# TIR-20240917 Royal Rebrands as BlackSuit Ransomware

*9/17/2024*

Prepared for:

Aspire Technology Partners
25 James Way
Eatontown, NJ 07724

**NOTICE:**

*This document is marked TLP: CLEAR, allowing recipients to share this information globally without any disclosure limitations.*

*This report is governed by the terms outlined in the Master Services Agreement (MSA) or any other master agreement between Aspire Technology Partners and the client receiving this report, along with the Statement of Work (SOW) or Order detailing the services that led to its creation.*



**Contributor(s)**

**Portia S. Cole**
CTI Threat Researcher
Aspire Technology Partners
pcole@aspiretransforms.com

# Table of Contents

# Executive Summary

The BlackSuit ransomware operation surfaced in April/May 2023, quickly becoming a significant threat with its multi-layered extortion tactics. This group not only encrypts sensitive data but also steals it, using public data leak sites to pressure victims who don't comply with their ransom demands.

BlackSuit has carried out notable attacks on the healthcare and education sectors, as well as other critical industries. Unlike many other ransomware groups, BlackSuit operates privately without known public partners. Its ransomware shares many technical characteristics with Royal ransomware, including similar encryption techniques and command-line parameters.

BlackSuit's attack strategy is calculated, starting with data theft and extortion before proceeding to system encryption. If victims refuse to pay the ransom, their stolen data is publicly exposed on a leak site. Let's explore BlackSuit's tactics and techniques and discuss how your organization can protect itself against this type of threat actor.

**TIR Snapshot**

- In 2023, researchers found that Royal ransomware, which first appeared in January 2022, was rebranding as BlackSuit.
  - Initially targeting U.S. entities, Royal escalated its attacks by using encryptors from other groups like BlackCat before developing its own Zeon encryptor. By November 2022, Royal disrupted events at the Silverstone Circuit and later targeted the Travis Central Appraisal District in December.
  - The group used various methods to spread their ransomware, including malicious ads and phishing.
- BlackSuit, now sharing similar code with Royal but with enhanced capabilities, uses a selective encryption method to improve speed and evade detection. It also uses double extortion, threatening to release exfiltrated data if the ransom is not paid.
- In May 2024, BlackSuit took responsibility for a breach at Young Consulting, exposing personal information of nearly one million individuals.
- In June 2024, reports surfaced that BlackSuit attacked the software provider CDK Global and disrupted the operations of car dealerships across the U.S. The incident was part of a larger pattern where ransomware groups targeted large companies by compromising their software suppliers.
- BlackSuit ransomware is a significant threat to various sectors, particularly the healthcare and technology sectors, due to its capability to target widely used Linux and Windows systems.
- Is your organization prepared to tackle a threat actor as powerful as BlackSuit?

# BlackSuit

In 2023, security researchers uncovered that the Royal ransomware group was planning to rebrand as BlackSuit. At the time, Royal ransomware was already a prominent threat, gaining further attention in May 2023 after launching a significant attack on IT systems in Dallas, Texas. Following this attack, researchers discovered a new ransomware family called BlackSuit, which targeted both Windows and Linux users. As investigations progressed, researchers began connecting the dots, revealing clear links between BlackSuit and Royal ransomware.

**Royal Ransomware 2022 - 2023**

Before exploring BlackSuit further, it's important to understand the background of Royal ransomware. Royal ransomware first appeared in January 2022, initially focusing on targets within the U.S. Although it was a relatively new operation at the time, researchers suspected that the group consisted of highly experienced threat actors, as they observed the use of well-established tactics and techniques from previous ransomware campaigns.

In September 2022, the Royal ransomware group escalated its operations, leveraging encryptors from other ransomware groups, such as BlackCat. By November 2022, they claimed responsibility for a significant attack on the Silverstone Circuit in the United Kingdom, disrupting numerous Formula One and motorcycle events. Although details of the attack were kept confidential, experts noted that Royal's encryption methods were highly secure, making decryption nearly impossible. Unlike many ransomware groups, Royal used multiple ransomware types, consistently using the **.Royal** extension for encrypted files instead of randomly generated ones.

The group continued attacks in December 2022, targeting the Travis Central Appraisal District, disrupting its servers, website, and email systems for over two weeks. Despite this, the agency managed to maintain operations by diversifying its data storage. Around the same time, the U.S. Department of Health and Human Services Cybersecurity Coordination Center (HC3) issued a warning about the rising threat established by Royal ransomware, especially to the healthcare sector. The group's ransom demands for the sector ranged from $250,000 to over $2 million.

Royal had initially used BlackCat's encryptor in their attacks but later developed their own Zeon encryptor, drawing comparisons to Conti, another notorious ransomware group that frequently targeted healthcare organizations.

Royal spreads its ransomware through tactics like malicious ads, phishing links disguised as software installers, spam emails, and deceptive forum posts. Their phishing campaigns often involved callback phishing, where they posed as service providers in fake subscription renewal emails. Victims were prompted to call a phone number, leading to social engineering that tricked them into installing remote access software, granting Royal access to corporate networks.

Operating with a select group of members, Royal kept a low profile, unlike many ransomware groups. Their ransom note, README.TXT, directed victims to a private Tor page for negotiations, where they would decrypt a few files to prove their decryption capability. The group also threatened to release stolen data if their demands weren't met, hosting victim information on a Tor site with links to the exfiltrated files.

These methods allowed the ransomware operators to expand their reach and successfully deploy various post-compromise payloads. According to Microsoft, Royal used signed binaries and delivered encrypted malware payloads, relying extensively on defense evasion techniques.

## BlackSuit's Tactics and Techniques

Currently, it appears that BlackSuit still shares similar coding with Royal ransomware. However, the group has also shown improved capabilities. BlackSuit uses a unique partial encryption method, allowing the threat actors to choose a specific percentage of data within a file to encrypt.

This selective encryption technique allows BlackSuit to lower the encryption percentage for larger files, which not only improves encryption speed but also helps evade detection by security systems. In addition to file encryption, BlackSuit's operators use double extortion tactics, threatening to release exfiltrated data publicly if the victim refuses to pay the ransom.

BlackSuit gains initial access to victim networks in several ways:

- **Phishing** - Phishing emails are the most common method used by BlackSuit to infiltrate networks. Victims often unknowingly install malware after interacting with malicious PDF documents or malvertising links embedded in phishing emails.
- **Remote Desktop Protocol (RDP)** - The second most frequent entry point, accounting for around 13.3% of incidents, involves the compromise of RDP services.
- **Public-Facing Applications** - BlackSuit actors exploit vulnerabilities in public-facing applications to gain access.
- **Initial Access Brokers** - Reports state that BlackSuit may also use initial access brokers to harvest VPN credentials from stealer logs, which are then used to breach networks.

Once inside a network, BlackSuit communicates with command and control (C2) infrastructure, downloading various tools to strengthen its foothold within the victim's network. They often repurpose legitimate Windows software to aid in their operations. In the past, Royal actors, who are associated with BlackSuit, have utilized tools like:

- Chisel
- PuTTY
- OpenSSH
- MobaXterm for

BlackSuit moves laterally across networks using tools like RDP, PsExec, and SMB, and maintains persistence with software like SystemBC and Gootloader. For data exfiltration, they utilize tools such as Cobalt Strike, RClone, and Brute Ratel, before encrypting files and disabling recovery options by deleting shadow copies and system logs.

Before initiating the encryption process, BlackSuit actors take several preliminary steps:

- **Windows Restart Manager:** They use this service to determine if targeted files are currently in use or blocked by other applications, ensuring smooth encryption.
- **Shadow Copy Deletion:** They use the Windows Volume Shadow Copy service (vssadmin.exe) to delete shadow copies, inhibiting system recovery efforts.

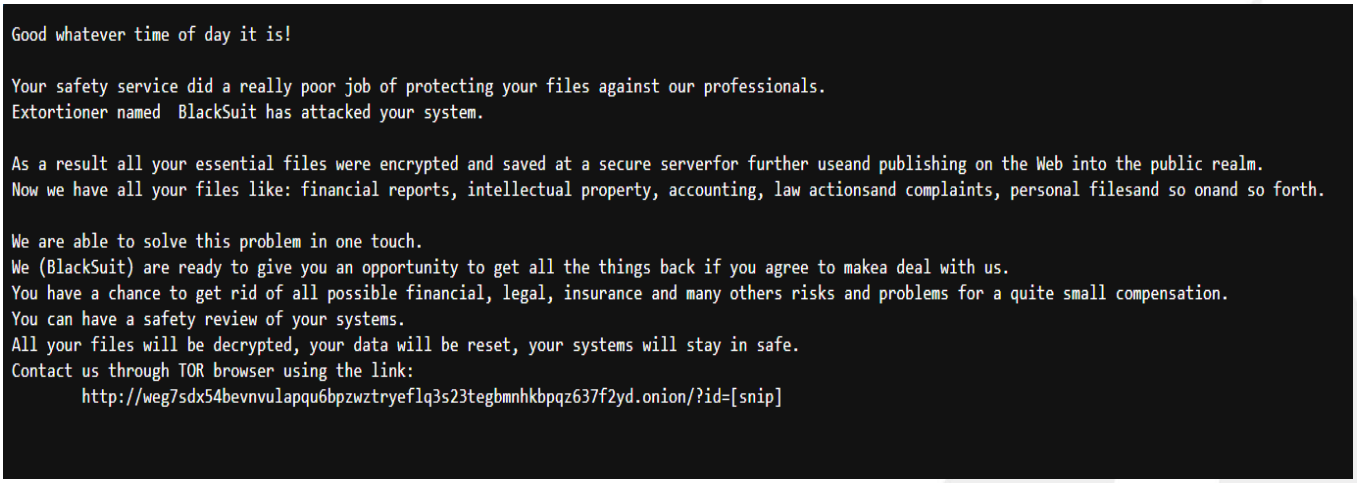
BlackSuit often stores malicious files in various directories within the victim's network, including:

- C:\Temp\
- C:\Users\<user>\AppData\Roaming\
- C:\Users\<users>\
- C:\ProgramData\

Please note that the root C:\ directory has also been used as a storage location for these malicious files.

The ransom note is written to all folders that contain encrypted items. The notes are written as "README.BlackSuit.txt".

**Image 1: BlackSuit Ransom Note**




Source: Ransomware.Live

## Recent Attacks

### Young Consulting

On May 7th, BlackSuit claimed responsibility for a data breach for Young Consulting (now operating as Connexure) – a software solutions provider. The breach occurred between April 10th and April 13th, 2024, when an unauthorized actor infiltrated the company's network and downloaded sensitive files. Nearly one million individuals had their **personal medical insurance information** exposed, including names, Social Security numbers, dates of birth, and insurance details.

BlackSuit threatened to release the stolen data publicly if the company did not respond within three days. Despite the threat, Young Consulting's management chose not to negotiate, leading to the data being posted on the dark web.

BlackSuit's post on their TOR site criticized Young Consulting's leadership for neglecting the privacy of their business partners and employees. In response, Young Consulting assured affected individuals of its commitment to information security, launched an internal review of its security practices, and offered free credit monitoring and identity theft restoration services. The FBI has already warned organizations about BlackSuit's increased targeting of critical infrastructure sectors, with ransom demands reaching as high as $60 million.

**CDK Global**

In June 2024, reports surfaced that BlackSuit attacked the software provider CDK Global and disrupted the operations of car dealerships across the U.S. The incident was part of a larger pattern where ransomware groups targeted large companies by compromising their software suppliers. CDK Global's software, commonly used by auto dealerships to process sales and other transactions, was impacted, forcing many dealers to revert to manual processing.

At the time, not much was known about BlackSuit and the number of victims on its data leak site suggested that they did not have as many hacking partners as larger ransomware groups. Although BlackSuit was not as aggressive as other ransomware groups like LockBit and ALPHV/BlackCat, it still managed to breach at least 95 organizations globally, with most victims located in the U.S. Analysts suspected that the actual number of BlackSuit victims was higher, and the group had been observed seeking new partnerships in underground forums to expand its operations.

## Conclusion

BlackSuit ransomware is a significant threat to various sectors, particularly the healthcare and technology sectors, due to its capability to target widely used Linux and Windows systems. In healthcare, these operating systems are integral for managing electronic health records, medical imaging, and other essential functions, making them prime targets for BlackSuit's attacks.

Similarly, in the technology sector, Linux and Windows systems are prevalent across various applications and infrastructures, further strengthening the potential impact of such ransomware. BlackSuit's cross-platform approach highlights the need for comprehensive cybersecurity strategies that address vulnerabilities across both operating systems, preserving the continuity and integrity of operations in critical industries. **Is your organization prepared to tackle a threat actor as powerful as BlackSuit?**

## Aspire's Recommendations

- **Endpoint Protection** - Ensure that advanced endpoint detection and response (EDR) solutions, such as CrowdStrike Falcon, are installed and properly configured to prevent ransomware from executing and to detect suspicious activities.
- **Network Segmentation and Least Privilege** - Apply the principle of least privilege to user accounts and network access, ensuring that employees only have access to the resources necessary for their roles.
- **Harden Remote Access Points** - Secure Remote Desktop Protocol (RDP) by using multi-factor authentication (MFA) and limiting RDP access to trusted IP addresses.
    - Regularly audit and secure public-facing applications to prevent exploitation.
- **Monitor and Analyze Network Traffic** - Deploy robust anti-phishing solutions and educate employees on recognizing phishing attempts, which are a common vector for initial access.
- **Prepare and Test Incident Response Plans** - Develop and regularly test an incident response plan specifically tailored to handle ransomware attacks.
    - Ensure that backup systems are regularly tested and that backup copies are stored securely and are not directly accessible from the network.

## MITRE Map

| | |
|---|---|
| **Initial Access** | T1204.002 - Malicious File<br>T1021.001 - Remote Desktop Protocol<br>T1071.001 - Web Protocols |
| **Execution** | T1059.001 - PowerShell<br>T1059.003 - Windows Command Shell<br>T1569.002 - Service Execution |
| **Persistence** | T1547.001 - Registry Run Keys / Startup Folder |
| **Privilege Escalation** | T1548 - Abuse Elevation Control Mechanism<br>T1558.004 - AS-REP Roasting<br>T1558.003 - Kerberoasting<br>T1550.002 - Pass the Hash |
| **Defense Evasion** | T1055 - Process Injection<br>T1490 - Inhibit System Recovery<br>T1486 - Data Encrypted for Impact |
| **Credential Access** | T1003.001 - LSASS Memory<br>T1550.002 - Pass the Hash<br>T1558.003 - Kerberoasting |
| **Lateral Movement** | T1021.002 - SMB/Windows Admin Shares<br>T1090 - Proxy |
| **Exfiltration** | T1071.001 - Web Protocols |

## Aspire Protects

- **Aspire Managed XDR (MXDR)**
  - Aspire Managed XDR (MXDR) combines next-generation eXtended Detection and Response (XDR) technology, a 24x7 security operations center (SOC), and the expertise of a US-based team of security professionals to identify and respond to threats across a broader attack surface.
  - Building on the existing capabilities of Managed Detection and Response (MDR), Aspire Managed XDR integrates and correlates telemetry from endpoints, networks, cloud, email, identity, and more. This advanced platform creates valuable context enabling end-to-end visibility across all threat vectors. Experienced security analysts and incident responders deliver 24x7 threat detection, analysis, and investigations – with both automated and human-led response actions to quickly mitigate cyberattacks.
- **Aspire Managed Detection and Response (MDR)**
  - Accelerate the maturity of your security operations and reduce risk with faster threat detection and response capabilities. Aspire MDR delivers around-the-clock protection across the cloud, network, and endpoints in one integrated solution.
  - Our team of experts act as an extension of your IT operations to quickly identify and mitigate security threats before they impact your business.
- **Aspire Incident Response**
  - The ability to respond effectively to data breaches is critical to every organization. When attacks occur, IT leaders need a process that will ultimately maintain business continuity, protect the company's reputation, and avoid fines, legal fees, and remediation costs.
  - Aspire offers incident response services to help you prepare for, manage, and recover from data breaches and network attacks. An experienced team uses industry-leading threat intelligence and the most current security technology to quickly respond to attacks, reduce damage, and minimize exposure.

## Indicators of Compromise (IoCs)

MD5 File Hashes

- 9b02dd2a1a15e94922be3f85129083ac
- b5266cd35d1b3770b05ad6870c0c4bde

SHA1 File Hashes

- 2bb6c8b6461edc49e22f3d0c7dc45904b2ed8a2b
- 2cb6ff75b38a3f24f3b60a2742b6f4d6027f0f2a

SHA256 File Hashes

- 27e300fa67828d8ffd72d0325c6957ff54d2dc6a060bbf6fc7aa5965513468e0
- 3b873bc8c7ee12fe879ab175d439b5968c8803fbb92e414de39176e2371896b2
- 55cde638e9bcc335c79c605a564419819abf5d569c128b95b005b2f48ccc43c1
- 60dcbfb30802e7f4c37c9cdfc04ddb411060918d19e5b309a5be6b4a73c8b18a
- 6c884e4a9962441155af0ac8e7eea4ac84b1a8e71faee0beafc4dd95c4e4753f
- 9493b512d7d15510ebee5b300c55b67f9f2ff1dda64bddc99ba8ba5024113300
- a39dc30bd672b66dc400f4633dfa4bdd289b5e79909c2e25e9c08b44d99b8953
- b1102ed4bca6dae6f2f498ade2f73f76af527fa803f0e0b46e100d4cf5150682
- e92912153cf82e70d52203a1a5c996e68b7753818c831ac7415aedbe6f3f007d
- f474241a5d082500be84a62f013bc2ac5cde7f18b50bf9bb127e52bf282fffbf

IPv4

- 147[.]78[.]47[.]178

Domains

- Svchorst[.]com

Hostnames

- As[.]regsvcast[.]com
- qw[.]regsvcast[.]com
- zx[.]regsvcast[.]com

## Supporting Documentation


Microsoft Warns of Cybercrime Group Delivering Royal Ransomware, Other Malware - SecurityWeek

CISA, FBI warn that Royal ransomware gang may rebrand as 'BlackSuit' (therecord.media)

DEV-0569 finds new ways to deliver Royal ransomware, various payloads | Microsoft Security Blog

ransomware.live/ransomware_notes/blacksuit/README.BlackSuit.txt

Deep Dive: Exposing BlackSuit Ransomware (deepinstinct.com)

Almost a million affected by Young Consulting breach, BlackSuit ransomware claims responsibility | Cybernews

Blacksuit Ransomware Compromised Network - LevelBlue - Open Threat Exchange (alienvault.com)

Investigating BlackSuit Ransomware's Similarities to Royal | Trend Micro (US)

Young Consulting notifies 954K people of data breach that compromised SSNs and other info - Comparitech

#StopRansomware: BlackSuit (Royal) Ransomware (cisa.gov)

BlackSuit Ransomware – The DFIR Report

Over 950K compromised in BlackSuit ransomware attack against Connexure | SC Media (scmagazine.com)

BlackSuit ransomware stole data of 950,000 from software vendor (bleepingcomputer.com)

BlackSuit - SentinelOne

BlackSuit Attack Analysis - ReliaQuest

Explainer: The 'BlackSuit' hacker behind the CDK Global attack hitting US car dealers | Reuters

## Appendix II: Disclaimer

*This document and its contents are not intended to serve as legal advice and should not be used as a substitute for it. The results of a Security Risk Assessment are intended to guide the implementation of diligent measures to reduce the risk of potential vulnerabilities being exploited to compromise data.*

*While the Services and this report may offer information that the Client can use to support its compliance efforts, the responsibility for evaluating and fulfilling compliance obligations rests solely with the Client, not Aspire. This report does not guarantee or assure the Client's compliance with any law, regulation, or standard.*