Threat Intelligence Report

BlackSuit Ransomware: What to Know

The BlackSuit ransomware group emerged in May 2023 and is believed to be a rebranded version of the Royal ransomware group, which itself originated from the notorious and now-defunct Conti ransomware group. Due to its connections to established ransomware groups, BlackSuit's operators have demonstrated attack methods that are more sophisticated than typical emerging ransomware groups, which indicates they are likely experienced and well-funded. While the Royal and Conti groups are distributors of ransomware-as-a-service (RaaS), BlackSuit is not currently considered a RaaS. In April 2024, there was a significant spike in activity from BlackSuit, after a steadily increasing number of attacks had been observed earlier in the year. As of May 2024, the group had leaked stolen data from at least 53 organizations. Since then, the group has steadily added more victims to their dark web shame site.

THREAT ACTIVITY

- BlackSuit employs a double extortion model, which involves both encrypting and exfiltrating data, then threatening to publish the stolen data on leak sites if ransoms are not paid. The group uses the Advanced Encryption Standard (AES) for encryption and employs intermittent encryption techniques, which are designed to impact more files over a shorter course of time by encrypting only parts of a file, helping save time and avoid detection. Their method uses API functions to enumerate the files and directories and initiate encryption.
- BlackSuit ransomware payloads are known to affect both Windows and Linux operating systems. The group has successfully used a variety of initial access vectors to access organizational networks before deploying ransomware, including phishing emails, malicious torrent files, third-party tools, malicious ads, trojans, and stolen Virtual Private Network (VPN) credentials.
- BlackSuit primarily targets organizations in the United States. The group focuses on organizations within critical infrastructure sectors, including healthcare, education, government, and manufacturing. However, BlackSuit also targets consumer sectors like retail and automotive.

SIGNATURES

- Initially, the actors target Virtual Machine infrastructure and execute commands to enumerate all virtual machines. Upon identifying relevant targets, lateral movement to systems of interest commonly results in identification of data for staging and exfiltration.
- The actors then execute encrypted file extensions that are appended with ".blacksuit," and a ransom note (README.Blacksuit.txt) is dropped in the directory where the files are located. This note will typically list the group's TOR chat site (a platform for exchanging messages and negotiating with BlackSuit), and a unique ID for the victim.
- Other signatures include changing the desktop wallpaper of its victims and renaming files. As part of their double extortion strategy, BlackSuit will set up a data leak site to publicize the hack and publish data.

RECOMMENDED ACTIONS

- Determine if security controls are tailored to the threat of ransomware and whether staff know what to do if their workstations are disabled. This can be achieved through cybersecurity incident response simulation exercises, led by an independent third party.
- Understand your organization's policies surrounding ransom negotiations and payment. Ensure your cybersecurity incident response plan details how stakeholders will respond to a ransomware attack.
- Have a strong understanding of access points across your organization, including the processes in place for resetting passwords and other methods of authentication.
- Train help desk staff to recognize signs of social engineering, and to verify identities before granting access to accounts. Make employees aware of the psychological tactics that could be used against them by threat actors.
- Create authentic, believable test phishing campaigns to send to employees for evaluating their awareness to social engineering threats.
- Retain a third party incident response firm to ensure seamless and rapid response to a cybersecurity incident.

SOURCES

- #StopRansomware: Blacksuit (Royal) Ransomware
- CISA #StopRansomware: Royal Ransomware
- CISA Conti Ransomware
- BlackSuit ransomware publishes Kansas City, Kansas, police files
- BlackSuit Claims Dozens of Victims With Carefully Curated Ransomware
- CISA, FBI warn that Royal ransomware gang may rebrand as 'BlackSuit'

Why FTI Cybersecurity

MULTIDISCIPLINARY EXPERTISE

Intelligence-led, expert-driven, strategic approach to cybersecurity challenges

Core team from intelligence agencies, law enforcement, prosecuting offices, and global private sector institutions

GLOBALLY POSITIONED

Ability to respond anywhere in the world

Ability to staff the largest and most complex engagements and investigations

Relationships with the top global intelligence agencies, regulatory authorities, and private agencies

INTEGRATED & COMPREHENSIVE

Comprehensive services include crisis communications, e-discovery, forensic investigations, and more

Seamless integration of FTI Consulting's expertise across service offerings

FTI Cybersecurity Global Offices

AMERICAS

Atlanta	Los Angeles	Sao Paulo
Boston	Mexico City	Seattle
Chicago	Miami	Toronto
Houston	New York	Washington, DC
Irvine	San Francisco	Wayne

EMEA

Berlin	Dusseldorf	Mumbai
Brussels	Frankfurt	Munich
Cape Town	Johannesburg	Paris
Dubai	London	Zurich
Dublin	Madrid	

APAC

Brisbane	Perth	Sydney
Hong Kong	Shanghai	Tokyo
Melbourne	Singapore	

CONTACT FTI CYBERSECURITY

Email: #fticybersecurity@fticonsulting.com

Phone: +1-844-CYBR-FTI (+1-844-292-7384)

FTI CONSULTING