مجلس الأمن السيبراني
CYBER SECURITY COUNCIL
United Arab Emirates

Royal Ransomware Rebrand as “BlackSuit"

Tracking #:432316132

Date:09-08-2024

TLP: WHITE

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed Royal Ransomware Actors Rebrand as "BlackSuit and this advisory provides new indicators of compromise (IOCs) associated with BlackSuit.

TECHNICAL DETAILS:

BlackSuit ransomware attacks have spread across numerous critical infrastructure sectors including, but not limited to, commercial facilities, healthcare and public health, government facilities, and critical manufacturing.

- BlackSuit ransomware is the evolution of the previously identified Royal ransomware, which was used from September 2022 through June 2023. BlackSuit shares numerous coding similarities with Royal and has exhibited improved capabilities.
- Initial Access Techniques: BlackSuit actors typically initial access through phishing emails, exploiting Remote Desktop Protocol (RDP) vulnerabilities, and leveraging malicious public-facing applications.
- BlackSuit conducts data exfiltration and extortion prior to encryption, and publishes victim data to a leak site if a ransom is not paid.
- After gaining access, BlackSuit actors disable antivirus software, exfiltrate large amounts of data, and then deploy the ransomware to encrypt systems.
- Ransom demands typically range from $1 million to $10 million USD, with a total demand exceeding $500 million. BlackSuit actors have exhibited a willingness to negotiate payment amounts.
- BlackSuit actors have been observed using legitimate software and open source tools during ransomware operations, including SystemBC, Gootloader, SharpShares, SoftPerfect NetWorx, Mimikatz, PowerTool, GMER, RClone, and Brute Rate.

INDICATORS OF COMPROMISE:

Attached file

RECOMMENDATIONS:

- Remediate Vulnerabilities: Prioritize patching known exploited vulnerabilities in systems.
- User Training: Conduct regular training sessions for employees to recognize and report phishing attempts.
- Multifactor Authentication: Enable and enforce multifactor authentication across all user accounts to enhance security.
- Incident Response Planning: Develop and regularly update incident response plans to ensure readiness in the event of a ransomware attack.
- Data Backup: Implement a robust data backup strategy to ensure data can be restored without paying ransoms.
- Monitoring and Detection: Utilize advanced threat detection tools to monitor network activity for signs of ransomware behavior.

- IOC and TTPs: Organizations are advised to stay informed regarding Indicators of Compromise (IOCs) related to BlackSuit ransomware, which include specific filenames, file paths, and malicious IP addresses.

Kindly circulate this information to your subsidiaries and partners as well as share with us any relevant information and findings.

The UAE Cyber Security Council extends its appreciation for the continued collaboration.

REFERENCES:

- https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-061a