R

Royal Ransomware: Intrusion and Response

Royal was a human-operated ransomware operation first reported in 2022. Its intrusions combined initial access, credential abuse, data theft, and encryption.

PUBLISHER
Gridinsoft Support

UPDATED
Jul 17, 2026

READ TIME
2 min

What it is

Royal was a human-operated ransomware threat that emerged in 2022 and targeted organizations in sectors such as healthcare, manufacturing, communications, and education. Public advisories described it as a private group rather than a typical open ransomware-as-a-service program. Operators also used data theft to increase pressure on victims.

How it works

Reported entry paths included phishing, malicious advertising that led to fake software downloads, callback-based social engineering, and compromised remote access. After entry, attackers used legitimate administration tools and credential access to move through networks, collect data, weaken defenses, and deploy the Royal encryptor broadly.

Key points

- The distinction from public RaaS matters because not every ransomware operation uses interchangeable outside affiliates.
- Remote-management tools can be legitimate, so timing, user, command line, and destination provide essential context.
- Encryption may be the last visible stage of an intrusion that already exposed sensitive information.

What to do

- Contain affected identities and network segments and protect backup administration immediately.
- Review fake software, callback phishing, remote tools, and privileged logins for the original path.
- Preserve evidence of collection and exfiltration for breach assessment.
- Rebuild clean systems and rotate credentials before restoring normal connectivity.

Historical name and defensive value

Royal is a historical ransomware name; government advisories later tracked related activity as BlackSuit. Keep detections based on behavior, not only a family label: unusual remote management, new privileged sessions, bulk file access, backup tampering, and outbound transfer before encryption. Review phishing and malvertising as common entry paths, then use the ransomware response checklist for containment and recovery.