HUNTER

EMERGING THREATS

BLACKSUIT RANSOMWARE

BlackSuit Ransomware has recently established itself as a significant threat since its emergence in May 2023. Originating from members of the Royal Ransomware group, which was split off from the infamous Conti ransomware gang, BlackSuit represents a continuation and evolution of sophisticated ransomware tactics. The ransomware is utilized by several operators a part of a Ransomware as a Service (RaaS). Its operators, leveraging extensive experience and advanced methods, have targeted a variety of sectors with particular focus on critical infrastructure, healthcare, construction, manufacturing, and industrial goods. The ransomwareâ€™s dual-extortion strategy involves both data encryption and exfiltration, pressuring victims to pay hefty ransoms under the threat of data leakage. Most recently, according to Bleeping Computer, **BlackSuit** was responsible for taking CDK Global offline, causing massive outages and a several day outage for users of their products, such as car dealerships. It is worth noting, the outage was extended from its original cyber security incident, due to a second incident occurring as the organization was brining their services back online.

THREAT SUMMARY

BlackSuit Ransomware has recently established itself as a significant threat since its emergence in May 2023. Originating from members of the Royal Ransomware group, which was split off from the infamous Conti ransomware gang, BlackSuit represents a continuation and evolution of sophisticated ransomware tactics. The ransomware is utilized by several operators a part of a Ransomware as a Service (RaaS). Its operators, leveraging extensive experience and advanced methods, have targeted a variety of sectors with particular focus on critical infrastructure, healthcare, construction, manufacturing, and industrial goods. The ransomwareâ€™s dual-extortion strategy involves both data encryption and exfiltration, pressuring victims to pay hefty ransoms under the threat of data leakage. Most recently, according to Bleeping Computer, **BlackSuit** was responsible for taking CDK Global offline, causing massive outages and a several day outage for users of their products, such as car dealerships. It is worth noting, the outage was extended from its original cyber security incident, due to a second incident occurring as the organization was brining their services back online.

BlackSuit's operators are characterized by their use of legitimate administrative tools for lateral movement, exploitation and abuse of misconfigured VPNs for initial access, and sophisticated command and control (C2) structures. Other notable attacks include operational impacts on Kansas Cityâ€™s public systems and attacks against Healthcare services. These attacks underscore the ransomwareâ€™s ability to cause widespread operational disruptions and financial losses.

Intel 471 References:

[TITAN Finished Intel Report: New phishing attacks linked to The Com (Scattered Spider) deploy Spectre RAT malware](https://titan.intel471.com/report/fintel/418738e3c9607078ca741c06a6c0bcc1)

SYNOPSIS

Purported Origins

BlackSuit Ransomware surfaced in 2023 and quickly gained attention for its sophisticated operations and their work with their affiliates/operators. The ransomware is linked to the remnants of the Conti ransomware gang, particularly through the Royal ransomware group. Researchers from AdvIntel suggest that Royal, which shares personnel and techniques with Conti, has been instrumental in developing BlackSuit. Research from Intel 471 has also corroborated these connections from the BlackSuit Ransomware group. The group is composed of seasoned cybercriminals who have seamlessly transitioned from Conti and other associated operations like Ryuk, Silent, and Quantumâ€‹.

Target Industries and Sectors

BlackSuit primarily targets organizations, industries and sectors with critical operational dependencies, including healthcare, industrial goods, and public infrastructure. The ransomware exploits these sectors' vulnerability to downtime and operational disruptions, making them more likely to pay ransoms outright with little negotiations, garnering a large profit for the affiliate and group. Key incidents, such as the attack on CDK Global and the breach of Kansas Cityâ€™s public services, illustrate BlackSuit's capability to disrupt vital services and operationsâ€‹.

Tactics and Techniques

The BlackSuit Ransomware maintains a high execution and installation probability in recent attacks, subverting security controls and successfully rendering victims unable to operate. Affiliates and operators of the ransomware have utilized several initial access vectors, such as misconfigured or outdated VPNs, purchased credentials via Access Brokers or pure brute force attacks utilizing previously compromised credentials or purchase of password lists for password spraying and other password based attacks. Once access is obtained, recent attacks have immediately pivoted to gathering credentials from services such as Active Directory and local hosts via Mimikatz and dumping credential related databases with tools such as ntdsutil, or Red Team tools such as "PowerSharpPack".

After credentials are obtained, Lateral Movement is performed to broaden the scope of their access and determine critical assets. Credentials are also utilized to access sensitive information for later exfiltration. In recent attacks, researchers have noted the attacker paused their activity for several days after credential theft or initial access to put space between their activities to appear more legitimate within the target environment. Other tools utilized for Lateral Movement have included WMIC/WMI remote commands, PSExec and RDP. These legitimate tools helped the attacker stay under the radar as they continued to spread throughout the environment.

In the final stages the attackers utilized legitimate remote access mechanisms such as RDP and WinSCP to gather and exfiltrate the sensitive data they had gathered via compressed archives (7zip). Once they had gathered the data for extortion, they delivered the BlackSuit Ransomware via remote WMI commands or PSExec. This ensured proper execution of the payload disguised as a DLL file.

HUNT PACKAGES

FIRST TIME SCRIPT OR SYSINTERNALS EXECUTION - REGISTRY KEY MODIFICATION
https://hunter.cyborgsecurity.io/research/hunt-package/d48db011-2f77-4db7-a069-e126340f4273

BLACKSUIT RANSOMWARE COMMAND FLAGS
https://hunter.cyborgsecurity.io/research/hunt-package/0FA4F8B4-18BC-4B40-AFF6-7672EABDE78D

PSEXEC COPY COMMAND ISSUED INVOLVING NETWORK SHARE - POTENTIAL MALWARE COPY
https://hunter.cyborgsecurity.io/research/hunt-package/

POSSIBLE KERBEROASTING - TICKET GRANTING SERVICE (TGS) REQUEST WITHOUT LOGIN
https://hunter.cyborgsecurity.io/research/hunt-package/86186a7b-3cd7-43d0-846a-26d5c51e5c8f

REMOTE WMI COMMAND ATTEMPT
https://hunter.cyborgsecurity.io/research/hunt-package/9f2e163b-4f26-4972-b3d5-31c0b24b98a0

DUMP ACTIVE DIRECTORY DATABASE WITH NTDSUTIL - POTENTIAL CREDENTIAL DUMPING
https://hunter.cyborgsecurity.io/research/hunt-package/98846e7f-c90c-4156-8643-54a613286b66

SUSPICIOUS BCDEDIT ACTIVITY - POTENTIAL RANSOMWARE
https://hunter.cyborgsecurity.io/research/hunt-package/8a4f0a60-2b55-4dfd-8788-8691e11e1ca1

WINSCP SESSION CREATED - POSSIBLE DATA EXFIL
https://hunter.cyborgsecurity.io/research/hunt-package/acbe6ddb-8762-4af5-9d85-e644d7bcce44

POSSIBLE KERBEROASTING - ENCRYPTION DOWNGRADE ATTACK
https://hunter.cyborgsecurity.io/research/hunt-package/08731b63-37a5-4230-a2c0-a93985407c6d

REMOTE PROCESS INSTANTIATION VIA WMI
https://hunter.cyborgsecurity.io/research/hunt-package/dd0ca1e2-046f-4878-b7f8-32b790420ef2

SHADOW COPIES DELETION USING OPERATING SYSTEMS UTILITIES
https://hunter.cyborgsecurity.io/research/hunt-package/2e3e9910-70c1-4822-804a-ee9919b0c419

RELATED LINKS
Sign up for free HUNTER access
BlackSuit Ransomware Emerging Threat Collection

MITRE CONTEXT

- Tactic Names:
  - Defense Evasion
  - Impact
  - Credential Access
  - Execution
  - Exfiltration
- Technique Names:
  - Inhibit System Recovery
  - Kerberoasting
  - NTDS
  - Windows Management Instrumentation
  - Disable or Modify Tools
  - Exfiltration Over Alternative Protocol
- Threat Names:
  - BlackSuit Ransomware
  - Conti Ransomware
  - Royal Ransomware

REFERENCES

1. https://www.cisa.gov/news-events/cybersecurity-advisories/aa24-131a
2. https://thedfirreport.com/2021/08/01/bazarcall-to-conti-ransomware-via-trickbot-and-cobalt-strike/
3. https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/lockbit-targets-servers
4. https://www.trendmicro.com/en_us/research/22/i/play-ransomware-s-attack-playbook-unmasks-it-as-another-hive-aff.html
5. https://app.any.run/tasks/6d72bdc6-2438-470c-9715-cc2dd983aeb1/
6. https://www.microsoft.com/security/blog/2022/10/14/new-prestige-ransomware-impacts-organizations-in-ukraine-and-poland/
7. https://www.cyborgsecurity.com/cyborg_labs/hunting-ransomware-inhibiting-system-backup-or-recovery/
8. https://www.sentinelone.com/labs/black-basta-ransomware-attacks-deploy-custom-edr-evasion-tools-tied-to-fin7-threat-actor/
9. https://cybersecurity.att.com/blogs/labs-research/blackcat-ransomware
10. https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2012-r2-and-2012/cc753343(v=ws.11)
11. https://www.bleepingcomputer.com/news/security/revil-ransomware-has-a-new-windows-safe-mode-encryption-mode/
12. https://www.trendmicro.com/en_us/research/23/e/investigating-blacksuit-ransomwares-similarities-to-royal.html
13. https://blog.cyble.com/2023/04/06/demystifying-money-message-ransomware/
14. https://app.any.run/tasks/135cbcd7-06bb-49d6-8ac4-b86936049365/
15. https://thehackernews.com/2023/04/taiwanese-pc-company-msi-falls-victim.html
16. https://app.any.run/tasks/cf5f25d9-62ff-4660-b999-89d9ea0c6971/
17. https://twitter.com/Threatlabz/status/1641113991824158720
18. https://www.ic3.gov/Media/News/2021/210825.pdf
19. https://www.blackhillsinfosec.com/got-privs-crack-those-hashes/
20. https://app.any.run/tasks/b343af28-87da-4458-a733-6d0ff25851af/
21. https://adsecurity.org/?p=3513
22. https://app.any.run/tasks/f85bbd56-9f8e-4887-b003-21c2acc57cd3/
23. https://thedfirreport.com/2021/03/29/sodinokibi-aka-revil-ransomware/
24. https://car.mitre.org/analytics/CAR-2016-03-002/
25. https://blog.group-ib.com/apt41-world-tour-2021
26. https://www.bleepingcomputer.com/news/security/magniber-ransomware-now-infects-windows-users-via-javascript-files/
27. https://www.bleepingcomputer.com/news/security/meet-noescape-avaddon-ransomware-gangs-likely-successor/
28. https://www.shadowstackre.com/analysis/cactus