BlackSuit Ransomware

Executive Summary
A relatively new ransomware group and strain known as BlackSuit, with significant similarities to the Royal ransomware family, will likely be a credible threat to the Healthcare and Public Health (HPH) sector. Discovered in early May 2023, BlackSuit’s striking parallels with Royal, the direct successor of the former notorious Russian-linked Conti operation, potentially places the group with one of the most active ransomware groups in operation today. Both Royal and the now defunct Conti are known to have aggressively targeted the HPH sector, and if their purported ties to BlackSuit prove to be verified, then the sector will likely continue to be attacked profoundly. What follows is an overview of the potential new group, possible connections to other threat actors, an analysis of its ransomware attacks, its target industries and victim countries, impact to the HPH sector, MITRE ATT&CK techniques, indicators of compromise, and recommended defense and mitigations against the group.

Overview
BlackSuit operates using a double extortion method that steals and encrypts sensitive data on a compromised network. So far, the specific use of BlackSuit ransomware has been observed in a small number of attacks. The most recent suspected attack, in October 2023, was against a U.S.-based HPH organization whose servers and systems were encrypted with malware, tentatively identified as BlackSuit. One cybersecurity company also documented at least three attacks involving the BlackSuit encryptor, with ransoms below $1 million. Another company annotated at least five attacks in the manufacturing, business technology, business retail, and government sectors spanning the United States, Canada, Brazil, and the United Kingdom. With only a small number of victims, the ransomware gang is considered more infamous for their purported connections to the more prolific Royal ransomware family. If their connection is confirmed, it would augment BlackSuit as a threat actor to be closely watched in the near future.

<table>
<thead>
<tr>
<th>BlackSuit Ransomware at a Glance</th>
</tr>
</thead>
<tbody>
<tr>
<td>Names Utilized</td>
</tr>
<tr>
<td>Threat Type</td>
</tr>
<tr>
<td>Encrypted Files Extension</td>
</tr>
<tr>
<td>Ransom Demanding Message</td>
</tr>
<tr>
<td>Detection Names</td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td>Distribution Methods</td>
</tr>
<tr>
<td>Consequences</td>
</tr>
</tbody>
</table>

Associations
BlackSuit operates as a private ransomware operation without any known affiliates, and is therefore not considered to be a Ransomware-as-a-Group (RaaS). Its operators are likely experienced, due to the potential ties to Royal (and by default, Conti). Both Royal and the former Conti groups were known to have well-known organizational systems, business models, and skilled operators.
Following a May 2023 attack on a major city in Texas by the Royal ransomware group, many cybersecurity researchers speculated that they would rebrand under a new name after widespread media attention and pressure from law enforcement. A new BlackSuit ransomware operation was discovered in the same month that was using its own branded encryptor and Tor negotiation sites. It was believed that this was the ransomware operation that the Royal ransomware group would rebrand into. However, a rebrand never occurred, and Royal is still actively attacking the enterprise while using BlackSuit in limited attacks.

One cybersecurity company’s analysis of the Linux variant of BlackSuit uncovered significant similarities to the Royal ransomware family. The researchers, who examined an x64 VMware ESXi version targeting Linux machines, said that they identified an “extremely high degree of similarity” between Royal and BlackSuit. Furthermore, they stated that “they're nearly identical, with 98% similarities in functions, 99.5% similarities in blocks, and 98.9% similarities in jumps based on BinDiff, a comparison tool for binary files.” A comparison of the Windows artifacts has identified 93.2% similarity in functions, 99.3% in basic blocks, and 98.4% in jumps based on BinDiff.

The most recent findings from the same company note that BlackSuit and Royal use OpenSSL’s AES for encryption, and utilize similar intermittent encryption techniques to speed up the encryption process. Overlaps aside, BlackSuit incorporates additional command-line arguments and avoids a different list of files with specific extensions during enumeration and encryption. The emergence of BlackSuit ransomware (with its similarities to Royal) indicates that it is either a new variant developed by the same authors, a copycat using similar code, an affiliate of the Royal ransomware gang that has implemented modifications to the original family, or emerged from a splinter group within the original Royal ransomware family.

Conti Ransomware
First observed in 2019, Conti is a Russian-speaking RaaS group connected to more than 400 multi-sector cyberattacks, three-quarters of which were based in the United States. Notorious for their aggressive tactics and large-scale attacks, they were known for demanding ransoms as high as $25 million. Often conducting double extortion, they relied on affiliates to target organizations with more than $100 million in annual revenue. However, leaked chats showed that some Conti members began to question the targeting of the healthcare sector, especially during the height of the COVID-19 pandemic. This led to speculation that there might be a fracturing within the group. Subsequently, following a multi-government sting operation in February 2022, the group disbanded, splintered into smaller groups, and rebranded to evade law enforcement. Despite the shutdown of that particular threat group, Conti operators remain active and collaborative in new factions, like Royal. For additional information on the Conti threat group, see four previous HC3 reports: Overview of Conti Ransomware, Conti Ransomware Amplify Alert, Conti Ransomware (Update), and Conti Ransomware and the Health Sector.

Royal Ransomware
First observed in 2022, the Royal ransomware gang thrived after the post-Conti disbanding. In its early campaigns, Royal deployed BlackCat’s encryptor. It then shifted to its own called Zeon, which dropped ransom notes similar to Conti’s. Royal later rebranded and began using Royal in the ransom notes generated by its new encryptor. The group combines the use of old and new techniques, suggesting an extensive knowledge of the ransomware scene. Their use of callback phishing to deceive victims into installing remote desktop malware lets them infiltrate victims’ machines with minimal effort. Meanwhile, the ransomware group’s intermittent encryption tactics also speed up their encryption of victims’ files. In
previous attacks, the group has requested ransom payments from $250,000 to over $2 million.

Unlike their predecessor, Royal appears to not operate as a RaaS, but as a private group without any affiliates. With financial motivation as their primary goal, the group steals data from double extortion attacks. Royal compromises have affected multiple industries, including the HPH sector. For additional information on the Royal threat group, see two previous HC3 reports: Royal Ransomware and Royal & BlackCat Ransomware: The Threat to the Health Sector.

Technical Details
BlackSuit primarily targets Linux and Windows systems, and prevents victims from accessing their files by encrypting them. BlackSuit appends the blacksuit file extension (".blacksuit") to the files it encrypts, changes the desktop wallpaper, creates and drops its ransom note ("README.BlackSuit.txt") into the directory, renames files, and lists its TOR chat site in the ransom note along with a unique ID for each of its victims. Its operators also set up a data leak site as part of their double extortion strategy to coerce victims into paying the ransom demand. The BlackSuit ransom note will make several claims, most notably that essential files have been encrypted and stored on a secure server; therefore, any financial reports, intellectual property, personal files, and other sensitive data have been compromised. Currently, there is no known public decryptor for BlackSuit ransomware available.

Once the ransomware infects a system, it uses the FindFirstFileW() and FindNextFileW() API functions to enumerate the files and directories, and initiates the encryption process. BlackSuit ransomware uses the Advanced Encryption Standard (AES) algorithm to encrypt files. The AES algorithm is a symmetric encryption algorithm that is widely used for encrypting data. BlackSuit ransomware uses OpenSSL’s AES for encryption, and leverages similar intermittent encryption techniques for fast and efficient encryption of victim files.

![Figure 1: BlackSuit Ransom Note (Source: TrendMicro)](image)

Variants
Windows Variant: The 32-bit Windows variants of the BlackSuit and Royal ransomware families share a 93.2% similarity in functions, 99.3% similarity in basic blocks, and 98.4% similarity in jumps based on BinDiff. BlackSuit and Royal use OpenSSL’s AES for encryption and leverage similar intermittent encryption techniques.
Linux Variant: The Linux variant of the BlackSuit ransomware is a 64-bit ELF executable compiled with GCC with sha256 as 1c849adccad4643303297fb66bfe81c5536be39a87601d67664af1d14e02b9e. The Linux variants of Royal and BlackSuit share 98% similarity in function, 99.5% similarity in blocks, and 98.9% similarity in jumps based on the BinDiff comparison tool.

Distribution Methods
Infected email attachments (macros): Cybercriminals may distribute BlackSuit ransomware through email attachments that contain infected links or macros. Users who open these attachments or enable macros can inadvertently trigger the execution of the ransomware on their system.

Torrent websites: BlackSuit ransomware can be embedded into torrent files, which are commonly used for downloading and sharing files through peer-to-peer networks. When users download and open these infected torrent files, their systems can become infected with the ransomware.

Malicious ads: Malicious ads, also known as malvertising, can be used as a method to distribute BlackSuit ransomware. Users who click on these ads may be redirected to websites that automatically download and install the ransomware on their system.

Trojans: BlackSuit ransomware can be delivered through Trojans, which are malicious programs that can download and install other types of malware, including ransomware. Trojans can be distributed through various means, such as phishing emails, fake software updates, or compromised websites.

Target Countries and Industries
With only a small number of victims, it is difficult to draw any tangible conclusions about the BlackSuit threat group’s preferred targets, if any. Thus far, the group has targeted the following countries: The United States, Canada, Brazil, and the United Kingdom. If ties to Royal (and by extension, Conti) are confirmed, then the correlation to these Russian-speaking threat actors will likely support a geographic exclusionary pattern by the group. Both Royal and Conti are known to exclude ex-Soviet or Commonwealth of Independent States (CIS) countries from being targeted in attacks. Additionally, while only a few victims are known, its target industries appear to be indiscriminate, including the healthcare, manufacturing, business technology, business retail, and government sectors. Continued monitoring of this group over the next year will likely demonstrate more about their motivations and specific targeting preferences.

Impact to Healthcare and Public Health (HPH) Sector
BlackSuit has only one purported victim from the HPH sector in the United States. The ransomware attack was significant, as the victim provides medical scans and radiology services for almost 1,000 hospitals and health systems in 48 states. The initial impact of the attack caused the victim to shut down computer systems and turn away patients at fixed-site locations. No further details are known at this time, although given the ubiquitous geographic presence of the victim, significant impacts could still follow. Given both Royal and Conti’s longstanding record of targeting this particular sector, if BlackSuit’s ties to either of the two groups is confirmed, then the healthcare industry should anticipate more attacks to come.

MITRE ATT&CK Techniques
Several cybersecurity researchers have annotated specific MITRE ATT&CK techniques.
## MITRE ATT&CK TTPs of BlackSuit Ransomware (Source: Cyble)

<table>
<thead>
<tr>
<th>Tactic</th>
<th>Technique ID</th>
<th>Technique Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>Execution</td>
<td>T1204</td>
<td>User Execution</td>
</tr>
<tr>
<td></td>
<td>T1059</td>
<td>Command and Scripting Interpreter</td>
</tr>
<tr>
<td>Discovery</td>
<td>T1057</td>
<td>Process Discovery</td>
</tr>
<tr>
<td></td>
<td>T1082</td>
<td>System Information Discovery</td>
</tr>
<tr>
<td></td>
<td>T1083</td>
<td>File and Directory Discovery</td>
</tr>
<tr>
<td>Impact</td>
<td>T1486</td>
<td>Data Encrypted for Impact</td>
</tr>
<tr>
<td></td>
<td>T1490</td>
<td>Inhibit System Recovery</td>
</tr>
</tbody>
</table>

### Indicators of Compromise (IOCs)

#### BlackSuit IOCs (Source: Alien Vault)

<table>
<thead>
<tr>
<th>Indicator</th>
<th>Indicator Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>748de52961d2f182d47e88d736f6c835</td>
<td>MD5</td>
<td>BlackSuit Windows Executable</td>
</tr>
<tr>
<td>30cc7724be4a09d5bcd9254197af05e9fab76455</td>
<td>SHA1</td>
<td>BlackSuit Windows Executable</td>
</tr>
<tr>
<td>90ae0c693f6f6d6dc5bb2d5a5ef078629c3d77f874b2d2ebd9e109d8ca049f2c</td>
<td>SHA256</td>
<td>BlackSuit Windows Executable</td>
</tr>
<tr>
<td>9656cd12e3a85b869ad90a0528ca026e</td>
<td>MD5</td>
<td>BlackSuit Linux Executable</td>
</tr>
<tr>
<td>861793c4e0d4a92844994b640cc6bc3e20944a73</td>
<td>SHA1</td>
<td>BlackSuit Linux Executable</td>
</tr>
<tr>
<td>1c849adcccad4643303297fb66bfe81c5536be39a87601d67664af1d14e02b9e</td>
<td>SHA256</td>
<td>BlackSuit Linux Executable</td>
</tr>
</tbody>
</table>

#### BlackSuit IOCs (Source: Trend Micro)

<table>
<thead>
<tr>
<th>SHA256</th>
<th>Detection Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>90ae0c693f6f6d6dc5bb2d5a5ef078629c3d77f874b2d2ebd9e109d8ca049f2c</td>
<td>Ransom.Win32.BLACKSUIT.THEODBC</td>
</tr>
<tr>
<td>1c849adcccad4643303297fb66bfe81c5536be39a87601d67664af1d14e02b9e</td>
<td>Ransom.Win32.BLACKSUIT.THEODBC</td>
</tr>
<tr>
<td>6ac8e7384767d1cbb792e62e09ef3c1a07398ca2043652ab11c090e6a585b310</td>
<td>Ransom.Win32.ROYAL.AA</td>
</tr>
<tr>
<td>4d7f66c6a051ecb1f8410243cc6941b339570165ebcf3cc7db48d2a924874e99</td>
<td>Ransom.Win32.ROYAL.SMYECJYT</td>
</tr>
<tr>
<td>b57e5f0c857e807a03770feb4d3aa254d2c4c8d9e08687796be30e2093286c</td>
<td>Ransom.Win32.ROYAL.TBOBBC</td>
</tr>
</tbody>
</table>
Defense and Mitigations
Organizations can defend against ransomware attacks by implementing a comprehensive security framework that directs resources towards establishing a strong defense strategy. Here are some recommendations:

- Create an inventory of assets and data
- Identify authorized and unauthorized devices and software
- Conduct audits of event and incident logs
- Manage hardware and software configurations
- Grant administrative privileges and access only when necessary
- Monitor network ports, protocols, and services
- Establish a whitelist of approved software applications
- Implement measures for data protection, backup, and recovery
- Enable multi-factor authentication (MFA)
- Deploy up-to-date security solutions across all system layers
- Remain vigilant for early indications of an attack

For U.S. residents and businesses, the local Federal Bureau of Investigation (FBI) field office and the Internet Crime Complaint Center (IC3) can assist with reporting a cybercrime incident. When reporting a ransomware attack, any information about it must be gathered, including:

- Screenshots of the ransom note
- Communications with the ransomware actors (if you have them)
- A sample of an encrypted file

The Way Forward
The disintegration of the Conti team produced new threat actors, many of whom carried on the legacy of the former Russian-speaking group. One of its progeny, Royal, has proven itself to be an aggressive and formidable ransomware actor in its indiscriminate targeting, but especially against the HPH sector. BlackSuit, while still in its infancy, has also shown the destructive potential of its attacks. The group’s coding and encryption correlations to Royal demonstrate the difficulty in ascertaining whether it is a novel ransomware operation, or a continuation of a previous threat actor. BlackSuit’s ties to the former two groups notwithstanding, its ransomware is currently being actively employed in cyberattacks across multiple industries and countries. The value of HPH data, in particular, signals that the healthcare industry will remain a viable target to this threat actor. In addition to the aforementioned defense and mitigation strategies, HC3 recommends that HPH organizations utilize resources from CISA Stop Ransomware, HHS 405(d), and the H-ISAC to proactively and reactively aid healthcare organizations with cybersecurity awareness and guidance.

The probability of cyber threat actors targeting any industry remains high, but especially so for the Healthcare and Public Health sector. Prioritizing security by maintaining awareness of the threat landscape, assessing the situation, and providing staff with tools and resources necessary to prevent a cyberattack remain the best ways forward for healthcare organizations.

Relevant HHS Reports
HC3: Alert – Conti Ransomware Amplify Alert (September 30, 2021)
HC3: Alert – Conti Ransomware (Update) (March 10, 2022)

HC3: Alert - Russian State-Sponsored and Criminal Cyber Threats to Critical Infrastructure (May 9, 2022)

HC3: Alert - Understanding and Mitigating Russian State-Sponsored Cyber Threats to U.S. Critical Infrastructure (March 1, 2022)

HC3: Analyst Note – Healthcare Sector DDoS Guide (February 13, 2023)

HC3: Analyst Note – Overview of Conti Ransomware (May 25, 2021)

HC3: Analyst Note – Royal Ransomware (December 7, 2022)

HC3: Threat Briefing – Conti Ransomware and the Health Sector (July 8, 2021)

HC3: Threat Briefing – Royal & BlackCat Ransomware: The Threat to the Health Sector (January 12, 2023)

References


Contact Information
If you have any additional questions, we encourage you to contact us at HC3@hhs.gov.

We want to know how satisfied you are with the resources HC3 provides. Your answers will be anonymous, and we will use the responses to improve all future updates, features, and distributions. Share Your Feedback