مجلس الأمن السيبراني
CYBER SECURITY COUNCIL
United Arab Emirates

RansomHub Ransomware Campaign

Tracking #:432316208

Date:02-09-2024

TLP: WHITE

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed a ransomware campaign "RansomHub" as an escalating ransomware-as-a-service threat that has significantly affected multiple sectors, including healthcare, government, and critical infrastructure, since it first appeared in February 2024.

TECHNICAL DETAILS:

The "RansomHub" ransomware campaign as an escalating ransomware-as-a-service threat that has significantly affected multiple sectors, including healthcare, government, and critical infrastructure, since it first appeared in February 2024. This ransomware variant, which has gained notoriety for its double-extortion tactics, has already compromised over 210 organizations across various industries.

Observed Tactics, Techniques, and Procedures:

Initial Access:
RansomHub affiliates typically obtain proof-of-concept (PoC) exploits from sources like ExploitDB and GitHub to compromise systems. Some notable CVEs they have exploited include:

- **CVE-2023-3519**: Citrix ADC Remote Code Execution vulnerability allowing unauthenticated attackers to trigger a stack buffer overflow
- **CVE-2023-27997**: Heap-based buffer overflow in FortiOS and FortiProxy allowing remote code execution
- **CVE-2023-46604**: Remote Code Execution vulnerability in Apache ActiveMQ's Java OpenWire protocol marshaller
- **CVE-2023-22515**: Vulnerability in Confluence Data Center and Server allowing unauthorized admin account creation
- **CVE-2023-46747**: Bypass of authentication in BIG-IP configuration utility allowing arbitrary command execution
- **CVE-2023-48788**: SQL injection in FortiClientEMS allowing unauthorized code execution
- **CVE-2017-0144**: SMBv1 remote code execution vulnerability in Windows
- **CVE-2020-1472**: Netlogon elevation of privilege vulnerability (Zerologon

Discovery and Lateral Movement:
RansomHub affiliates use tools like AngryIPScanner, Nmap, and PowerShell for network scanning. They move laterally using methods such as RDP, PsExec, Anydesk, Cobalt Strike, and Metasploit.

Privilege Escalation, and Defense Evasion:
Affiliates escalate privileges with Mimikatz to gather credentials and gain SYSTEM access. They disable antivirus and EDR tools using WMI and custom tools. Logs are cleared and ransomware is renamed to evade detection.

Data Exfiltration:
Exfiltration is done through tools like PuTTY, AWS S3, HTTP POST, WinSCP, Rclone, Cobalt Strike and Metasploit. The ransomware itself does not contain exfiltration mechanisms.

Encryption:
RansomHub ransomware typically encrypts files using Curve 25519 elliptic curve encryption with a unique public/private key pair per victim. Encrypted files are inaccessible until the ransom is paid and the decryption key is provided.

Indicators of Compromise:
Attached File.

RECOMMENDATIONS:

- Review the Indicators of Compromise (IOCs) and implement the necessary security measures.
- Apply patches and/or mitigations for the exploited vulnerabilities.
- Employ advanced security solutions to detect and block malicious scripts. Ensure these tools are updated frequently.
- Implement MFA to add an additional layer of security, reducing the impact of compromised credentials.
- Develop and regularly update an incident response plan to ensure swift action against potential malware infections.

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/aa24-242a