R

Royal and BlackSuit Ransomware: Detection and Response

Royal was a human-operated ransomware operation later tracked by U.S. agencies as rebranded BlackSuit activity. Learn how to investigate and respond safely.

PUBLISHER
Gridinsoft Support

UPDATED
Oct 8, 2026

READ TIME
4 min

CONTENTS

In this guide

01 Royal, BlackSuit, and naming
02 How an intrusion may unfold
03 Evidence to preserve
04 Immediate containment
05 Eradication and recovery
06 Reducing risk
07 Ransom and communications considerations
08 Frequently asked questions

Quick answer: Royal was a human-operated ransomware group and malware family active from 2022. U.S. agencies later updated their advisory to track the actors' rebrand as BlackSuit. Incidents may involve credential access, legitimate remote tools, data theft, and encryption. Defenders should use current behavior and evidence rather than rely only on an old Royal ransom-note name, extension, or IP list.

01 Royal, BlackSuit, and naming

Threat names can refer to a group, malware, encryption payload, or cluster of activity. In August 2024, the FBI and CISA updated their joint advisory to describe Royal actors' rebrand as BlackSuit and added related tactics, indicators, and detection guidance. See the current BlackSuit (Royal) advisory.

This relationship does not mean every BlackSuit-like sample proves the same people conducted an intrusion, or that old Royal indicators remain current forever. Record whether attribution is based on malware code, note style, infrastructure, victim communication, or a broader investigation.

02 How an intrusion may unfold

1. **Initial access:** actors may use phishing, stolen credentials, remote services, vulnerable public applications, or access obtained from another criminal.
2. **Discovery:** they enumerate identities, domain systems, servers, virtualization, backups, and security tools.
3. **Privilege and movement:** compromised accounts and legitimate administration or remote-management tools can help reach additional systems.
4. **Data theft:** sensitive information may be collected and transferred for double-extortion pressure.
5. **Defense evasion and encryption:** actors may interfere with security, logs, or recovery services before encrypting local and network data.

The sequence and tools vary. An incident discovered before encryption can still be a serious identity and data breach.

03 Evidence to preserve

- the ransom note, encrypted samples, extension, executable hash, process tree, and command line;
- endpoint alerts and activity involving security, backup, remote-access, scripting, or credential tools;
- authentication, VPN, identity-provider, and privileged account events;
- DNS, proxy, firewall, and data-transfer records;
- administrative actions in domain, RMM, hypervisor, cloud, and backup consoles;
- the earliest suspicious email, exploit, account use, or remote session.

Old IoCs from a public advisory are useful for historical hunting but are not a complete detection strategy. Infrastructure changes, and many tools used during ransomware intrusions also have legitimate purposes.

04 Immediate containment

1. **Isolate affected hosts and segments.** Stop active encryption and lateral movement while preserving representative evidence.
2. **Protect identity systems.** Disable confirmed compromised accounts, revoke sessions, and rotate privileged and service credentials from clean administration systems.
3. **Secure management planes.** Review domain, remote-management, virtualization, cloud, and backup consoles for unauthorized access and persistence.
4. **Protect backups.** Prevent attacker access without overwriting clean recovery points.
5. **Determine scope and data impact.** Find the first access, affected organizations and systems, exposed data, and regulatory or contractual obligations.

6. **Engage response partners.** Follow the incident plan and involve legal, privacy, insurance, law enforcement, and national cyber authorities as appropriate.

05 Eradication and recovery

Remove the initial access path and all persistence before broad restoration. Rebuild systems whose integrity is uncertain, especially domain, management, virtualization, and backup infrastructure. Reset secrets in an order that does not expose new credentials to compromised systems.

Restore verified clean data into a segmented recovery environment, validate essential applications and dependencies, and reconnect by business priority. Monitor for repeated access, privilege changes, data transfer, and encryption. Decryption alone does not remove an intruder or address stolen data.

06 Reducing risk

Prioritize actively exploited vulnerabilities on public services, require phishing-resistant MFA for remote and privileged access, and remove dormant accounts. Separate administrator identities from email and browsing, limit service-account privileges, and segment management, backups, endpoints, and servers.

Centralize tamper-resistant endpoint, identity, DNS, and network logs. Alert on new remote tools, mass file changes, backup-policy modification, unusual service creation, and high-volume transfers. Maintain offline or immutable backups under separate credentials and test full recovery, including identity services.

07 Ransom and communications considerations

Payment does not guarantee working decryption, deletion of stolen data, or protection from later extortion. It may create legal and sanctions concerns. Decisions require executive, legal, insurance, law-enforcement, and incident-response input. Communicate with an actor only through an approved clean channel and preserve all messages.

08 Frequently asked questions

Are Royal and BlackSuit the same?

U.S. government reporting describes Royal actors as rebranding to BlackSuit. Use the name with its evidence and date because malware and actor labels can evolve.

Does no encryption mean no incident?

No. Credentials and data may have been stolen before encryption, or defenders may have interrupted the attack.

Can old Royal hashes protect us now?

They help detect known historical files but must be combined with behavior, identity, and current threat intelligence.

NEED MORE HELP?

We are here when the guide is not enough.

Visit the Gridinsoft Support Center for current product guidance or submit a support request with the details of your case.

Open this guide online at support.gridinsoft.com