233aec7917cf34294c19dd60ff79a6e0fac5ed6f0cb57af98013c08201a7a1c
66dbf939c00b09d8d22c692864b68c4a602e7a59c4b925b2e2bef57b1ad047bd
dcf536edd67a98868759f4e72bcbd1f4404c70048a2a3257e77d8af06cb036ac
b1ef7b267d887e34bf0242a94b38e7dc9fd5e6f8b2c5c440ce4ec98cc74642fb
5226ea8e0f516565ba825a1bbed10020982c16414750237068b602c5b4ac6abd
e622f3b743c7fc0a011b07a2e656aa2b5e50a4876721bcf1f405d582ca4cda22
20ed21bfdb7aa970b12e7368eba8e26a711752f1cc5416b6fd6629d0e2a44e5d
dd15ce869aa79884753e3baad19b0437075202be86268b84f3ec2303e1ecd966
7e223a685d5324491bcacf3127869f9f3ec5d5100c5e7cb5af45a227e6ab4603

MD5

c5c47f7a17ef4533d1c162042aa0313b
61d7585b5702d195bc35e0be2f75915c
2456fdd65bc48203815f22e444d78fb0
54e383ca658ebd3caaf586f032f1c401
54e383ca658ebd3caaf586f032f1c401
834c7fd865eee5f7e17a3a1fb62e7051
ca8ff8fb255a47d4be94af4ee3327c07
039f85a7670428430274476cbe733db4
f7a3a35cde86dc89bc76dbb59d5ce6de

Remediation

- Conduct regular vulnerability scans and address detected issues.
- Reset potentially compromised account passwords.
- Enforce multi-factor authentication (MFA) on all critical systems.
- Maintain offline, encrypted backups of critical data.
- Educate employees on phishing and social engineering tactics.
- Conduct simulated phishing and ransomware attacks for awareness.
- Notify internal stakeholders, regulators, and affected parties as required.
- Adopt Zero Trust principles to minimize the attack surface.
- Assess and secure third-party vendors to strengthen supply chain security.
- Block all IOCs on your XDR, EDR and other security tools.

ThreatCure

Cyber Threat Advisory

Secure your byte world

FunSec Ransomware

Threat Actor Malware

Get Started Today

For more information about the ThreatCure ShieldOps Platform
or to schedule a demo, please contact:

- Website: www.threatcure.net
- Email: info@threatcure.net

THREAT CURE
RE-ARCHITECT YOUR THREAT LANDSCAPE