# BlackSuit Attack Analysis

reliaquest.com/blog/blacksuit-attack-analysis/

May 28, 2024


## Table of contents



### Key Points:

- In April 2024, ReliaQuest identified Kerberoasting in a customer's environment that marked the onset of a cyber attack by the "BlackSuit" ransomware group. The attack led to the encryption of critical systems and the exfiltration of sensitive data.
- Since May 2023, BlackSuit has successfully targeted US-based companies in critical sectors like education and industrial goods, employing varied methods to deploy its ransomware.
- An investigation by the ReliaQuest Threat Research team identified BlackSuit leveraging PsExec for lateral movement, Kerberoasting, data exfiltration, and deployment of ransomware from a virtual machine.

- This report examines the continued success of straightforward tactics, techniques, and procedures (TTPs), such as brute forcing, PsExec for lateral movement, and FTP for exfiltration, highlighting the efficacy of these techniques and the challenges in mitigating them.

---

In April 2024, ReliaQuest detected Kerberoasting in a customer's environment that marked the start of a BlackSuit ransomware attack, culminating in the encryption of critical systems and the exfiltration of sensitive data. Investigation yielded indicators of intrusion and intelligence about the adversary's TTPs. The impacted organization operates in multiple regions and has historically struggled with asset inventory and endpoint visibility due to its large number of devices and the breadth of deployments.

This report details the attack lifecycle, from the initial access achieved through an initial access broker brute-forcing a misconfigured VPN, the likely hand-off to the BlackSuit gang or affiliate, and the final encryption executed via Windows Management Instrumentation Command-line (WMIC). This report explores the adversary's methods and the critical vulnerabilities involved, reviews the defensive measures taken to mitigate the incident's impact, and highlights how automation in response and containment could have shifted the burden to the adversary during their breakout window. The report provides actionable insights for organizations to enhance their own defensive posture against similar ransomware threats.

## BlackSuit Overview

Security researchers first observed the double-extortion ransomware group Blacksuit in May 2023. Multiple investigations, including one by the US Department of Health and Human Services, have noted similarities between BlackSuit and the "Royal" ransomware operation, which is reportedly a successor to the now-defunct Conti ransomware gang. The group's pedigree, varied malware deployment methods, and advanced encryption and system recovery processes indicate that BlackSuit's operators are likely experienced and technically proficient.

BlackSuit has named 53 organizations on its data-leak site since commencing operations. Its victims are largely US-based but range in industry vertical; the group has targeted the education, industrial-goods-and-services, and construction sectors. This targeting pattern strongly suggests a financial motivation with a focus on critical sectors that either have smaller cybersecurity budgets or a low tolerance for downtime, thereby increasing the likelihood of a successful attack or a speedy ransom payment.

## Attack Lifecycle

Throughout this investigation, we observed BlackSuit favoring well-known and well-researched TTPs. The threat actor used tools like PsExec, remote desktop protocol (RDP), and Rubeus, which are all well represented in historical intrusion events. This reinforces the need for organizations to employ defense-in-depth strategies, which can help shift the burden back to the attacker and force them to come up with new techniques to accomplish their goal.

## Initial Access

In early April 2024, an unknown threat actor gained VPN access to the customer's environment through a valid account. Though there was incomplete authentication data from the VPN, it is highly likely the credentials were obtained via a brute-force attack or an external source like a former password dump.

The firewall was a non-primary VPN gateway at a disaster recovery site and was not configured to enforce MFA or certificate requirements, both of which were enforced for other firewalls, enabling the initial foothold.

**Centralized Configuration Management for Network Devices:** Using centralized change management and version control to deploy network device configurations instead of managing devices individually will cut down on misconfigurations, and, when paired with an automated inventory mapping solution, will help to ensure there are no hidden misconfigured or legacy devices.

## Lateral Movement

Over the next week, the attacker moved laterally across several Windows workstations, primarily using PsExec, a remote administration tool that was already being used within the environment.

There was a three-day pause in activity after the last workstation-related event until the next significant step in the attack chain. This delay likely indicates that an initial access broker gained access to the target system and then sold it to the BlackSuit ransomware group—or an affiliate linked to the group—who conducted further malicious activity.

Since the affected devices did not forward event logs and because the organization lacked a robust endpoint detection and response (EDR) tool, tracking lateral movement during the triage phase was difficult. Much of this activity was revealed through later forensics.

**Logging for Workstations:** Many organizations choose not to forward Windows logs from workstations because of ingest restrictions on existing SIEM licenses. It's important for organizations to be aware of the risks when making this decision and to compensate if possible.

For example, install an EDR solution or configure a tiered network so that only privileged access workstations (PAWs) can access critical infrastructure, or that, at a minimum, critical infrastructure can only be accessed through a chokepoint where logging does exist.

## Credential Access

Approximately ten days after initial access, BlackSuit used this newly gained account access to authenticate to a Windows server. The attacker then downloaded a custom payload that allowed them to load Rubeus, a toolkit for Kerberos abuse, into PowerShell, rather than ingress a compiled binary. This process is similar to those of popular offensive toolkits like PowerSharpPack.

It's possible that the threat actor pivoted to the Windows server directly from the VPN. However, because the Windows server was not forwarding logs, we were unable to confirm this. The adversary compromised more than 20 users through Kerberoasting. One additional account, which was the only one with preauthentication disabled, was compromised via AS-REP roasting.

One of the users compromised via Kerberoasting, "admin1," was a domain administrator; the attacker used this account to dump the NTDS.DIT file from several domain controllers via ntdsutil, leading to the compromise of the forest.

```
ntdsutil "ac in ntds" "ifm" "cr fu C:\Users\Public" q q
```

**Disabling Weak Encryption:** Kerberoasting is difficult to mitigate entirely because anyone can request a ticket-granting service (TGS) ticket for any service principal name (SPN) to crack offline. However, there are steps that can be taken to put the burden on the adversary and make it an unattractive option.

We overwhelmingly see attackers use Kerberoasting by taking advantage of weak encryption support (specifically RC4) in conjunction with weak account passwords. Organizations should disable the ability to request weak encryption types, which is often more straightforward than retroactively enforcing password complexity.

Before disabling support for RC4 encryption types, it's important to understand the current adoption of RC4. Searching for security event logs with Event ID 4769 logged by domain controllers that request encryption types 0x17 or 0x18 is an effective way to get an initial footprint and determine whether a configuration change is needed or if the OS itself doesn't support stronger encryption (AES support began in Windows Server 2008 and Windows Vista).

## Exfiltration

Several hours after the dump of the NTDS.DIT file, an unmonitored Windows server began initiating FTP connections to an external IP address, sending over 100GB of data over the next six hours. Subsequent device forensics revealed that the admin1 account ingressed 7zip, a file archive utility, and WinSCP, a tool for file transfer across multiple protocols, to the server approximately 30 minutes before the file transfer began.

7zip was used to locally stage and compress data from connected network shares, following which WinSCP was used to facilitate the FTP connection.

**Network Share Canaries:** Exfiltration is famously difficult to detect and stop because there are so many tools and methods threat actors can use to get data out of a network. Defending against exfiltration requires a layered approach to shift the burden back onto the adversary.

There's a lot that organizations can do from a network architecture level to make it much harder to directly transfer data out of a network, and this can be especially effective when combined with a comprehensive data loss prevention (DLP) solution to categorize, restrict access to, and audit ongoing access of data and to monitor for potentially unauthorized usage.

In the more immediate term, organizations can embed canary files within network shares to detect unauthorized access attempts that may indicate impending exfiltration.

### Impact

Approximately six hours after exfiltration, the threat actor set up a Windows virtual machine (VM) by installing VirtualBox and downloading a virtual machine file. They likely used the malicious VM to obfuscate the ransomware deployment from endpoint security tools—a tactic we've previously seen as effective.

The threat actor used PsExec from their VM to copy the ransomware payload—which was hosted on a network share—to hundreds of hosts through Server Message Block (SMB). Following this, WMIC was used to load the ransomware payload as a library, thus executing the encryptor.

```
start PsExec.exe --accepteula @C:\share$\hosts1.txt cmd /c COPY
“\\server\share$\payload.dll” "C:\****

WMIC /node:"X.X.X.X" process call create 'cmd.exe /c regsvr32.exe /n /I:"-id
\"<UNIQUE

_STRING>\" -ep 70" "C:\****payload.dll"'
```

Notably, external reporting on Royal ransomware describes the same argument schema being provided at the time of encryption, supporting the idea that there is a relationship between these groups.

## Remediation Efforts

The impacted organization took immediate action, including rolling passwords across the domain and isolating the compromised site from other global locations to limit the impact. It ran numerous response plays, focusing on remediation through hash banning and host isolation using endpoint security solutions.

To detect potential data leakage, GreyMatter Digital Risk Protection (DRP) was configured to monitor the organization's digital assets, and the ReliaQuest Threat Research team tracked the BlackSuit data-leak site for any mentions or leaked data. Various detection rules were deployed to strengthen the organization's defensive posture, including those to identify malware, suspicious DNS requests, and lateral movement activities.

## Conclusion

The investigation into the BlackSuit ransomware attack revealed a relatively straightforward set of TTPs. Our analysis identified initial access via brute forcing, lateral movement facilitated by tools like PsExec, and successful exfiltration through FTP. These techniques are not novel, and their continued success highlights the efficacy of the techniques and the difficulty of appropriate mitigation. In this case, correctly configuring the VPN, more complete endpoint visibility, and implementing automated response or containment plays could have prevented impact earlier in the attack chain. By ensuring you have the correct defenses and configurations in place, straightforward TTPs like those highlighted in this case study can be detected and prevented in the early stages, minimizing or stopping any impact on your organization.